Safety-related Applications over Wireless Time-Sensitive Networks

Jetmir Haxhibeqiri
IDLab, Ghent University – imec
9052 Ghent, Belgium
jetmir.haxhibeqiri@ugent.be

Pablo Avila Campos
IDLab, Ghent University – imec
9052 Ghent, Belgium
pablo.avila@ugent.be

Ingrid Moerman
IDLab, Ghent University – imec
9052 Ghent, Belgium
ingrid.moerman@ugent.be

Jereoen Hoebeke
IDLab, Ghent University – imec
9052 Ghent, Belgium
jeroen.hoebeke@ugent.be

***Abstract*—Industrial communication systems provide deterministic and reliable communication between various industrial components. In the past several decades, different communication technologies (Fieldbus, Real-Time Ethernet (RTE)) were used to achieve such determinism. Recently, Time-Sensitive Networking (TSN) is being utilized in industrial environments to support end-to-end low latency deterministic communication by providing mechanisms for accurate time synchronization, traffic scheduling/shaping, and reliability. With many use cases requiring portability and seamless mobility, such features are being developed for wireless networks as well, expanding the time-sensitive communication to the wireless domain. Wireless TSN's aim is to provide wired TSN-like features, achieving wired-wireless interoperability and flattening the automation system pyramid. In this paper, we present an integration between the wireless TSN and PROFINET. We show that the safety-related applications can be supported seamlessly, providing deterministic communication and reliability under best-effort traffic load in the wireless network. The solution is evaluated in terms of the achieved end-to-end latency and the probability of failure per hour of the fail-safe communication. It is shown that by using wireless time-sensitive networking with dedicated time slots per traffic flow a safety integrity level up to grade 4 can be achieved.**

***Index Terms*—Wireless time-sensitive networking, PROFINET, fail-safe, safety-related, PROFIsafe**

I. Introduction

Industrial communication networks are a vital point in industrial operation providing reliable communication between industrial processes, machines, and workers. Such communication needs to foster flexibility, and achieve sustainability and customization opportunities. As such, industrial communication networks should support the tight requirements of industrial applications offering accurate time synchronization, real-time communication, low latency, and jitter as well as high-reliability [1]. Over the past decades, several communication technologies (Fieldbuses, real-time Ethernet (RTE)) were used to support determinism for wired industrial networks. Similarly, several technologies (WirelessHART, ISA 100.11A) are used in the wireless network domain, which are not interoperable with the wired technologies or with each other.

In the last decade, time-sensitive networking (TSN) has become popular in industrial environments for its ability to support deterministic communication over Ethernet networks. TSN is a set of standards defined by the IEEE 802.1 TSN task group covering accurate time synchronization [2], traffic scheduling [3], frame preemption [4], frame replication [5] and network management [6]. Additionally, recent developments in the research community are bringing TSN to the wireless domain, integrating it with 5G networks [7] or WiFi [8], offering end-to-end wired-wireless time-sensitive networking.

One set of critical applications in industrial environments is safety-related applications. As such, a system to support safety-related applications needs to implement fail-safe functions. Fail-safe functions are system design characteristics that avoid any harmful or minimal damages to industrial machines, workers, and/or environment in case of system failure [9]. There are different ways to deal with system safety, such as providing redundancy (network redundancy, controller redundancy, etc.), fault-tolerance (reduced throughput or increased latency at certain levels), or contingency plans.

Several protocols have been developed to support fail-safe features like: PROFIsafe [10], openSAFETY [11], OPC UA safety [12] etc. The main characteristic of all these protocols is that they consider the communication network as a black box and do not rely on any support from the network. With the latest developments in TSN and Wireless-TSN (W-TSN), integration feasibility between such networks and safety-related applications should be proved.

In order to bring wireless flexibility for safety-related applications, the network should support a degree of determinism as well. Moreover, integration and interoperability between the industrial Ethernet network and wireless counterpart need to happen, which currently is missing. In this paper, we show (i) how safety-related applications can be integrated with a W-TSN setup, (ii) integration between PROFINET and W-TSN (iii) and feasibility of supporting safety-related over W-TSN. The paper is organized as follows. In section II we discuss the related works. Section III gives a technical background to

10.1109/ETFA52439.2022.9921559

wireless TSN and the PROFINET protocol, both being used to support the safety-related application covered in this paper. Section IV details more the design of the PROFINET packet encapsulation in the wireless channel and traffic classification. Section V shows the evaluation of the communication in terms of achieved latencies and safety integrity level for different scheduling strategies, while section VI concludes the paper.

II. Related Work

Several studies have been published regarding safety-related applications and their usage over wired TSNs as well as wireless networks. To the best of the knowledge of the authors, this paper shows for the first time the integration between the safety-related applications and a W-TSN.

In [13] authors show the feasibility of running openSafety applications on top of wired TSN and their performance. By configuring the TSN schedules of the measurement setup based on the openSafety application requirements, the time in the fail-safe state becomes zero. In [14] authors evaluate different implementations of OPC UA in terms of CPU usage, task execution time, and the power consumption for Industrial Internet of Things (IIoT) use cases. In [15] authors analyze the features of different protocols (AMPQ, MQTT, CoAP) in relation to safety-critical application support.

