Towards Functional Safety in Dynamic Distributed Systems

Dirk Dahlhaus[1,*], Ingrid Moerman[2], Nour Mansour[1], Jeroen Hoebeke[2], Xianjun Jiao[2], Jetmir Haxhibeqiri[2] and Josef Börcsök[1]

[1]*University of Kassel, Germany*
[2]*imec – Ghent University, Belgium*
E-mail: dahlhaus@uni-kassel.de; ingrid.moerman@imec.be; mansour@uni-kassel.de; Jeroen.Hoebeke@UGent.be; xianjun.jiao@ugent.be; jetmir.haxhibeqiri@imec.be; boercsoe@uni-kassel.de
[*]*Corresponding Author*

Received 21 July 2023; Accepted 27 October 2023;
Publication 07 February 2024

Abstract

Functional safety (FS) is a well-established concept to avoid technical systems to cause harm during operation. Since FS is based on information exchange, the communication infrastructure plays a vital role to enable FS. Black channel or grey channel approaches are the basis for achieving effective and efficient FS schemes. While simple safety functions (SFs) can be implemented using point-to-point (P2P) transmission protocols, they are usually not suitable to provide FS in dynamic distributed systems (DDSs). This paper discusses time-sensitive networking (TSN) as an important approach for providing FS in wireless TSN (W-TSN) and evaluates the achievable safety integrity levels (SILs) for applications based on PROFISafe running

Journal of Mobile Multimedia, Vol. 20_1, 157–180.
doi: 10.13052/jmm1550-4646.2016

over W-TSN. A discussion on initial ideas for providing FS in DDSs reveals that FS concepts have to be designed and optimized jointly with communication protocols beyond P2P transmission to improve the resulting efficiency required for applying the concepts in industrial processes.

Keywords: Dynamic distributed systems, safety integrity level, hard quality-of-service, time-sensitive networking, black/grey channel approach.

1 Introduction

Complex modern systems are characterized by distributed components and processes which are interconnected via a specific communication infrastructure to exchange information among a potentially large number of entities. Usually, the systems are described in the framework of dynamic distributed systems (DDSs) [1] which comprise, e.g., road-side units on smart intersections. In DDSs, the implementation of functional safety (FS) being concerned with the management of the level of risk in a piece of equipment or a system is of utmost importance.

The IEC 61508 standard [2, 3] is key to defining general notions and fundamental conditions to provide FS. A central notion of systems with FS is the safety integrity level (SIL) being defined in part 5 of IEC 61508. Clearly, a system can only be functionally safe if the communication among the different components to characterize the system state is working reliably and adhering to specific quality-of-service (QoS) requirements. If one considers the mitigation of a particular hazard, the entity of devices and processes in a system to implement FS is called a safety function (SF).

DDSs requiring FS and increasingly including wireless links in combination with cloud-edge computing services (CECSs) for implementation include, e.g.,

- hyperautomation referring to the combination of machine vision, robotics, communication, and learning with the explicit involvement of humans [4] or autonomous car networks
- spatially large-scale systems like electrical power distribution (smart grids) for wind power curtailment in smart grids (beyond regular re-dispatches) or fleet operation of drones
- smart warehouses and automation with mobile robots and cobots
- more abstract applications like the softwarization/virtualization of production processes.

In the cloud-edge paradigm, the edges in the aforementioned DDSs contain wind power stations, robots or intelligent sensors/actuators at production sites.

FS approaches are highly dependent on the considered application [5–7]. FS in CECSs is usually implemented using some form of certified virtual machines while additional application-specific FS aspects can then be implemented and certified individually. DDSs with FS have been investigated for specific tasks, e.g., for distributed safety within autonomous vehicles [8] and safety-related wireless machine control systems [9].

All aforementioned applications use IP layer communications over communication networks which are random in nature, time-variant, and, in general, a combination of wired and wireless transmission links. Usually, only point-to-point (P2P) communication is implemented which corresponds to the recursion of steps in the SFs similar to resolving delay-free loops in recursive filters [10].

In future DDSs with CECSs, several key problems are to be addressed for which no solution is currently available:

- There is a fundamental self-referential/dynamic problem since distributed exchange and organization of data in the cloud and/or edges should be functionally safe themselves under dynamic system conditions.
- A DDS might not just have to deal with dynamic system conditions, but with time-variant CECS components resulting, e.g., from mobile agents challenging potential solutions for static systems.
- The P2P communication must be replaced by redundant information transmission where multicast protocols are to be designed to provide the required safety integrity level (SIL).

This paper discusses specific aspects of communication systems with FS in an attempt to continue the design path towards FS in DDSs. Section 2 considers classical SFs with a centralized logic in a system providing FS. In particular, the so-called black channel approach (BCA) is discussed leading to a specific communication paradigm. The latter is then complemented by an adaptive cross-layer approach resulting in a grey channel approach (GCA). In Section 3, distributed applications are discussed which in a conventional approach can be treated conceptually in the same way as SFs in Section 2. However, the requirements are far more stringent due to the distributed hierarchy of the decision-making logic. In Section 4, a specific architecture of a classical SF is considered, where time-sensitive networking (TSN) in a

connection-oriented system set-up with wireless local area (WLAN) transmission serves for providing FS in terms of reliability and latency-bounded connectivity. Finally, conclusions are drawn in Section 5.

2 Safety Function with Centralized E/E/PES Logic

2.1 Safety Integrity Level

The standard IEC 61508-5, namely part 5 of IEC 61508, defines the SIL [3]. Annex C of IEC 61508-5 is on the determination of SIL values. The SIL is a function of specific metrics like, e.g., the probability of failure and related parameters. The higher the probability of failure, the lower the SIL, which can take values 1, 2, 3 or 4. Increasing the SIL by one corresponds to decreasing the probability of failure by an order of magnitude.

Table 1 shows the SIL values for two modes of the considered system, namely the average probability of failure on demand (PFD) for a so-called low-demand mode and the probability of dangerous failure per hour (PFH) for a high-demand (continuous) mode, respectively.

In the context of FS in DDSs, mainly the high-demand (continuous) mode PFH value is relevant.

2.2 Black Channel Approach

The standard IEC 61508-5 is on 'Functional safety of electrical/electronic/programmable electronic safety-related systems' which is usually abbreviated to "Functional safety of E/E/PES". Most SFs are implemented using a conceptual architecture as shown in Figure 1.

