The Model of Functional Safety Protocol

Subjects: Automation & Control Systems

Contributor: Alberto Morato, Stefano Vitturi, Federico Tramarin, Claudio Zunino, Manuel Cheminod

Industry 4.0 has significantly improved the industrial manufacturing scenario in recent years. The Industrial Internet of Things (IIoT) enables the creation of globally interconnected smart factories, where constituent elements seamlessly exchange information. Industry 5.0 has further complemented these achievements, as it focuses on a human-centric approach where humans become part of this network of things, leading to a robust human–machine interaction. In this distributed, dynamic, and highly interconnected environment, functional safety is essential for adequately protecting people and machinery. The increasing availability of wireless networks makes it possible to implement distributed and flexible functional safety systems.

Keywords: functional safety networks ; Industry 4.0 ; Industrial Internet of Things

1. Introduction

Factory automation has undergone a profound revolution thanks to the introduction of the Industrial Internet of Things (IIoT) concept. In this context, information and communication technologies (ICT) are ever more used to create smart factory ecosystems comprising distributed networks of objects capable of seamlessly interacting. Since the introduction of such technologies, the push for innovation has continued to grow, as witnessed by the industrial revolution, referred to as Industry 4.0 [1], which has been recently followed by Industry 5.0 [2][3].

Basically, Industry 4.0 is a concept introduced about a decade ago which relies on the intelligent networking among machines, controllers, sensors and actuators, and processes in general, to implement digitized production systems [4]. This technology-driven paradigm enhances the manufacturing capabilities, improving production efficiency and flexibility, while ensuring energy efficiency, rational use of resources, and environmental sustainability.

Industry 5.0 is a value-driven paradigm that is designed to complement and enhance the aforementioned features. Its origin can be traced back to pioneering works, such as [5], and has since been adopted by the European Commission [6]. Industry 5.0 focuses on three main concepts, namely, the human-centric approach, sustainability, and resilience [7]. Particularly, the human-centric approach involves the direct participation of humans in the production processes to facilitate robust, profound, and fruitful cooperation with machines. In this respect, a common example involves the interaction between humans and collaborative robots (CoBots).

The innovative context described above poses further requirements for the communication systems deployed in the industrial scenario [8]. Two fundamental issues need to be addressed: (i) the pervasive use of industrial wireless networks and (ii) the implementation of robust and effective distributed functional safety systems. In this regard, as collaboration between individuals and machines is essential, ensuring a high level of protection is crucial for both operators and the surrounding environment. Therefore, functional safety systems are of the utmost importance [9]. Thus, in the Industry 4.0–5.0 scenarios, it is necessary to implement robust, reliable, and safe communication protocols over wireless networks. The benefits of this implementation are manifold. Notably, eliminating cabling results in significant cost-savings and greatly enhances the flexibility and scalability of networks.

In this direction, the IEC 61784–3 International Standard [10] defined some effective protocols such as Fail Safe over EtherCAT (FSoE), ProfiSAFE, and OpenSafety that, however, were primarily conceived to work with wired communication systems. Nevertheless, thanks to the “Black Channel Approach” introduced by IEC 61784–3, they can be implemented on wireless networks as well. Unfortunately, the introduction of wireless systems may negatively impact the behavior of the plants that use the functional safety networks, due to the implicit uncertainty of the communication medium. As an example, impairments like a delay in delivery a packet or, worse, a lost packet that occur during the operation of a functional safety network may trigger the intervention of the safety stop function, with the consequent shutdown of the plant.

In this scenario, however, the opportunities offered by Time-Sensitive Networking (TSN) [11][12] may represent a valuable and significant step forward. TSN is a family of standards originally conceived for Ethernet networks that has recently started to be considered for industrial wireless communication systems as well. It includes protocols for distributed device synchronization, traffic shaping and scheduling, and network redundancy (to mention some) that can be profitably used to dramatically improve communication performance, particularly in terms of timeliness and reliability [13].

To the best of the authors' knowledge, TSN has never been considered to implement functional safety networks, whether wired or wireless. Based on this consideration, this research addresses the adoption of TSN for functional safety protocols implemented over wireless networks, specifically Wi-Fi. In light of the current state of the art, and particularly with reference to the contribution described in [14], this research presents some novel elements, as follows:

- A reference functional safety protocol is introduced to make the analysis more general;
- Various Wi-Fi modulation and coding schemes (MCSs) are used;
- Different channel models are taken into account;
- Two TSN protocols, namely, IEEE 802.1AS and IEEE 802.1Qbv, over Wi-Fi are employed.

The analysis is based on the specific case study of an automated warehouse in which robots and humans cooperate to transfer goods from/to different areas of the plant. It is carried out through numerical simulations and focuses on the behavior of two meaningful performance indexes, namely, the safety function response time (*SFRT*) and the percentage of failed pollings (*PFP*), which will be formally defined in the following. The final goal is to assess whether TSN can bring significant performance improvements, as well as to investigate the most suitable configurations of Wi-Fi and TSN in this challenging field of application.

2. Reference Functional Safety Protocol

The proposed reference protocol is based on a master/slave technique that resembles those adopted by the protocols of the IEC 61784-3. Basically, a master device cyclically polls a set of slave devices to exchange safety PDUs (SPDUs), which contain safety-related data. In detail, such a polling operation can be either *continuous* or *slotted*. In the continuous polling, the master starts querying the first slave and, upon completion of the polling operation, sequentially moves to the following ones. When the last slave has been polled, the master returns immediately to the first one and starts a new cycle.