In [16] authors study the performance of openSafety over IEEE 802.11 wireless networks for both UDP and TCP protocols. While for clear channel usage the functional safety application can perform pretty well, under interference the time in a safe state can go up to 380 s in one hour for a stringent application with a cycle time of 5 ms [16]. Similarly, authors in [17] assess the feasibility of using WiFi for supporting Fail-Safe EtherCAT (FSoE) protocol. In a controllable wireless setup (communication happening via the coaxial cables) they evaluate the FSoE performance in terms of packet loss and the polling time statistics. It is shown that by decreasing the received power level the polling time is increased as well as packet losses. In [18] authors present an integration method between PROFIsafe and WirelessHART. Further, in [19] authors evaluate the feasibility of such integration. They analyze the round-trip time and bit-error rate of safety-critical communication and show that under certain conditions (e.g. high noise in the wireless channel) safety-critical certification requirements are not fulfilled. In [20] authors propose a safety architecture for low-latency industrial sensor networks based on IO-Link wireless networks.

In [21] authors present a methodology to characterize the safety capabilities of a wireless redundant system. To improve availability and reduce the failure probability a voting system based on a combination of filtering and cross-checking technique is proposed. Similarly in [22] authors present a methodology to characterize the deep fading impact on wireless links in regards to the ability to support safety functions.

Contrary to using the wireless communication (being it IEEE 802.11 in [16] or WirelessHART in [18], [19] or IO-Link [20]) as is, the presented work uses W-TSN to show the feasibility of supporting certain safety integrity levels (SIL).

III. Background

This section provides a short background on technologies to make it easier for the reader to navigate through the content of the paper.

A. Wireless Time-Sensitive Networking

As described in section I, TSN is a set of different standards that defines various network functionalities and features to support deterministic communication. The most basic set of TSN functionalities includes accurate time synchronization, traffic scheduling, and traffic classification mechanism.

End-to-end time synchronization of the network can be achieved using the Precise Time Protocol (PTP) [2] that has been extended to the wireless network as well [23]. Time synchronization is based on two-way exchanges of synchronization packets between the time master and its slaves. The time master will propagate *Sync* packets that are followed by *FollowUp* packets for accurate time-stamping of the time when the *Sync* packet was transmitted. The other two packet exchanges, *DelayReq* and *DelayResp*, are exchanged between the slave and the master to account for the transmission delays in the link.

Traffic scheduling is the second enabler for deterministic communication. Time-Aware Shaper (TAS) [3] deals with traffic scheduling in TSN, where each traffic class will get a portion of time to use the transmission medium. Such a mechanism is designed to separate certain time-critical traffic flows from other best-effort (non-time-critical) traffic flows in the network, by assigning dedicated time slots (TS) for it, ensuring fast channel access. As such, time is divided into communication cycles, while cycles are divided further into time slots. Each communication port in the network will have a certain number of physical queues to which a certain TS is assigned. Communication TS inside a cycle can be dedicated to a single queue or shared between different queues. In the latter case, the queue with higher priority will get the chance to transmit first. All the timing inside the cycle is managed by Gate Control List (GCL) that opens/closes queues at certain times. Such a gating system is shown in Figure 1.

To achieve traffic shaping, traffic flows need to be classified and be directed to certain queues based on their identifiers. Such identifiers include VLAN tag IDs inside the layer 2 packet header, or Differentiated Services Code Point (DSCP) values from layer 3 header when IP packets are used. For certain packet to be queued on certain hardware queue, a mapping between such values (VLAN ID or DSCP value) to the queue ID needs to happen. Usually there are far more classification IDs available than queues. Hence, a number of traffic flows will end up sharing the same queue.

B. PROFINET and PROFIsafe

PROFINET is an industrial Ethernet-based standard defined by IEC 61158 and IEC 61784 that supports all requirements for automation technology [24]. PROFINET is fully compatible with Ethernet communication at the physical layer. PROFINET defines the following device groups: PROFINET

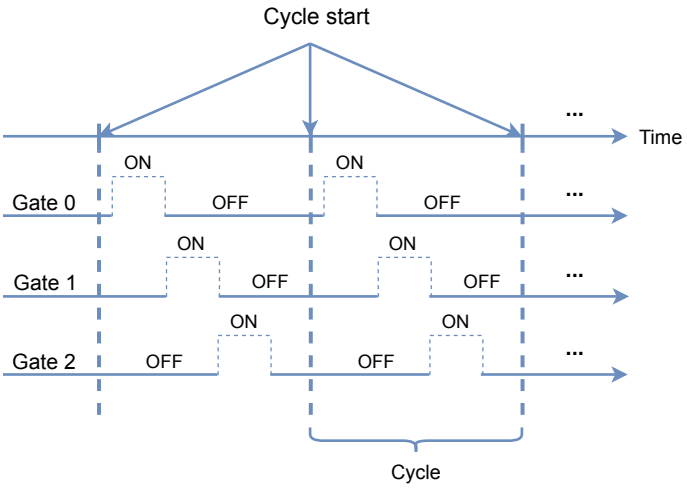


Fig. 1: Gating system for traffic scheduling in W-TSN

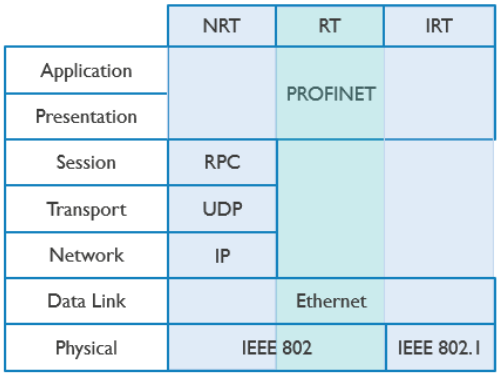


Fig. 2: PROFINET communication channels.

