International Journal of Advances in Engineering and Management (IJAEM)
Volume 4, Issue 8 Aug. 2022, pp: 1600-1602 www.ijaem.net ISSN: 2395-5252

Functional Safety and Industrial Communication Associated For the Smart Factory

Sathishkumar. S[1], Vimal. S[2], Thirukkumaran. B[3]

Submitted: 15-08-2022 Revised: 27-08-2022 Accepted: 30-08-2022

ABSTRACT: New and challenging applications have emerged such as hyper automation, which refers to the combination of machine vision, robotics, communication, and learning, with the explicit involvement of humans. Wireless communications are today fundamental to open up to new categories of autonomous devices that can actively collaborate with human personnel in the production process. This challenging scenario has important implications for safety. Indeed, a reliable coordination among sensors, actuators and computing systems is required to provide satisfactory levels of safety, especially in the case of innovative processes and technologies, such as mobile and collaborative robotics. In this paper, we address the challenges concerned with functional safety networks and protocols in Industrial Internet of Things ecosystems. We first introduce the design characteristics of functional safety networks and discuss the adoption of safety protocols over wireless networks. Then, we specifically address one of such protocols, namely Fail Safety over EtherCAT (FSoE), and provide the results of an extensive experimental session carried out exploiting a prototype system, implemented using commercial devices based on a Wi-Fi network. Finally, the outcomes of the experiments are used as a basis for a discussion about future trends of functional safety in the Industrial Internet of Things.

Keywords: FSoE, IIoT, FSN, CAGR.

I. INTRODUCTION:

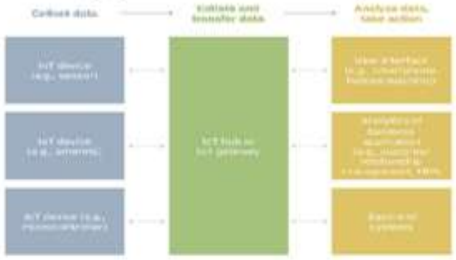
The smart manufacturing practices used by a smart factory are enabled by a variety of technologies including artificial intelligence (AI), big data analytics, cloud computing, and the industrial Internet of Things (IoT). An IoT sensor was attached to each equipment to measure data from the equipment, and this data is transmitted to the connected smart gateway. The smart gateway collects measurement data from multiple equipment and delivers it to the real- time monitoring server.Industrial automation systems have made extensive use of communication networks to connect their components deployed over (possibly large) distributed plant areas. This trend started roughly at the beginning of the 1990s and progressively enforced over the years, thanks to the improvements achieved by such networks in terms of performance indicators, such as timeliness, reliability, dependability, and scalability. Where a pervasive communication infrastructure allows connection of cloud systems, controllers, industrial equipment, sensors, and actuators to dramatically improve. The performance of manufacturing systems in terms of product quality, production efficiency, safety, and security. FSNs are expected to be ever more deployed and integrated in the factory communication infrastructures, so that plant safety data and information will become part of IIoT ecosystems and, as such, they will be accessed and elaborated using the new services and tools made available in such a context. FSNs are required to ensure the transmission of safety-related information among nodes with extremely low error probability and bounded reaction times. The platform includes the different technologies used in functional safety: safe relays, safe programmable logic controllers that can be programmed with the specific software of each manufacturer, various safe sensors, and actuators. For building a safety application system with a safety PLC or a safety relay and eventually an associated safety network, users shall consider to not only a safety programming but also technology, configuration, installation, operation, and maintenance [1]. The use of standard industrial programmable controllers in safety critical applications is considered. The use of independent machines and asynchronous processing are discussed. The role of serial communications in each configuration is explained and the benefits considered. Various issues of quality assurance and failure rate analysis are addressed [2]. In this paper sensorized glove for industrial safety based on Near-Field Communication (NFC). The demonstration is a proof-of-concept implementation that shows how an NFC-enabled sensor installed in the glove of a worker can be exploited to monitor worker's action and report dangerous situations in advance to prevent accidents and injuries [3]. It includes 5 function modules: risk identification module, accident simulation module, emergency drill module and ergonomic evaluation module. In addition, this paper conducts a series of experiments to verify the feasibility and validity of using electrocardiograph (ECG) and skin temperature (SKT) data to reflect the training effect and quality in the ergonomics evaluation. The results show that the changes of ECG and SKT can reflect the cognitive load of trainees during training, and they can be used to evaluate the safety training quality of trainees [4]. This paper is to develop a framework to use Assurance Case methodology for Industrial IoT systems (IIoT)[5].