Here, we have essentially three safe nodes. The node C containing the E/E/PES logic is receiving a signal *s* from node A representing a sensor. Upon reception and post-processing, node C is transmitting a signal *a* to node B representing an actuator. Communication per se is implemented in a way

Table 1 SIL values for low-/high-demand modes; average probability of failure on demand (PFD) and probability of dangerous failure per hour (PFH), respectively

SIL	low-demand mode: PFD	high-demand (continuous) mode: PFH
1	$10^{-2} \leq \mathrm{PFD} < 10^{-1}$	$10^{-6} \leq \mathrm{PFH} < 10^{-5}$
2	$10^{-3} \leq \mathrm{PFD} < 10^{-2}$	$10^{-7} \leq \mathrm{PFH} < 10^{-6}$
3	$10^{-4} \leq \mathrm{PFD} < 10^{-3}$	$10^{-8} \leq \mathrm{PFH} < 10^{-7}$
4	$10^{-5} \leq \mathrm{PFD} < 10^{-4}$	$10^{-9} \leq \mathrm{PFH} < 10^{-8}$

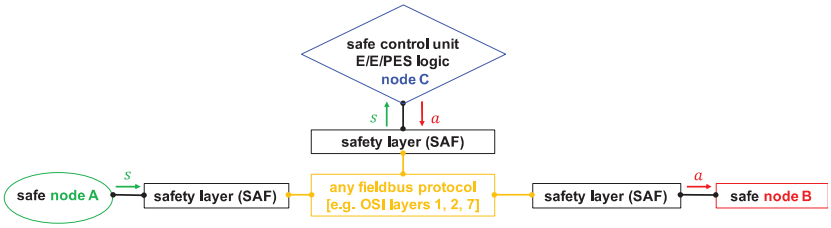


Figure 1 Conceptual SF architecture.

depending on the application at hand. Typically, some connection-oriented fieldbus protocol is being used comprising different functionalities in different layers of the Open Systems Interconnection (OSI) model.

The objective of the SF architecture comprising the sensor, the control logic, the actuator and the safety layers discussed below is to take the system to a safe state before harm can occur. As can be seen from Figure 1, the communication between the subsystems plays a fundamental role in the ability to implement FS. Specific quality-of-service (QoS) features are usually required in this context, where hard QoS is distinguished from weakly-hard QoS. FS builds upon hard non-functional QoS, in particular upon latency requirements being apparently crucial for the ability to provide FS. In DDSs, there is usually a large number of communication links which comprise wired, fibre-optical and wireless ones using different data link control protocols. The latter, in particular, are potentially based on best-effort unreliable services. Since any component, communication link, or process might be subject to failures, it is required to introduce monitoring of specific link parameters for providing FS. Therefore, in Figure 1, each node to be made safe is connected to the communication infrastructure by a so-called safety layer (SAF). The task of the latter is to ensure a proper reception of data by encapsulating the potentially unreliable communication infrastructure and to act in case a transmission error has been detected to bring the associated node into a safe state. A commonly applied SAF in industrial networks is the IEC 61784-3-3 standard known as PROFISafe [11]. Also, extensions of SAF exist for industrial wireless sensor networks (IWSNs) (Safe-WirelessHART) [12] as well as the integration between the WirelessHART and PROFISafe protocols [13]. The P2P communication in Figure 1 based on a master-slave operation and SAFs is called black channel approach (BCA) and contrasted in Figure 2 to a standard application not requiring FS. The name arises from the fact that the communication between two nodes is considered a black box and is monitored in an end-to-end (E2E) approach providing FS.

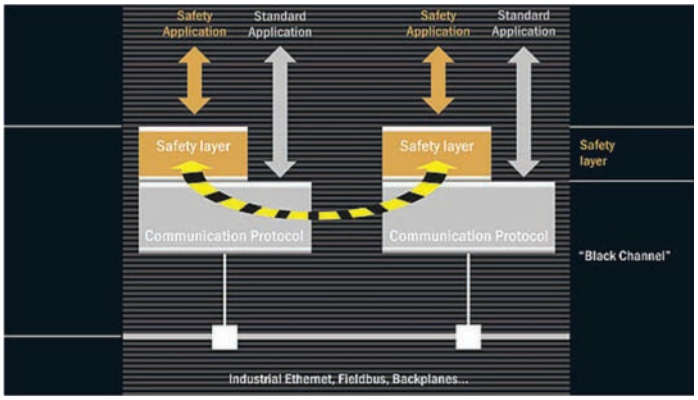


Figure 2 Black channel approach representation [14].

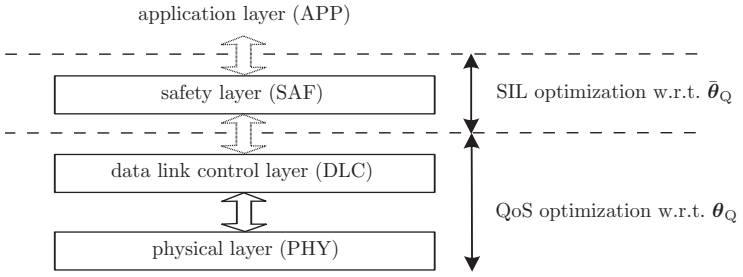


Figure 3 SIL optimization in a BCA.

The SAFs measure the SIL S and take actions according to FS standards like, e.g., the aforementioned IEC 61508 or application-specific ones. In a BCA, there are different ways to optimize the achievable SIL which can be parametrized according to $S = S(\boldsymbol{\theta})$. Here, the parameter vector $\boldsymbol{\theta} = [\boldsymbol{\theta}_{\mathrm{Q}}, \overline{\boldsymbol{\theta}}_{\mathrm{Q}}]$ contains a QoS parameter vector $\boldsymbol{\theta}_{\mathrm{Q}}$ and a non-QoS related parameter vector $\overline{\boldsymbol{\theta}}_{\mathrm{Q}}$. The OSI perspective to this set-up is shown in Figure 3.

The non-QoS related $\overline{\boldsymbol{\theta}}_{\mathrm{Q}}$ addresses, e.g., hardware (HW) redundancy, complexity and FS interfaces, while $\boldsymbol{\theta}_{\mathrm{Q}}$ contains, e.g., average bit-error rates (BERs) $\overline{P}_{\mathrm{b}}$, latency, Fourier and Shannon bandwidths and alike. The SIL $S = S(\boldsymbol{\theta})$ is calculated as shown in Figure 4.