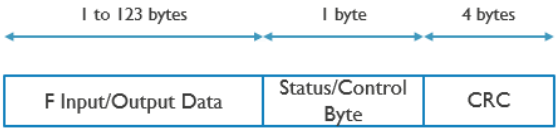


Fig. 3: Safe Protocol Data Unit (SPDU) format

controllers (Programmable Logic Controllers (PLCs), Distributed Control Systems (DCS), or Programmable Automation Controllers (PAC)), PROFINET devices (I/O blocks, drivers, process instruments, etc.) and PROFINET supervisors. PROFINET devices are stand-alone devices that communicate directly with their controllers. They transmit real-time (cyclically) data to the controller in addition to certain alarm data. On the other hand, PROFINET controllers aggregate all the real-time data received by the devices as well as collect the information regarding the alarms and maintenance status of the devices. PROFINET supervisors are similar to controllers, with the exception that they are not part of the network daily and they do not access real-time data from devices. They can be used only to read diagnostics data from devices when needed and to configure them [24].

Based on the application requirements, if the data needs to be delivered immediately or when the communication needs to be fail-safe, PROFINET supports different communication channels that differ in the number of OSI stack layers they employ. The non-real-time communication channel employs the full UDP/IP stack with PROFINET running at the application layer, whereas the real-time and isochronous real-time communication channel supports the PROFINET communication on top of the Ethernet layer as shown in Figure 2. Each device can use one or multiple communication channels at the same time. Based on this, three different device conformance classes (CC) are defined [25]. Devices of CC A support cyclic real-time communication, alarms, and topology information sharing using Link Layer Discovery Protocol (LLDP). Devices of CC B, in addition, support network diagnostics sharing via SNMP protocol over IP, while CC C devices support also bandwidth reservation and time synchronization.

PROFINET transfers data transparently, thus the end devices must interpret data in their user programs. As such, application profiles are determined by specifying certain properties, performance characteristics and device behavior [26]. One of the general application profiles is PROFIsafe which implements the fail-safe functions to reliably protect a system from harmful and hazardous operation [10]. The fail-safe messages (F-message) are exchanged between the F-host and F-device as a payload of a PROFINET frame. A safe protocol data unit (SPDU) is composed of F-Input/output data field (from 1 to 123 bytes maximum), the status/control byte (depending on if the SPDU is sent by F-host or F-device), and the CRC as shown in Figure 3. In addition to the CRC check, to ensure the safety of exchanged information, PROFIsafe includes a monitoring number generator. Such number generators are synchronized via the control/status byte. Further, the protocol foresees a watchdog time for each message exchange and a unique identifier (F-address) that is used to initialize the monitoring number generator seed for each connection [10].

C. Functional safety

Each industrial system must comply with a certain level of safety in order to prevent undesired interruptions in operation and hazardous operation. As such functional safety mechanisms need to be part of each industrial system, considering failure probability of individual parts of the system and minimizing the overall failure rate. A safety function maintains and/or achieves a safety state of the system once part of it fails. The functional safety mechanism needs to comply to the international safety standard defined by IEC 61508 [9].

Modern safety standards specify the safety integrity levels (SILs) based on the likelihood of a safety system performing the required function satisfactorily within a given time period [27]. The SIL is described as a discrete level (1 to 4) that specifies the integrity of safety function. The higher the SIL, the lower the failure probability of the safety system. SILs depend on the type of the system used, either being on high demand or low demand mode. For high demand mode

TABLE I: Safety integrity levels (SILs) and their probability of failure.

SIL	Low demand system	High demand system
4	10^{-4} to 10^{-5}	10^{-8} to 10^{-9}
3	10^{-3} to 10^{-4}	10^{-7} to 10^{-8}
2	10^{-2} to 10^{-3}	10^{-6} to 10^{-7}
1	10^{-1} to 10^{-2}	10^{-5} to 10^{-6}

operation SIL is based on the probability of dangerous failure per hour, while for low demand mode SIL is based on the average probability of failure on demand. The SILs and their probability of failures for both systems are given in Table I. Thus, if certain system will have a probability of failure per hour (PFH) of 10^{-4} but requires SIL 4 for continuous system, the difference must be achieved by implementing functional safety mechanisms in the system.

IV. Integration between W-TSN and PROFINET

To support the transmission of PROFINET traffic via wireless TSN, we made use of imec's W-TSN evaluation kit, which has been built on top of openwifi [28], the first open-source Wi-Fi implementation. For achieving accurate time synchronization in the wireless domain, PTP over wireless is used [23], while for the scheduling a gated system similar to IEEE 802.1Qbv is used in the wireless end devices and the access point. In addition to the internal openwifi hardware queues, the gated system also considers the shared medium characteristic of the wireless channel. This means that when a dedicated TS is given to a queue in one node, all the other queues in the same node as well as in other nodes are closed. As such dedicated and fast channel access is ensured for the sensitive traffic flows.