II. SOFTWARE DESIGN

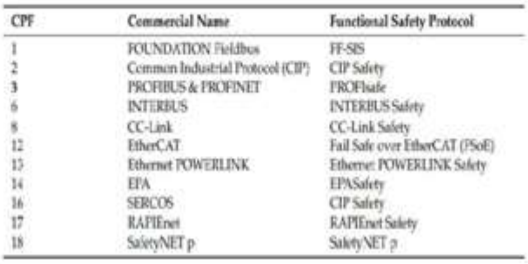
- **Internet of Thinks:** An IoT ecosystem consists of web-enabled smart devices that use embedded processors, sensors and communication hardware to collect, send and act on data they acquire from their environments. IoT devices share the sensor data they collect by connecting to an IoT gateway or other edge device where data is either sent to the cloud to be analyzed or analyzed locally. Sometimes, these devices communicate with other related devices and act on the information they get from one another. The devices do most of the work without human intervention, although people can interact with the devices for instance, to set them up, give them instructions or access the data.
-
- **Benefits of IoT:**

The internet of things offers several benefits to organizations, enabling them to: monitor their overall business processes, improve the customer experience, save time and money, enhance employee productivity, integrate and adapt business models.

III. PROPOSED SYSTEM

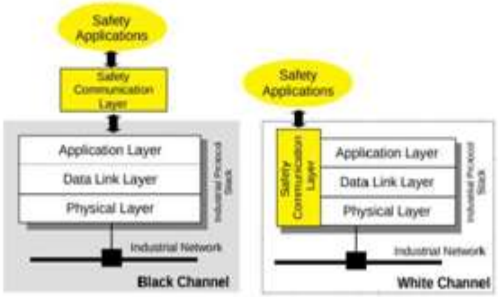


The most popular Functional Safety Networks are defined by the IEC International Standard with specific reference to the Communication Profile Families (CPFs) introduced by the fieldbus standardization framework. Table lists the CPFs for which functional safety protocols have been defined along with their commercial names.



CPF	Commercial Name	Functional Safety Protocol
1	FOUNDATION Fieldbus	FF-SIS
2	Common Industrial Protocol (CIP)	CIP Safety
3	PROFIBUS & PROFINET	PROFIsafe
6	INTERBUS	INTERBUS Safety
8	CC-Link	CC-Link Safety
12	EtherCAT	Fail Safe over EtherCAT (FSoE)
13	Ethernet POWERLINK	Ethernet POWERLINK Safety
14	EPA	EPASafety
16	SERCOS	CIP Safety
17	RAPIEnet	RAPIEnet Safety
18	SafetyNET p	SafetyNET p

OPC UA Safety has been recently defined in agreement with the guidelines of IEC, even though it is not included in such standard. CAN Open Safety is a popular European Standard, designed with a different approach, referred to as white channel from that of IEC. Below Figure, right side, assumes that the functional safety protocol is aware of the underlying communication system and makes use of its services and protocols, in all layers, to implement the safety functions. Regardless of the channel approach, functional safety protocols must deal with several types of communication errors. The most typical ones, as specified by IEC, are corruption, loss, and delay of the transmitted safety messages. To tackle such impairments, the protocols adopt some counter measure; the most effective being the use of enforced CRC, message numbering and time stamping. The complete list of errors and countermeasures can be found in the standard documents. When a functional safety network is used. It contributes to the risk analysis that has to determine the overall Safety Integrated Level (SIL).



This reflects on the performance figures that FSNs must provide, in terms of residual error probability per hour (REP). Clearly, the higher the SIL, the lower the REP. In general, REP is strictly related to the communication behavior and depends on the bit error rate of the underlying channel, The number of safety messages transmitted per hour, The countermeasures against errors adopted by the functional safety protocols.