The blocks $\mathcal{G}_1 \ldots \mathcal{G}_6$ calculate specific parameters, namely R (reliability), λ (error rate), λ_{S} (rate of safe failures), λ_{DD} (rate of dangerous detectable failures), λ_{D} (rate of dangerous failures), Λ_{PFH} (probability of failure per hour), Λ_{DC} (diagnostic coverage) and Λ_{SFF} (safe failure fraction). Finally, $\mathcal{G}_7$ calculates $S = S(\boldsymbol{\theta})$ based on $\boldsymbol{\theta}$, Λ_{PFH}, Λ_{DC} and Λ_{SFF}.

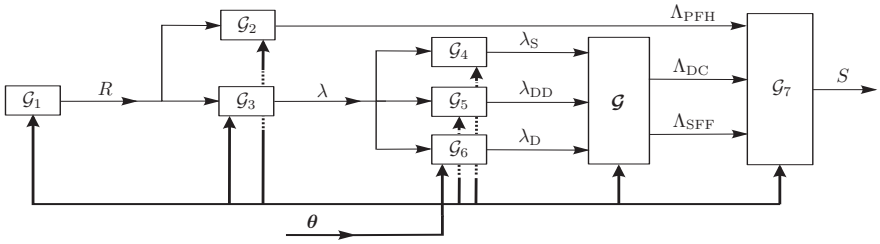


Figure 4 Calculation of SIL $S = S(\boldsymbol{\theta})$ from input vector $\boldsymbol{\theta} = [\boldsymbol{\theta}_{\mathrm{Q}}, \overline{\boldsymbol{\theta}}_{\mathrm{Q}}]$.

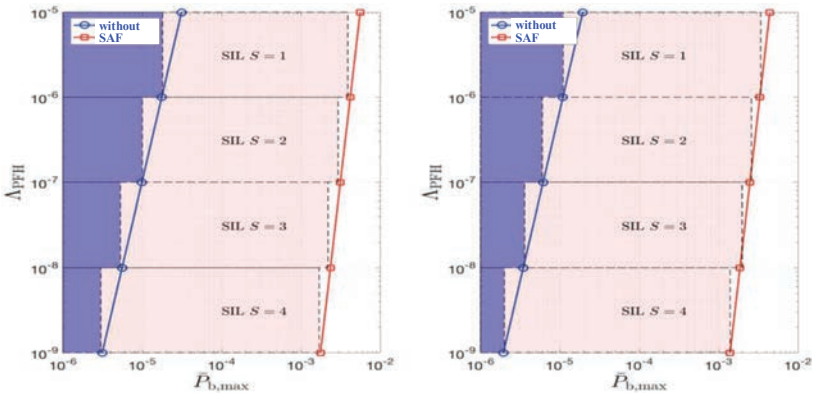


Figure 5 Ranges of achievable SIL S with/without SAF as a function of Λ_{PFH} and the admissible maximum average BER $\overline{P}_{\mathrm{b,max}}$ for Bluetooth transmission at 2.4 GHz [15]; left: data rate DM1 (108.8 kbit/s), right: data rate DH5 (723.2 kbit/s).

In Figure 5, the achievable SIL S for Bluetooth transmission in the industrial, scientific and medical (ISM) band at 2.4 GHz [15] is contrasted for a transmission with and without SAF as a function of Λ_{PFH} and the admissible maximum average BER $\overline{P}_{\mathrm{b,max}}$.

As can be concluded from Figure 5, for a given Λ_{PFH}, the range of admissible $\overline{P}_{\mathrm{b,max}}$ is increased using an SAF by more than two orders of magnitude to keep a specific value of S for both high and low data rates.

2.3 Grey Channel Approach

Apparently, using a BCA, it is no conceptual problem to achieve FS for a P2P link. However, one clearly wants to optimize system availability and thus to maximize the duration of a regular system operation. This can be done in a so-called grey channel approach (GCA) shown in Figure 6. Here, the optimization is done jointly for all components of $\boldsymbol{\theta}$.

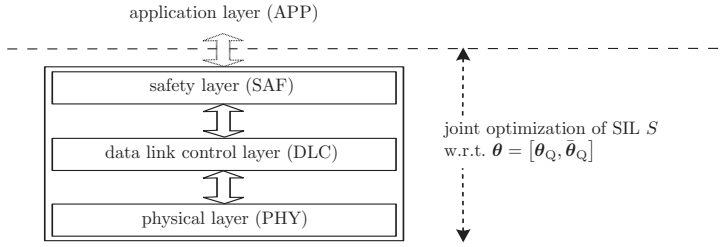


Figure 6 SIL optimization in a GCA.

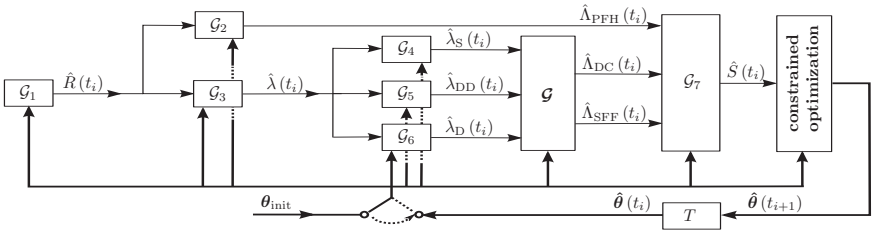


Figure 7 Dynamic constrained optimization of SIL $\hat{S}(t_i)$ for updating $\widehat{\boldsymbol{\theta}}(t_i)$.

The joint optimization cannot be implemented anymore as in Figure 4 since the jointly optimum $\boldsymbol{\theta}$ does not necessarily have the individually optimized vectors $\boldsymbol{\theta}_{\mathrm{Q}}$ and $\overline{\boldsymbol{\theta}}_{\mathrm{Q}}$ from Figure 4 as component vectors. Instead, and differently from the BCA, $\boldsymbol{\theta}$ is modelled parametrically and optimized dynamically. Therefore, the BCA's feedforward optimization is replaced by the control loop structure in Figure 7.

Here, at time t_0, the vector $\boldsymbol{\theta}$ is initialized by $\boldsymbol{\theta} = \boldsymbol{\theta}_{\mathrm{init}}$ which, for instance, might contain the individually optimized vectors $\boldsymbol{\theta}_{\mathrm{Q}}$ and $\overline{\boldsymbol{\theta}}_{\mathrm{Q}}$ from Figure 4. Based on the resulting $\hat{S}(t_0)$ and the conditions prevailing at time t_1, a constrained optimization is maximizing S to find $\widehat{\boldsymbol{\theta}}(t_1)$. Then, the switch is turned to the right and the feedback control is closed with a delay $T = t_{i+1} - t_i$. The equality and inequality constraints being used at time t_i contain all conditions on the vectors $\boldsymbol{\theta}_{\mathrm{Q}}$ and $\overline{\boldsymbol{\theta}}_{\mathrm{Q}}$ being valid at time t_{i+1}. Usually, these conditions represent control information for the next frame to be transmitted.