Next to enabling W-TSN between the wireless end devices and access point, the traffic needs to be bridged from the wired network domain (PROFINET) towards the wireless network domain, to be real-time monitored [29] and to be classified accordingly. We followed three main criteria for the integration. (i) The wireless TSN domain needs to behave like a layer two bridge for the TSN traffic. (ii) The traffic flows will be classified based on the layer two VLAN tags similar to what is followed in wired TSN. (iii) The traffic flows still need to be monitorable even in the layer two W-TSN bridge using in-band network telemetry [30]

A. Encapsulation in the wireless network domain

The wireless network domain can behave like a layer three routed network or like a layer two bridged network. In the former case, the PROFINET packet needs to be encapsulated in an IP packet just to be transferred in the W-TSN domain. Moreover, bookkeeping of mappings between the PROFINET devices served by a single wireless node needs to happen, which will increase the processing times of the packet in the wireless nodes. And lastly, it will break the layer two communication aspect required by the PROFINET real-time and isochronous channel. In the latter case, faster processing is ensured and the layer two communication is not broken even for PROFINET real-time communication.

When multiple end devices use a single wireless device to connect to the wireless network, then, according to the IEEE 802.11 standard, a 4-address tuple needs to be used where the source/destination and transmitter/receiver layer two addresses are specified in the packet. Another possibility is if the packet is already encapsulated in another layer two header that contemplates the layer two addresses of the devices in W-TSN domain. The Provide Backbone Bridge (PBB) specification, IEEE 802.1ah, [31] is used since a long time as a layer two encapsulation method that avoids the need for the network to learn all the MAC addresses of all the devices that are connected via it. In this case, the network only needs to learn the MAC addresses of the edges of the network.

In Figure 4, the packet format of the encapsulated PROFINET packet before it gets transmitted over the wireless channel is shown. The encapsulated packet is composed of the inner Ethernet header (the original header added by the PROFINET device) and the outer Ethernet header (added by the wireless device). The B-DA is the bridge destination MAC address, B-SA is the bridge source MAC address, the B-TAG is the VLAN tag of the outer Ethernet header, the C-DA is the PROFINET device destination MAC address, the C-SA is the PROFINET device source MAC address and the C-TAG is the VLAN tag of the inner Ethernet header. When transmitted over the air the outer Ethernet header will be used to form the layer two IEEE 802.11 header, while the encapsulated PROFINET packet will remain untouched.

B. Traffic classification

Traffic classification is important for scheduling in every TSN network. In our implemented W-TSN, the traffic classification can be done either by DSCP value of the IP header or by the VLAN tag.

In order to maintain the traffic priority set by PROFINET, the VLAN tag of the inner Ethernet header is mapped to the VLAN tag of the outer Ethernet header. For cases when traffic flows originating from a PROFINET device use the IP protocol, the encapsulation logic in the wireless device will map the DSCP value to the VLAN tag of the outer Ethernet header. As such, the wireless end device will only parse the VLAN tag of the outer header (B-TAG) to determine classification of the traffic flow.

V. Results

This section presents the obtained results in a dedicated W-TSN setup using two different traffic scheduling strategies.

A. Evaluation setup

The W-TSN of the evaluation setup is composed of one access point and two wireless clients. All wireless nodes run the openwifi implementation of WiFi chip, extended with time synchronization [23] and traffic scheduling capabilities [8]. The PROFIsafe application runs in two PROFINET devices (Siemens Simatic S7-1200 PLC devices), one of them being

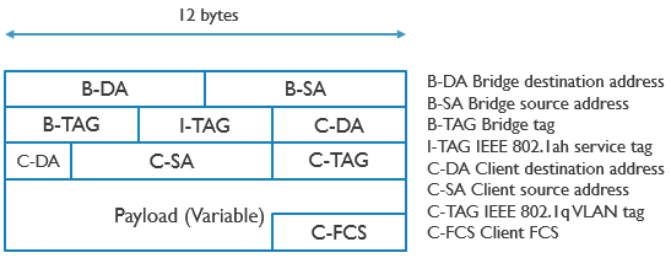


Fig. 4: IEEE 802.1ah packet format as seen before it gets transmitted over the air.

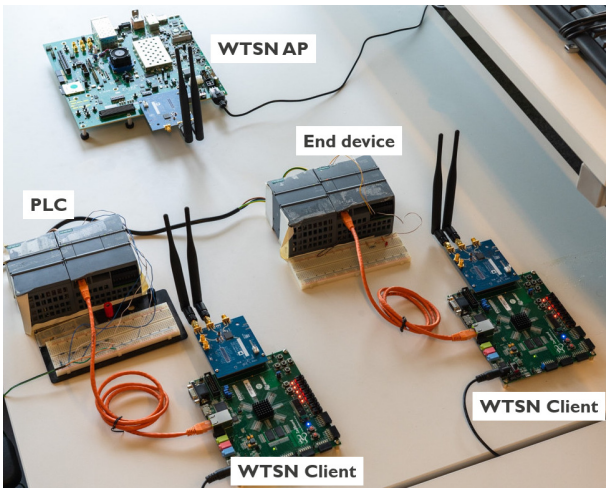


Fig. 5: Evaluation setup.

the PLC and the other the end device. The evaluation setup is shown in Figure 5. The PROFINET devices are connected to the wireless end devices, while the communication between them is enabled via the W-TSN.

The PROFIsafe application example parameters are given in Table II. The WD time is always set twice the cycle time. This means that if one F-message is missed or delayed for more than one cycle, the application will enter the safe state. A possible F-safe traffic application could be to control openings of gates of a fenced industrial yard where a crane is operating.