In the slotted polling, slots of fixed duration are assigned to master and slaves. The polling cycle is determined by the sequence of the slots. The master starts the cycle by sending the SPDUs to the slaves in its slot. Subsequently, each slave is granted to transmit its SFPU in the slot assigned to it. When the slot of the last slave has expired, a new cycle is started with the slot of the master. Clearly, TSN features are particularly helpful to implement such a technique since they allow (i) strict synchronization of the nodes and (ii) assigning of the time slots to the nodes.

In agreement with IEC 61784-3, the reference functional safety protocol implements some countermeasures against communication errors. They are listed in **Table 1** and briefly described in the following. The safety CRC is an additional CRC, with respect to that of the underlying communication system, calculated only on the safety PDU. The PDU numbering is a technique that assigns a sequential number to each safety PDU exchanged between master and slave. It is calculated by the protocol and inserted on a specific field of the safety PDUs. The watchdog is a procedure that allows the checking of whether or not a device is alive. Finally, the slave authentication is a further safety technique that allows the master to constantly know the list of slaves authorized to exchange safety information.

Table 1. Countermeasures implemented by the functional safety reference protocol.

Countermeasure	Description
Safety cyclic redundancy check (CRC)	**Additional safety-related CRC**
PDU numbering	**Numbering of safety PDUs exchanged between master and slaves**
Watchdog	**Time-out associated with each device**
Slave authentication	**Unique address assigned to each slave and stored by the master**

The countermeasures described so far are able to detect some specific communication errors, as listed in **Table 2** (the detailed description of the communication errors can be found in the IEC 61784-3 International Standard). When one of such errors occurs, if it is detected by the master, this device issues a safe state transition request to all the slaves and then enters the safe state by itself. Conversely, if the error is detected by a slave, this device sends the request to the master, which in turn dispatches it to all the other slaves and then enters the safe state by itself.

Table 2. Error detection by the functional safety reference protocol.

Error	Countermeasures
Corruption	**CRC and watchdog**
Repetition	**PDU numbering**
Incorrect sequence	**PDU numbering**
Loss	**PDU numbering and watchdog**
Delay	**Watchdog**
Insertion	**Slave authentication**
Masquerade	**CRC and slave authentication**
Addressing	**Slave authentication**

References

1. Rikalovic, A.; Suzic, N.; Bajic, B.; Piuri, V. Industry 4.0 Implementation Challenges and Opportunities: A Technological Perspective. IEEE Syst. J. 2022, 16, 2797–2810.
2. Xian, W.; Yu, K.; Han, F.; Fang, L.; He, D.; Han, Q.L. Advanced Manufacturing in Industry 5.0: A Survey of Key Enabling Technologies and Future Trends. IEEE Trans. Ind. Inform. 2023; 1–15.
3. Nahavandi, S. Industry 5.0—A human-centric solution. Sustainability 2019, 11, 4371.
4. Platform Industrie 4.0. Available online: https://www.plattform-i40.de (accessed on 28 August 2023).
5. Longo, F.; Padovano, A.; Umbrello, S. Value-Oriented and Ethical Technology Engineering in Industry 5.0: A Human-Centric Perspective for the Design of the Factory of the Future. Appl. Sci. 2020, 10, 4182.
6. Breque, M.; De Nul, L.; Petridis, A. Industry 5.0—Towards a Sustainable, Human-Centric and Resilient European Industry; Publications Office of the European Union: Brussels, Belgium, 2021.
7. Xu, X.; Lu, Y.; Vogel-Heuser, B.; Wang, L. Industry 4.0 and Industry 5.0—Inception, conception and perception. J. Manuf. Syst. 2021, 61, 530–535.
8. Vitturi, S.; Zunino, C.; Sauter, T. Industrial Communication Systems and Their Future Challenges: Next-Generation Ethernet, IIoT, and 5G. Proc. IEEE 2019, 107, 944–961.
9. Bicaku, A.; Schmittner, C.; Tauber, M.; Delsing, J. Monitoring industry 4.0 applications for security and safety standard compliance. In Proceedings of the 2018 IEEE Industrial Cyber-Physical Systems (ICPS), St. Petersburg, Russia, 15–18 May 2018; pp. 749–754.
10. IEC 61784-3; Industrial Communication Networks–Profiles—Part 3: Functional Safety Fieldbuses—General Rules and Profile Definitions. Technical Report; International Electrotechnical Commission: Geneva, Switzerland, 2021.
11. Lo Bello, L.; Steiner, W. A Perspective on IEEE Time-Sensitive Networking for Industrial Communication and Automation Systems. Proc. IEEE 2019, 107, 1094–1120.
12. Fedullo, T.; Morato, A.; Tramarin, F.; Rovati, L.; Vitturi, S. A Comprehensive Review on Time Sensitive Networks with a Special Focus on Its Applicability to Industrial Smart and Distributed Measurement Systems. Sensors 2022, 22, 1638.
13. Cavalcanti, D.; Perez-Ramirez, J.; Rashid, M.M.; Fang, J.; Galeev, M.; Stanton, K.B. Extending Accurate Time Distribution and Timeliness Capabilities Over the Air to Enable Future Wireless Industrial Automation Systems. Proc. IEEE 2019, 107, 1132–1152.
14. Peserico, G.; Morato, A.; Tramarin, F.; Vitturi, S. Functional Safety Networks and Protocols in the Industrial Internet of Things Era. Sensors 2021, 21, 6073.