2.4 Time-Sensitive Networking

In both BCA and GCA approaches, the optimization in $\boldsymbol{\theta}_{\mathrm{Q}}$ with regard to latency as a non-functional QoS plays a fundamental role to provide FS.

The latter can be implemented efficiently by time-sensitive networking (TSN). The idea is to characterize an E2E IP transmission as a virtual P2P link and apply subsequently the BCA/GCA optimization to the corresponding transmission. TSN is dealt with by the IEEE 802.1 Working Group (WG) focusing on standards and recommended practices in the following areas [16]:

- 802 Local Area Network/Metropolitan Area Network (LAN/MAN) architecture,
- Internetworking among 802 LANs, MANs and other wide area networks,
- 802 security,
- 802 overall network management and protocol layers above the MAC and LLC layers.

The TSN Task Group (TG) within the IEEE 802.1 WG deals with deterministic services for IEEE 802 networks where a set of time-sensitive features over Ethernet are standardized (amongst others), namely time synchronization [17], traffic scheduling [18], frame preemption and replication [19] and network management [20]. In addition to wired networks, W-TSN can be supported via 5G Ultra-Reliable and Low-Latency Communications (URLLC) integration with wired TSN, where 5G network behaves as logical bridge [16, 21, 22]. Next to this, wireless TSN can be achieved by introducing TSN features (e.g., time synchronization, traffic scheduling) over IEEE 802.11 based networks [6, 23].

To support GCA for FS, the network should provide determinism in terms of communication reliability and latency as well as mechanisms to verify and monitor achievable performance. To achieve the first two, TSN makes use of accurate time synchronization and traffic scheduling, while the latter can be achieved by in-band network telemetry [7] that feeds back the monitored information to FS application in real time. As such, GCA is enabled in the network.

3 Functional Safety in Dynamic Distributed Systems

Alternative approaches to design DDSs with FS are cast in a distributed control system framework [24, 25] where the latter is built on some type of control hierarchy with local control tasks being supervised by a higher entity.

Indeed, the processes and topologies of a DDS are not properly represented by Figure 1. As shown in the exemplary system in Figure 8, there is usually a large number of sensors and actuators instead which are

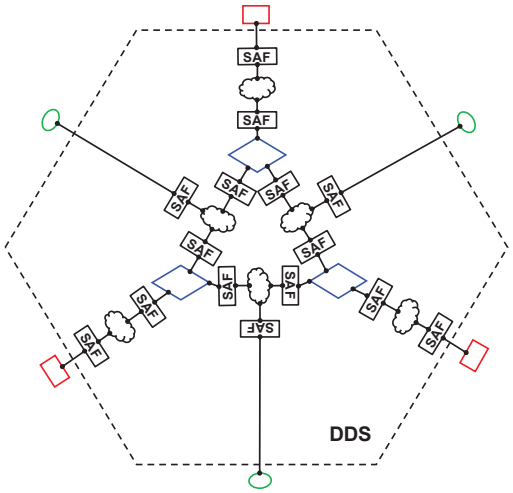


Figure 8 DDS with three sensors (in green ellipsoids), three actuators (in red rectangles) and three control E/E/PES logic units (in blue diamonds).

interconnected with a certain number of E/E/PES logic units. As mentioned above, a conventional approach to provide FS in Figure 8 is to assign a local functionality to a nearby actuator given that the corresponding sensor is also located in close vicinity. The individual SFs may be interconnected hierarchically via a superimposed control unit. In this context, a contract-based QoS assurance for centralized, hierarchical systems can be adopted, which requires local verification only and has the potential to cope with dynamic changes and uncertainties [1]. As an alternative, in case the individual processes of the logic units depend on each other, one can conceptually define a specific sequence of decisions to 'unwind' the otherwise temporally undefined sequence of processing steps. In this case, a consecutive P2P communication approach between the involved nodes may be applied including the TSN in Section 2.4.

The downside of the aforementioned approach is that the DDS state might not be available in time to implement the approach in an efficient way. Instead, one should rather generalize the FS approach as well as the corresponding communication approach to sensor vector inputs and actuator vector outputs. This results in state space descriptions of the DDS and a communication infrastructure including redundant transmissions with multicast, broadcast and diversity capabilities of the employed protocols instead of the P2P transmissions in Figure 1. In an attempt to solve the

self-referential/dynamic problem mentioned in the introduction, a completely new approach must be developed to design the FS requirements and the underlying communication protocols jointly.

4 Wireless Time-Sensitive Networking (W-TSN)

Since there is no FS paradigm currently available which would allow to design a DDS architecture according to the approach outlined in Section 3, we are considering TSN in greater depth and its impact on the achievable SIL for P2P wireless communication. In this section, we will cover the time synchronization, traffic scheduling and network monitoring approach in W-TSN and evaluate the SIL of PROFISafe over W-TSN.

4.1 Synchronization

The general E2E TSN architecture considered in the following is shown in Figure 9. For bounded communication latency, the E2E network architecture should support network-wide accurate time synchronization as well as traffic scheduling on each network hop. While both of these features are currently supported in the wired TSN, their extension to wireless IEEE 802.11 networks is ongoing. A particular realization has been achieved by utilizing OpenWiFi, an open-source IEEE 802.11 implementation for software-defined radio (SDR) platforms [26]. Time synchronization is implemented using Precise Time Protocol (PTP) over wireless links, where timestamping of PTP packets is performed utilizing Time Synchronization Function (TSF) [27]. To measure the synchronization error under different network

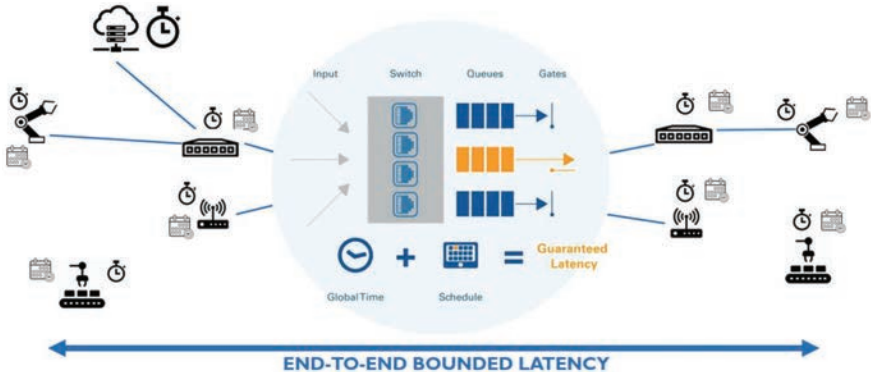


Figure 9 TSN architecture.