For each test, we create a dedicated schedule for the fail-safe traffic, while the background traffic is assigned its own schedule. To maintain the timing requirements of the fail-safe traffic the scheduling is adjusted accordingly. The schedule cycle time is set to half of the F-safe application cycle time. This will ensure that there are sufficient transmission TSs in the schedule to transmit all the F-safe traffic. The schedule organization is shown in Figure 6. The F-safe traffic is scheduled in queue 4. Each PROFIsafe node will send F-messages to the other node periodically. For that, each queue 4 TS at the wireless client-side is followed by the AP queue 4 TS. As such, the transmission of the F-messages from the wireless client to AP and from AP to the other wireless client is not delayed. Queue 1 is used for PTP traffic and other IEEE 802.11 control and management traffic. In this

TABLE II: PROFIsafe application parameters

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

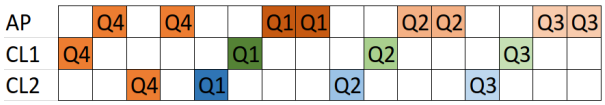


Fig. 6: Schedule organization. Time slot (TS) length from the set {256,512,1024} μs with respective cycle length from the set {4.096,8.192,16.384} ms.

case, the client TSs are followed immediately by a longer AP TS as the AP needs to respond to both clients. The background traffic is scheduled in queue 3. As it is UDP traffic it will be uni-directional from client to client and the client transmission opportunities are scheduled before the AP transmission opportunities. TS lengths are 256,512,1024 μs with respective cycle length of 4.096,8.192,16.384 ms, for test IDs 1,2 and 3, respectively (Table II).

Each test includes a set of measurements done under background traffic scheduled in dedicated and shared time slots with the F-safe traffic. The load of the background traffic is introduced based on the physical data rate used and the amount of time assigned during one cycle for the background traffic. This was chosen in order not to have buffer overflows due to a mismatch between the capacity of the physical layer to transmit the packets and the generated load in the application layer. As seen from Figure 6, the time portion during one cycle assigned to background traffic is 1/16, independent of the TS length. Since the data rate used was fixed at 26 Mbps, the data rate at the application layer was set no higher than 1.6 Mbps. The other measurement parameters are given in Table III.

B. Dedicated time slot (TS) scenario

In order to ensure the PROFIsafe communication between PLC devices, dedicated TSs are assigned for such communication. Similarly, the background traffic is assigned to dedicated TSs in order not to impact the PROFIsafe traffic. In Figure 7 the results for the end-to-end latency of all the three measurement cases are shown. For the PROFIsafe traffic we disable layer two re-transmission, as in case of a

TABLE III: Measurement parameters

Parameter	Value
Center frequency	5170 MHz
Bandwidth	20 MHz
Data rate	26 Mbps
Time Slot (TS) length	[256,512,1024] μs
Schedule cycle length	[4.096,8.192,16.384] ms
Measurement time	1 h
Background traffic	UDP with 2Mbps

TABLE IV: Achieved PFH for dedicated time slot (TS) scenario

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

TABLE V: Achieved PFH under shared time slot (TS) condition

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

*Not possible to reach any of the SILs

re-transmission the re-transmitted packet will be transmitted following a randomized back-off breaking the deterministic communication. As such the packet will either be received on the first try or will be declared lost.

Based on the determined schedule cycle length it is observed that in none of the cases the end-to-end latency passes the threshold of the watchdog time of the PROFIsafe, except in a single case in Figure 7c. For test cases 1 and 2, the end-to-end latency is bounded by the schedule cycle length, i.e. 99% of the end-to-end latency is lower than 16.5 ms, and lower than 8.5 ms, respectively (Figures 7d, 7e). In the third case (Figures 7c, 7f) due to short TSs imposed for the transmission, it might happen that the background traffic transmitted from the other neighbour queue (queue 3) can cross the boundary of its TS. In such a case, the PROFIsafe traffic will be delayed until the TS in the subsequent scheduling cycle, increasing thus the end-to-end latency. In this case, the end-to-end latency in 99% of the cases was smaller than 8.6 ms, twice the cycle length.

As explained, all the PROFIsafe packets are received within the time boundaries. In order to determine the supported SIL by our system, we compare the counters of the received F-messages in order to determine the packet loss as well as the percentage of time the system entered the safe state. The probability of failures per hour are shown in Table IV. W-TSN based on dedicated time-slots for fail-safe traffic can support a SIL of two for a high demand system, wile for a low demand system it can reach the highest SIL of 4.

C. Shared time slot (TS) scenario

In normal IEEE 802.11 operation there is no scheduling system to dedicate TSs to certain traffic flows. All the traffic flows and different nodes will share the channel by competing between each other based on CSMA-CA mechanism. Similarly, in case when the TSs are shared between different devices and different traffic flows, all of them will compete to access the channel.

In this scenario both PROFIsafe traffic and the background traffic share the same TSs, increasing thus the channel access competition. In Figure 8 the results of end-to-end latency and its cumulative distribution function (CDF) of all the three measurement cases are shown.