- **Wireless Networks**: The introduction of the IIoT paradigm relies on a pervasive connectivity that can be ensured by the introduction of wireless networks at all the automation levels. Hence, the black channel approach discussed so far represents an ideal approach for porting functional safety protocols over those industrial communication systems not having a specific safety extension. Wireless networks could be adopted, paving the way to the introduction and integration of wireless functional safety networks in IIoT ecosystems.

- **Android Ubidots:** App developers can access the Android platform to create an account and data source. The account created on Android can then be connected to Ubidots. This will enable developers to push the app on the smartphones.
- **Thingworx:** The renowned avenue provides app developers with advanced and powerful tools to market their products. Industrialists can go for Gartner Magic Quadrant for assistance in market research and trends. Another top platform is the Forester Wave Report for viable IoT Strategies. That’s not all industrial companies often consult Colfax Company for the best IoT strategies and plans.

IV. CONCLUSION

Functional safety networks are expected to be increasingly used in IIoT ecosystems, particularly over wireless media. In this respect, in this paper, we addressed safety protocols, focusing on those described by the IEC 61784–3 International Standard, and investigated their suitability for IIoT applications. First, the black channel principle can be successfully exploited to bring safety protocols over communication media different from those for which they were natively designed. Second, although the black channel approach in principle ensures feasibility, it is clear it might introduce limitations, particularly with respect to performance. This aspect derives from the undeniable fact that each protocol has been conceived for a specific network. As an example, referring to wired systems, functional safety protocols designed for Ethernet networks can be difficultly implemented on communication systems that use short payloads such as Controller Area Network. Even more evidently, referring to OPC UA Safety, SPDUs may reach large sizes, thus, they need adequate MAC and physical layers to be transferred. Possible performance limitations have been clearly evidenced by the experimental assessment of FSoE over Wi-Fi provided in Section 4. Indeed, as we have seen, the behavior of FSoE is strictly related to the protocol stack included in the black channel. Nevertheless, it has also been shown that there is large room for improvement and future developments.

REFERENCES

[1]. Cao Wen-Jing-“Requirements Analysis for Vehicle-to-Vehicle Safety Communication” IJASEIT-11(5):1787, DOI: 10.18517 / ijaseit. 11.5.13067 - November 2020.

[2]. E. Sun, J. Li, Z. Li, D. Gao, Y. Chen and M. Wang, "Virtual Training and Ergonomics Evaluation System for Industrial Production Safety Based on Visible Light Communication," 2019 IEEE 19th International Conference on Communication Technology (ICCT), 2019, pp. 695-700, doi: 10.1109/ICCT46805.2019.8947232.

[3]. J. -H. Kim, K. -S. Lee and Y. -G. Kim, "Development of IoT-based Safety Management Method through an Analysis of Structural Characteristics and Risk Factors for Industrial Valves," 2019 International Conference on Machine Learning and Data Engineering (iCMLDE), 2019, pp. 30-35, doi: 10.1109/iCMLDE49015.2019.00017.

[4]. Shaikh Rehan-“Industrial and Home Automation, Control, Safety and Security System using Bolt IoT Platform”- October 2020.

[5]. T. K. Tran-“Functional Safety and Industrial Communication Associated for the Smart Factory”- July 2019.

[6]. Michael Frey; Cenk Gündoğan; Peter Kietzmann; Martine Lenders; Hauke Petersen-“Security for the Industrial IoT: The Case for Information-Centric Networking” IEEE World Forum on Internet of Things (WF-IoT)- July 2019.

[7]. Fan Wu, Taiyang Wu, Mehmet Rasit Yuce-“Design and Implementation of a Wearable Sensor Network System for IoT-Connected Safety and Health Applications” 10.1109/WF-IoT.2019.8767280- July 2019.

[8]. Vladimir Sklyar-“Challenges in assurance case application for industrial IoT” DOI: 10.1109 / WF-IoT.2019.8767280, November 2017.