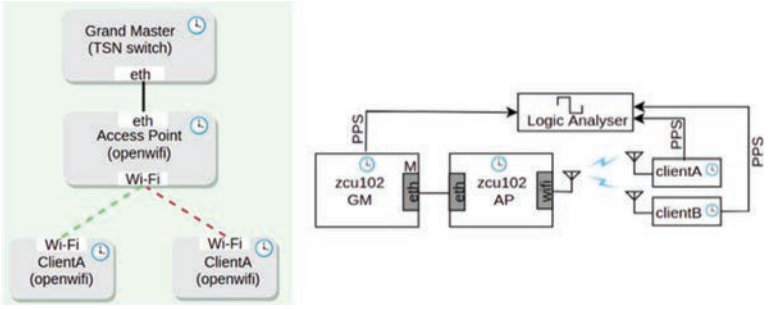


Figure 10 Experimental set-up for investigating synchronization errors in W-TSN.

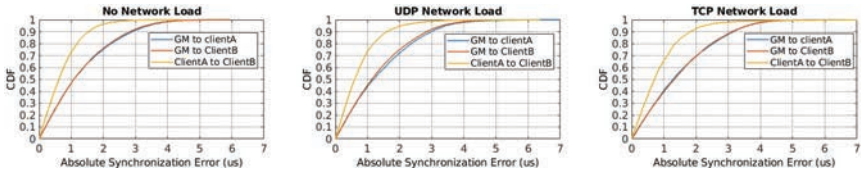


Figure 11 CDF of ASE in μs for different types of network load.

loads, the set-up in Figure 10 is being used. A grand master (GM) residing in a TSN switch is connected via Ethernet (eth) to a WLAN access point (AP) (cf. left part of Figure 10), which serves as time master for the wireless clients. For analyzing the absolute synchronization error (ASE) (cf. right part of Figure 10), the grand master (TSN Switch) and both wireless clients are connected to a logic analyzer, where they feed their PPS signal generated based on their clocks The synchronization error between the GM and each of the wireless clients as well as between wireless clients, resp., is measured by comparing their respective PPS signals.

In Figure 11, the resulting cumulative density function (CDF) of the ASE in μs is shown for three different cases, namely one case with no network load and two cases with additional traffic load over the wireless link. The latter is either User Datagram Protocol (UDP) or Transmission Control Protocol (TCP) traffic. In case of UDP, the amount of data sent over the wireless link is related to the link capacity to not overload the buffers in each of the clients and the AP. As can be concluded, there are only minor differences between the cases when the network is loaded with traffic and the case with no additional traffic.

Independently of the latter, the ASE from client A to client B is considerably less than between the GM and either of both clients. This results from

Table 2 Mean μ, standard deviation σ and 90th percentile P_{90} in μs of absolute synchronization error in μs for different types of network load

	No Load			UDP load			TCP Load		
Description	μ (μs)	σ (μs)	P_{90} (μs)	μ (μs)	σ (μs)	P_{90} (μs)	μ (μs)	σ (μs)	P_{90} (μs)
Client A to GM	0.94	1.42	2.88	0.98	1.49	2.98	0.90	1.65	3.16
Client B to GM	0.87	1.43	2.81	0.93	1.42	2.82	0.87	1.68	3.10
Client A to Client B	−0.08	0.94	1.54	−0.05	1.02	1.66	−0.03	1.19	1.8

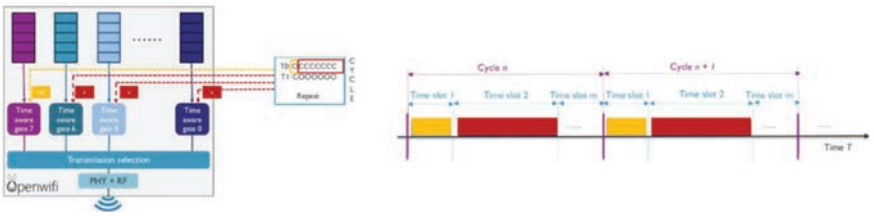


Figure 12 Gating mechanism in W-TSN.

the fact that, in the latter case, the synchronization is performed across two hops (TSN switch to AP and from AP to each of the clients).

Table 2 contains the mean μ, the standard deviation σ and the 90th percentile P_{90} in μs. It can be seen that in 90% of the cases, the E2E synchronization error is smaller than 2.88 μs in case of no traffic load, and smaller than 3.16 μs in case of TCP traffic load.

Next to time synchronization, traffic scheduling is the second important TSN feature to support E2E bounded communication latency. One way to support this in wired networks is to make use of a time-aware shaper (TAS) [18] where each traffic class will get a portion of time to access the channel on a periodic basis. The period is known as the communication cycle and gate control logic controls which queue can transmit over the medium at which moment within the cycle. When multiple queues are scheduled at the same time, channel access is done based on priorities.

To support this for wireless links, in OpenWiFi [26], a similar control logic has been implemented and applied to 8 hardware queues. As the wireless channel is a shared medium, dedicated channel access to a certain node and a certain queue is realized by muting all the other nodes during that specific time slot inside the communication cycle. For the shared time slots in the communication cycle, nodes will perform normal contention-based channel access, while conflicts between different queues are resolved based on priorities. On the left of Figure 12, the gating mechanism of TSN is shown, where the communication cycle consists of two time slots with the

first slot dedicated to queue 7 and the second slot shared amongst all the other queues. To the right of the gating mechanism in Figure 12, an example of a schedule cycle and assignment of time slots is shown.

4.2 In-Band Network Telemetry (INT)

For accurate E2E performance monitoring and verification, the concept of INT has been adopted [7]. In-band network telemetry is extended to wireless networks with various wireless link information being added, such as received signal strength indicator (RSSI), signal-to-noise ratio (SNR), retransmissions, contention window and data rate used, etc. The concept of INT is shown in Figure 13.