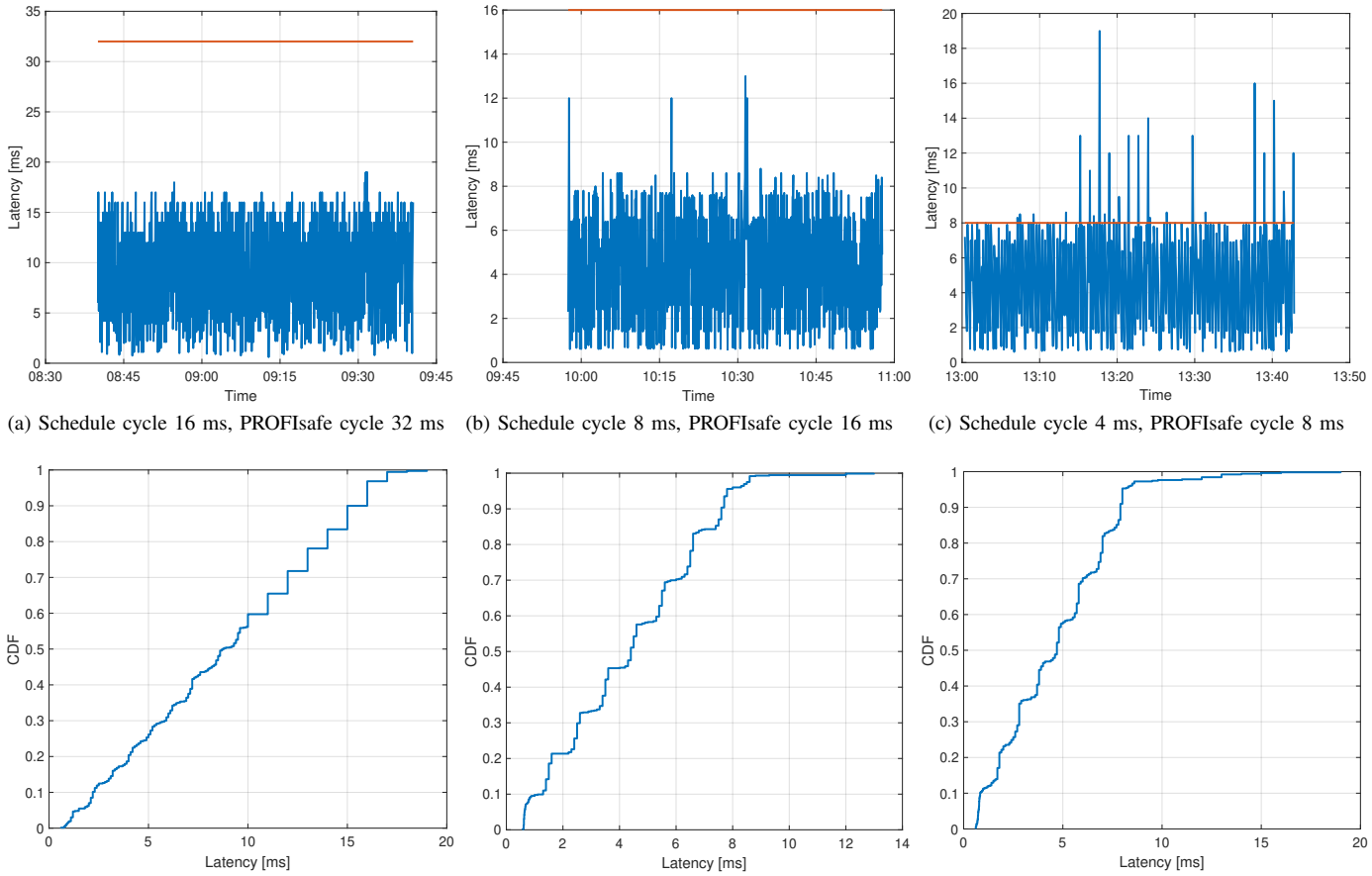
Normally the end to end latency should be based on the schedule cycle length. However, in many cases, due to competition between traffic flows the PROFIsafe link breaks, entering the safe state. This is also noticeable in the end-to-end latency graph (i.e. discontinuities in the graph in Figure 8a around time 13:15 and in Figure 8c between 14:17 to 14:20). Compared to test 1, in test 2 and 3 the TS length was shorter (512 and 256, respectively) increasing thus the traffic competition. In case of test 1, the system enters the safe state in $\sim 10^{-3}$, while the latency in 99% of the cases is smaller than 16.5 ms (Figure 8d). As such, for test ID 1 in this scenario a SIL of 3 can be provided for low demand systems, while no SIL guaranties can be provide for high demand systems. For other test measurements, none of the SILs can be provided neither for high demand systems nor for low demand systems. This is due to the long time that the system enters in safe state, that can go up to several seconds in the row. Table V summarize such findings.

VI. Conclusion and Future Work

In this paper we showed how PROFINET (as one of the widely used RTEs) is integrated with a wireless time-sensitive network (W-TSN) in order to provide certain safety integrity levels and deterministic communication latency for safety-related applications. Integration between W-TSN (based on openwifi software defined radio platform) and PROFINET is achieved by providing layer two bridging over wireless links. This is realized by encapsulating the layer two PROFINET packets in IEEE 802.1ah packets in order to support transparent transmission of such traffic over the air. Then the traffic classification is based on the VLAN ID of the outer Ethernet header of the IEEE 802.1ah header.

Such integration is validated with the ability to support safety-related application on top of a wireless time-sensitive network. A setup with one PLC and one end device connected to the wireless clients, that communicate between each other via an AP, was used for evaluating the integration. The PROFIsafe profile with three different cycle times (8, 16, 32 ms) was used with a watchdog time of twice the cycle time. Two test scenarios covered the dedicated TSs per safety-related traffic and shared TS between safety-related traffic and background traffic. It was shown that the safety integrity level of grade 4 could be achieved under the dedicated TS scenario. For shared TS scenario the SIL of grade 3 was achieved only for the case where the cycle time was set at 32 ms. For other cases the integrity level could not be ensured by the communication system.

Currently part of end-to-end latency is a result of mismatch between the traffic generation time and the applied schedule. Future work on alignment of traffic generation time with the applied schedule via an application network interface would improve the latency. Using only time access for scheduling has its scalability limits. With OFDMA as inherit part of the



(a) Schedule cycle 16 ms, PROFIsafe cycle 32 ms (b) Schedule cycle 8 ms, PROFIsafe cycle 16 ms (c) Schedule cycle 4 ms, PROFIsafe cycle 8 ms

(d) End-to-end latency CDF for schedule cycle of 16ms (e) End-to-end latency CDF for schedule cycle of 8ms (f) End-to-end latency CDF for schedule cycle of 4ms

Fig. 7: End-to-end latency and its CDF for each measurement case using dedicated time slot (TS).

latest WiFi standard (802.11ax) scalability can be improved by employing scheduling in frequency as well.

ACKNOWLEDGMENT

This research was partially funded by the Flemish FWO SBO S003921N VERI-END.com (Verifiable and elastic end-to-end communication infrastructures for private professional environments) project, the Flemish Government under the "Onderzoeksprogramma Artificiële Intelligentie (AI) Vlaanderen" program, and from the FWO-Flanders, under grant agreement G055619N.

REFERENCES

[1] S. Vitturi, C. Zunino, and T. Sauter, "Industrial communication systems and their future challenges: Next-generation ethernet, iiot, and 5g," *Proceedings of the IEEE*, vol. 107, no. 6, pp. 944–961, 2019.

[2] *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.

[3] *IEEE Standard 802.1Q-2018, "IEEE Standard for Local and metropolitan area networks: Bridges and Bridged Networks"*, IEEE Standards Association, July 2018.

[4] *IEEE 802.1Qbu-2016 "IEEE Standard for Local and metropolitan area networks, Bridges and Bridged Networks, Amendment 26: Frame Preemption"*, IEEE Standards Association, August 2016.

[5] *IEEE 802.1CB-2017, "IEEE Standard for Local and metropolitan area networks-Frame Replication and Elimination for Reliability"*, IEEE Standards Association, October 2018.

[6] *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.

[7] *Integration of 5G with Time-Sensitive Networking for Industrial Communications*, 5G-ACIA, White Paper, January 2021.

[8] J. Haxhibeqiri, X. Jiao, E. Municio, J. M. Marquez-Barja, I. Moerman, and J. Hoebeke, "Bringing time-sensitive networking to wireless professional private networks," *Wireless Personal Communications*, vol. 121, no. 2, pp. 1255–1271, 2021.

[9] *Functional safety: Safety related systems*, IEC 61508, 2010.

[10] *PROFIsafe System Description*, PI, June 2016.

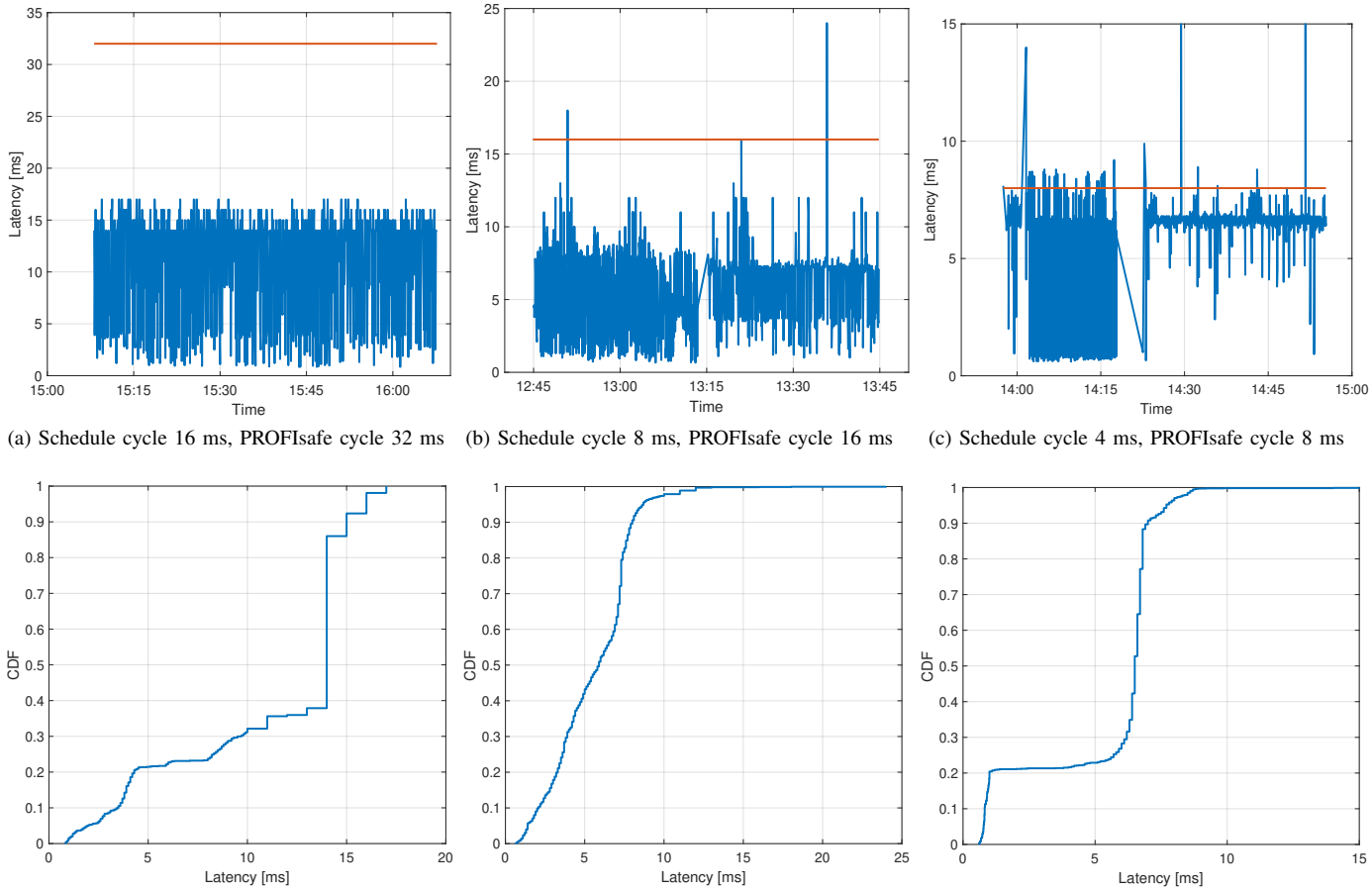
[11] *openSAFETY Safety Profile Specification*, Ethernet POWERLINK Standardisation Group (EPSG), 2017.