Here, a data packet is modified by an in-band network telemetry logic on each node to provide the corresponding monitoring information on each hop in an E2E fashion. The INT data are encapsulated either at layer 2 or at layer 3 of the OSI layer as IP extension header. Clearly, INT-enabled packets can also be used to infer service parameters like, e.g., availability (readiness for correct service), reliability (continuity of correct service), integrity (absence of improper system alterations) and maintainability (ability to undergo modifications, and repairs). This approach is being employed in Section 4.3.

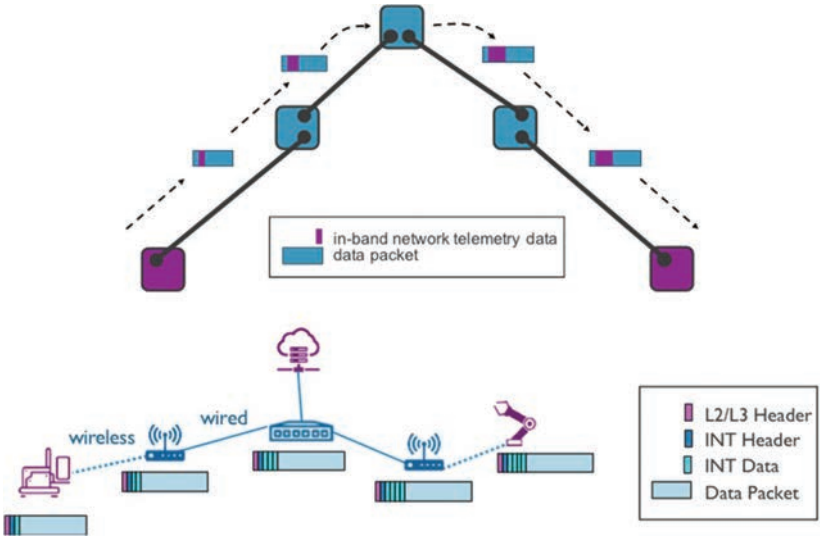


Figure 13 In-band network telemetry (INT) concept.

4.3 PROFINET Fail-Safe Verifiable E2E Traffic Over W-TSN

In this section, a PROFISafe [11, 12] application is investigated to run over W-TSN. The PROFISafe application runs on two PROFINET devices that are connected to W-TSN clients. The system set-up is shown in Figure 14 where one of the devices is a programmable logic controller (PLC) and the other is an end device controlled by the PLC. The system parameters are shown in Table 3. The PROFISafe cycle time is set to 32 ms, 16 ms and 8 ms, resp., for each test case, while the watchdog (WD) time is set to twice the cycle time.

As such, if two consecutive fail-safe packets are lost or any of the packets experiences a latency larger than the WD time, the system should enter its fail-safe state. Since the E2E latency is directly impacted by the schedule cycle length of the W-TSN, the cycle length is set to half of the length of the PROFISafe cycle time for each of the cases (e.g., 4.096 ms, 8.192 ms and 16.384 ms, respectively). Also, the time slot length is updated accordingly for each of the schedule cycles applied, as specified in Table 3. In addition, we fix the physical layer data rate at 26 Mbps using a channel bandwidth of 20 MHz for the wireless links.

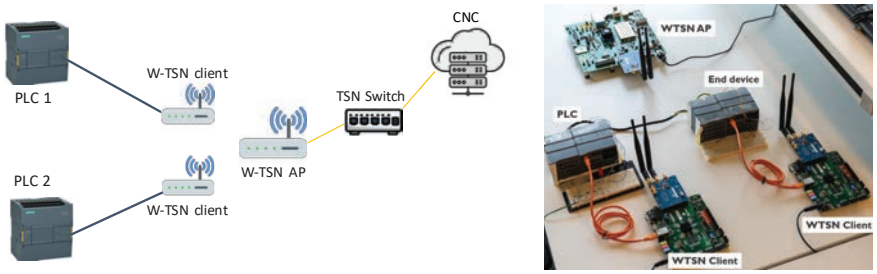


Figure 14 PROFISafe set-up: system overview (left), implementation (right).

Table 3 Application and system parameters for the PROFISafe application and W-TSN system in Figure 14

PROFIsafe application parameters

Test ID	Cycle Time [ms]	WD Time [ms]
1	32	64
2	16	32
3	8	16

System parameters

Parameter	Value
Center frequency	5170 MHz
Client bandwidth	20 MHz
Data rate	26 Mbps
Time slot length	[256, 512, 1024] μs
Schedule cycle length	[4.096, 8.192, 16.384] μs
Measurement time	1 hour

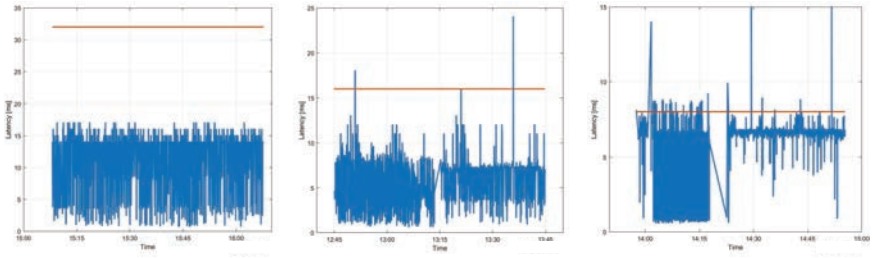


Figure 15 W-TSN with shared time slots for three different combinations of PROFISafe and schedule cycles.

Table 4 PROFISafe shared time slots results

Test ID	PFH	SIL
1	$6 * 10^{-3}$	– (HD); SIL 3 (LD)
2	$16 * 10^{-1}$	– (HD); – (LD)
3	$23 * 10^{-1}$	– (HD); – (LD)

PFH = probability of failure per hour
HD/LD = high/low demand

We consider two different scenarios. In the first one, shared time slots are employed for three different combinations of PROFISafe and schedule cycles.

During the shared time slot, the PROFISafe traffic coexists with background UDP traffic, hence, with increasing competition for channel access between PROFISafe and background traffic. The latency results are shown in Figure 15. We see that the E2E latency relates to the applied W-TSN schedule, however, in many cases, the communication link totally breaks (discontinuities in the graphs around time 13:15 and 14:17 in case of schedule cycles of 8 ms and 4 ms, respectively). Table 4 shows the resulting measured PFH values for each measurement scenario and the associated achievable SIL values resulting from Table 1. Only for the first case, the system is able to achieve SIL 1, while for the other cases, the system cannot maintain any of the SILs either for high demand or low demand specifications.