[12] *OPC 10000-15 Unified Architecture Part 15 Safety Scope*, 2019.

[13] S. Gent, P. G. Peón, T. Frühwirth, and D. Etz, "Hosting functional safety applications in factory networks through time-sensitive networking," in *2020 25th IEEE International Conference on Emerging Technologies and Factory Automation (ETFA)*, vol. 1. IEEE, 2020, pp. 230–237.

[14] A. Morato, S. Vitturi, F. Tramarin, and A. Cenedese, "Assessment of different opc ua implementations for industrial iot-based measurement applications," *IEEE Transactions on Instrumentation and Measurement*, vol. 70, pp. 1–11, 2020.

[15] J. Hoffmann, D. Kuschnerus, T. Jones, and M. Hubner, "Towards a safety and energy aware protocol for wireless communication," in



(a) Schedule cycle 16 ms, PROFIsafe cycle 32 ms (b) Schedule cycle 8 ms, PROFIsafe cycle 16 ms (c) Schedule cycle 4 ms, PROFIsafe cycle 8 ms

(d) End-to-end latency CDF for schedule cycle of 16ms (e) End-to-end latency CDF for schedule cycle of 8ms (f) End-to-end latency CDF for schedule cycle of 4ms

Fig. 8: End-to-end latency and its CDF for each measurement case using shared time slot (TS).

2018 13th International Symposium on Reconfigurable Communication-centric Systems-on-Chip (ReCoSoC). IEEE, 2018, pp. 1–6.

[16] A. Hadziaganović, M. K. Atiq, T. Blazek, H.-P. Bernhard, and A. Springer, "The performance of opensafety protocol via ieee 802.11 wireless communication," in *2021 26th IEEE International Conference on Emerging Technologies and Factory Automation (ETFA)*. IEEE, 2021, pp. 1–8.

[17] G. Peserico, T. Fedullo, A. Morato, F. Tramarin, and S. Vitturi, "Wi-fi based functional safety: an assessment of the fail safe over ethercat (fsoe) protocol," in *2021 26th IEEE International Conference on Emerging Technologies and Factory Automation (ETFA)*. IEEE, 2021, pp. 1–8.

[18] 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.

[19] J. Åkerberg, M. Gidlund, F. Reichenbach, and M. Björkman, "Measurements on an industrial wireless hart network supporting profisafe: A case study," in *ETFA2011*. IEEE, 2011, pp. 1–8.

[20] 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, 2021.

[21] P. Sanz, O. Seijo, M. C. Llorente, J. Montalban, P. Angueira, and I. Val, "On the feasibility of wireless communications for safety applications in industry," *IEEE Transactions on Industrial Informatics*, 2022.

[22] P. Sanz, I. Val, A. Urkidi, P. Angueira, and J. Montalban, "Safety related systems design methodology for wireless time-varying channels," in *2021 17th IEEE International Conference on Factory Communication Systems (WFCS)*. IEEE, 2021, pp. 123–130.

[23] 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.

[24] *PROFINET - The Solution Platform for Process Automation*, PI, White Paper, June 2018.

[25] *PROFINET IO Conformance Classes*, PI, March 2011.

[26] *PROFINET System Description*, PI, November 2018.

[27] F. Redmill, "Understanding the use, misuse and abuse of safety integrity levels," in *Proceedings of the Eighth Safety-critical Systems Symposium*. Citeseer, 2000, pp. 8–10.

[28] X. Jiao, W. Liu, and M. Mehari. (2019) open-source ieee802.11/wi-fi baseband chip/fpga design. [Online]. Available: https://github.com/open-sdr/openwifi

[29] J. Haxhibeqiri, I. Moerman, and J. Hoebeke, "Low overhead, fine-grained end-to-end monitoring of wireless networks using in-band telemetry," in *2019 15th international conference on network and service management (CNSM)*. IEEE, 2019, pp. 1–5.

[30] J. Haxhibeqiri, P. H. Isolani, J. M. Marquez-Barja, I. Moerman, and J. Hoebeke, "In-band network monitoring technique to support sdn-based wireless networks," *IEEE Transactions on Network and Service Management*, vol. 18, no. 1, pp. 627–641, 2020.

[31] R. C. Sofia, "A survey of advanced ethernet forwarding approaches," *IEEE Communications surveys & tutorials*, vol. 11, no. 1, pp. 92–115, 2009.