In the second scenario, dedicated time slots are employed for PROFISafe traffic and background UDP traffic for the three different PROFISafe cycle and W-TSN schedule cycle combinations. The E2E latency results are shown in Figure 16. Here one can observe that the E2E latency results are related to the applied W-TSN schedule. In addition, the amount of delayed packet cases (latency above the PROFISafe cycle shown by a red line) is limited

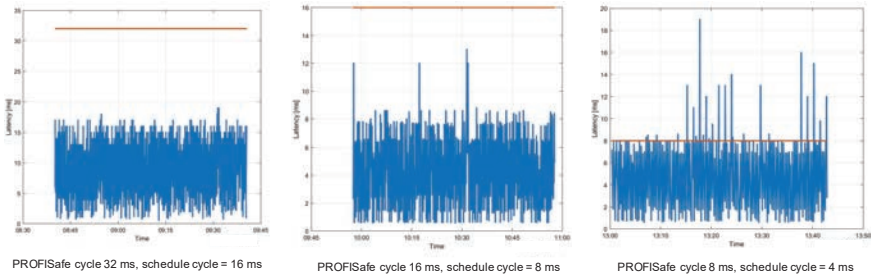


Figure 16 W-TSN with dedicated time slots for three different combinations of PROFISafe and schedule cycles.

Table 5 PROFISafe dedicated time slots results

Test ID	PFH	SIL
1	$89 * 10^{-7}$	SIL 2 (HD); SIL 4 (LD)
2	$30 * 10^{-6}$	SIL 2 (HD); SIL 4 (LD)
3	$70 * 10^{-6}$	SIL 2 (HD); SIL 4 (LD)

PFH = probability of failure per hour.
HD/LD = high/low demand.

and there are no continuous link breaks like in the previous case. Table 5 shows the resulting measured PFH values for each measurement scenario and the associated SIL values resulting from Table 1. In this case, SIL of 2 for high demand systems and SIL of 4 for low demand systems can be achieved, respectively.

5 Conclusions

The concept of FS in DDSs has been discussed with regard to the required communication infrastructure. The BCA with P2P communications turns out to be the architecture to provide FS independently of the underlying protocols for hard QoS required for sufficient SIL values.

Strategies for FS P2P fieldbus transmissions cannot be used directly in distributed applications with/without wireless communications. Yet, a BCA/GCA can be reused to maximize the SIL if combined with TSN. Specific TSN features like, e.g., high-precision time synchronization or time-aware scheduling in combination with in-band network telemetry to allow accurate E2E performance measurements over a communication network allow to overcome the impact of random/hybrid wired/wireless communication infrastructure on FS.

It is expected that a cross-layer parametric modeling of the three lower OSI layers can be used to implement dynamically a highly efficient, yet eventually complex, fail-safe network operation with large system availability. For a long-term and highly efficient FS in DDSs, a more general approach to distributed control systems must be optimized jointly with a correspondingly more general communication infrastructure and OSI protocols.

References

[1] L. Schönberger, S. Graf, S. Saidi, D. Ziegenbein and A. Hamann, "Contract-Based Quality-of-Service Assurance in Dynamic Distributed Systems," 2022 Design, Automation & Test in Europe Conference & Exhibition (DATE), Antwerp, Belgium, 2022, pp. 132–135, doi: 10.23919/DATE54114.2022.9774529.

[2] "Safety and Functional Safety", International Electrotechnical Commission (IEC), https://www.iec.ch/functional-safety.

[3] http://www.cechina.cn/eletter/standard/safety/iec61508-5.pdf.

[4] G. Peserico, A. Morato, F. Tramarin and S. Vitturi, "Functional Safety Networks and Protocols in the Industrial Internet of Things Era," Sensors, MDPI, Sept. 2021.

[5] Meany, Tom. "Functional Safety and Industry 4.0." *2017 28th Irish Signals and Systems Conference (ISSC)*. IEEE, 2017

[6] J. Haxhibeqiri, X. Jiao, E. Municio, J. Márquez-Barja, I. Moerman, J. Hoebeke, "Bringing Time-Sensitive Networking to Wireless Professional Private Networks," Wireless Pers. Commun. 121, pp. 1255–1271, 2021.

[7] J. Haxhibeqiri, P. Isolani, J. Márquez-Barja, I. Moerman and J. Hoebeke, "In-BandNetwork Monitoring Technique to Support SDN-Based Wireless Networks," IEEE Transaction of Network and Service Management 18(1), pp. 1–12, 2021.

[8] T. Bijlsma et al., "A Distributed Safety Mechanism using Middleware and Hypervisors for Autonomous Vehicles," 2020 Design, Automation & Test in Europe Conference & Exhibition (DATE), Grenoble, France, 2020, pp. 1175–1180, doi: 10.23919/DATE48585.2020.9116268.

[9] T. Malm, J. Hérard, J. Bøegh and M. Kivipuro, "Validation of Safety-Related Wireless Machine Control Systems," NT Technical Report, March 2007, https://cris.vtt.fi/en/publications/validation-of-safety-related-wireless-machine-control-systems.

[10] W. Pirkle, "Resolving Delay-Free Loops in Recursive Filters Using the Modified Härmä Method," 137th Audio Engineering Society Convention, pp. 720–729, 2014.
[11] PROFIsafe System Description, PI, June 2016.
[12] D. Yang, J. Ma, Y. Xu and M. Gidlund, "Safe-WirelessHART: A Novel Framework Enabling Safety-Critical Applications Over Industrial WSNs," in IEEE Transactions on Industrial Informatics, vol. 14, no. 8, pp. 3513–3523, Aug. 2018, doi: 10.1109/TII.2018.2829899.
[13] J. Åkerberg, F. Reichenbach, and M. Björkman, "Enabling Safety-Critical Wireless Communication Using WirelessHART and PROFIsafe," in 2010 IEEE 15th Conference on Emerging Technologies & Factory Automation (ETFA 2010). IEEE, 2010, pp. 1–8.
[14] https://www.ethernet-powerlink.org/.
[15] P. Pendli, M. Schwarz, H. Wacker, and J. Börcsök, "Mathematical Derivations for Safety related Systems with Wireless Communication," Recent Advances in Financial Planning and Product Development, pp. 23–30, Apr. 2014.
[16] https://www.comsoc.org/publications/ctn/quick-and-dead-rise-deterministic-networks.
[17] IEEE Standard 802.1AS-2020, "IEEE Standard for Local and Metropolitan Area Networks – Timing and Synchronization for Time-Sensitive Applications in Bridged Local Area Networks", IEEE Standards Association, June 2020.
[18] "IEEE Standard for Local and Metropolitan Area Networks – Bridges and Bridged Networks – Amendment 25: Enhancements for Scheduled Traffic," IEEE Std 802.1Qbv-2015 (Amendment to IEEE Std 802.1Q-2014 as amended by IEEE Std 802.1Qca-2015, IEEE Std 802.1Qcd-2015, and IEEE Std 802.1Q-2014/Cor 1-2015), pp. 1–57, 2016.
[19] IEEE 802.1CB-2017, "IEEE Standard for Local and Metropolitan Area Networks-Frame Replication and Elimination for Reliability", IEEE Standards Association, October 2018.
[20] IEEE P802.1Qcc-2018, "Standard for Local and metropolitan area networks – Bridges and Bridged Networks – Amendment: Stream Reservation Protocol (SRP) Enhancements and Performance Improvements", IEEE Standards Association, October 2018.
[21] J. Huang, L. Feng, F. Zhou, H. Liu, P. Yu and K. Xie, "5G URLLC Local Deployment Architecture for Industrial TSN Services," 2022 International Wireless Communications and Mobile

Computing (IWCMC), Dubrovnik, Croatia, 2022, pp. 7–11, doi: 10.1109/IWCMC55113.2022.9825113.
[22] Integration of 5G with Time-Sensitive Networking for Industrial Communications, 5G-ACIA, White Paper, January 2021.
[23] Cavalcanti, D. (2022). Wireless TSN: Market Expectations Capabilities and Certification. *White Paper, Avnu Alliance*, *2*.
[24] https://www.techtarget.com/whatis/definition/distributed-control-system.
[25] A. Gharbi, H. Gharsellaoui, M. Khalgui, S. B. Ahmed, "Functional Safety of Distributed Embedded Control Systems," Chapter 6 in *Handbook of Research on Industrial Informatics and Manufacturing Intelligence: Innovations and Solutions*, pp. 132–170, IGI Global, DOI: 10.4018/978-1-4666-0294-6, March 2012.
[26] X. Jiao, W. Liu, and M. Mehari. (2019) open-source ieee802.11/wi-fibaseband chip/fpga design. [Online]. Available: https://github.com/open-sdr/openwifi.
[27] M. Aslam, W. Liu, X. Jiao, J. Haxhibeqiri, G. Miranda, J. Hoebeke, J. M. Marquez-Barja, and I. Moerman, "Hardware Efficient Clock Synchronization Across Wi-Fi and Ethernet Based Network Using PTP," IEEE Transactions on Industrial Informatics, 2021.

Biographies

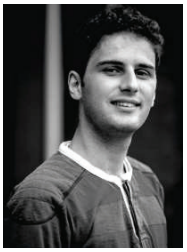
Dirk Dahlhaus received the Diploma degree in Electrical Engineering from Ruhr-University Bochum, Germany, in 1992 and the Post-Diploma in communications in 1995 and the Ph.D. degree in Electrical Engineering in 1998, resp., from ETH Zurich, Switzerland. Since 2005, he is full professor at the Faculty of Electrical Engineering and Computer Science with the University of Kassel, Germany. His research areas include wireless communications and signal processing.

Ingrid Moerman received her degree in Electrical Engineering (1987) and the Ph.D. degree (1992) from Ghent University, where she became a part-time professor in 2000. She currently combines a full professor position with part-time allocation at Ghent University and is a staff member at IDLab, a core research group of imec with research activities embedded in Ghent University and the University of Antwerp. Dr. Moerman is program manager of the 'Deterministic Connectivity Systems' track, part of the connectivity program at imec, and in this role, she coordinates research activities on end-to-end wired/wireless networking solutions driven by professional and mission-critical applications that have to meet strict Quality-of-Service requirements in terms of throughput, bounded latency and reliability in smart application areas like industrial automation, vehicular networks, safety-critical operations, professional entertainment, etc.

Nour Mansour received the B.Sc. degree in Electrical and Communications Engineering from Damascus university, in 2009. She received the M.Sc. degree in Electrical Communication Engineering in 2013 and the Ph.D. degree in Electrical Engineering in 2018, resp., from University of Kassel, Germany. Since 2018, she is a senior researcher in the Communication Laboratory (ComLab) at the Faculty of Electrical Engineering and Computer Science with the University of Kassel. Her research areas include wireless communications, machine learning and cross-layer optimization.

Jeroen Hoebeke received the Master's degree in Engineering Computer Science from Ghent University in 2002. In 2007, he obtained a Ph.D. in Engineering Computer Science with his research on adaptive ad hoc routing and Virtual Private Ad Hoc Networks. Currently, he is an associate professor in the Internet Technology and Data Science Lab of Ghent University and imec. He is conducting and coordinating research on wireless (IoT) connectivity, embedded communication stacks, deterministic wireless communication and wireless network management.

Xianjun Jiao received his bachelor degree in Electrical Engineering from Nankai university in 2001 and Ph.D. degree in communication and information system from Peking University in 2006. Then, he worked as a developer and researcher in the leading wireless tech companies, such as Nokia, Microsoft and Apple. In 2016, he joined IDLab, a core research group of imec with research activities embedded in Ghent University and University of Antwerp. As a senior researcher at imec, he works on real-time Software Defined Radio (SDR) platform. His main interests are high-performance signal processing and parallel/heterogeneous computation in wireless communications. On his research track, many international patents/papers have been granted/published.



Jetmir Haxhibeqiri received the Ph.D. degree in Computer Engineering from Ghent University, Belgium, in 2019 and the M.Sc. degree in Communication Engineering from RWTH Aachen University, Germany, in 2013. Before that, he finished his B.Sc. degree in Telecommunication from University of Prishtina, Kosovo, in 2010. Currently he is a senior researcher with IDLab research group at imec and Ghent University.

Josef Börcsök received his B.Sc. degree in 1986, the M.Sc. degree in 1991 and the Ph.D. in 1995 and his Habilitation in 2002. Since 2005, he is full professor at the Faculty of Electrical Engineering and Computer Science with Kassel University, Germany. His research areas include modelling of safety-related systems, safety chip technology (SoC) and Safety Systems on Chip (SSoC), cyberphysical systems, safe networks and distributed safety sensor systems.