SoK: Investigation of Security and Functional Safety in Industrial IoT

Emrah Tomur, Utku Gülen, Elif U. Soykan, Mehmet Akif Ersoy, Ferhat Karakoç, Leyli Karaçay and Pınar Çomak
Ericsson Research
{emrah.tomur, utku.gulen, elif.ustundag.soykan, mehmet.akif.ersoy, ferhat.karakoc, leyli.karacay, pinar.comak }@ericsson.com

2021 IEEE International Conference on Cyber Security and Resilience (CSR) | 978-1-6654-0285-9/21/$31.00 ©2021 IEEE | DOI: 10.1109/CSR51186.2021.9527921

***Abstract*—There has been an increasing popularity of industrial usage of Internet of Things (IoT) technologies in parallel to advancements in connectivity and automation. Security vulnerabilities in industrial systems, which are considered less likely to be exploited in conventional closed settings, have now started to be a major concern with Industrial IoT. One of the critical components of any industrial control system turning into a target for attackers is functional safety. This vital function is not originally designed to provide protection against malicious intentional parties but only accidents and errors. In this paper, we explore a generic IoT-based smart manufacturing use-case from a combined perspective of security and functional safety, which are indeed tightly correlated. Our main contribution is the presentation of a taxonomy of threats targeting directly the critical safety function in industrial IoT applications. Besides, based on this taxonomy, we identified particular attack scenarios that might have severe impact on physical assets like manufacturing equipment, even human life and cyber-assets like availability of Industrial IoT application. Finally, we recommend some solutions to mitigate such attacks based mainly on industry standards and advanced security features of mobile communication technologies.**

I. Introduction

Modern industrial systems utilize advanced process control and automation systems, which are usually named as Industrial Control Systems (ICS) or Operational Technology (OT). ICS are used in various sectors ranging from manufacturing to energy distribution. A typical ICS comprises of several control processes, human interfaces, and remote diagnostics functionality that are performed with various different IoT components such as controllers, actuators, and sensors and; software components like control programs and safety programs. Safety requirements are one of the key factors when designing an Industrial IoT (IIoT) system and that is why dedicated elements named safety related systems (SRS) or safety instrumented systems (SIS) are used to assure safety. SRS/SIS can be regarded as another control system to independently monitor the automation or process control function with regards to safety. These systems are responsible for maintaining the safety by continuously monitoring safety-related status via sensors and take necessary actions via actuators to bring the system into a safe state if any dangerous situation is detected. More detailed information about safety and safety function is presented in the following subsection.

978-1-6654-0285-9/21/$31.00 ©2021 IEEE

A. Safety and functional safety

Safety is generally defined as the state of being free from unacceptable risk, which causes direct or indirect harm to human health, environment or property [1]. A related concept, functional safety, is a function usually implemented in software to maintain the safe state in an IIoT system or subsystem. It is concerned with correct operation of the safety related system with the objective of keeping the risk of harm at an acceptable level. Functional safety provides an assurance on the control or communication system to accomplish its safety related task when it is required to do so [2]. Examples of safety function are a robot reducing its operating speed when a human is nearby or an automated sprinkler turning on when a potential fire is detected.

Assuring integrity in functional safety communication is very important since safety controller and safety devices continuously interact to detect dangerous situations and take preventative actions in a timely fashion. This is why there are particular protocols operating at application level to eliminate the effect of channel errors caused by noise, interference, equipment and other faults. These protocols provide integrity check mechanisms to handle unintentional modifications in functional safety communication but they are not designed to be effective against malicious intervening of safety related messages and programs.

B. Security, safety and functional safety

Security and safety are interrelated concepts having similarities and differences. Both of them have the main objective of preventing harm from unwanted incidents, and therefore they are related to risk and require risk management. Main source of risk in safety comes from passive resources such as randomness in nature, accidents, human faults or system errors. Security risks, however, are originated from deliberate malicious adversaries acting as creative and determined agents, which could be humans or AI-based software. Impacts of incidents in a lack of proper safety measures are on the physical world, while the exploited security vulnerabilities can affect both physical and cyber world.

Functional safety systems play the critical role of protecting invaluable assets in the physical world including human health and lives, environment, and equipment from hazardous effects of malfunctioning OT systems. Similarly, IT security

aims to provide protection for information and all other IT assets. Until recently, security systems and functional safety systems had mostly been split and operated on their own cyber or physical domains. Yet, these two systems have recently been intertwined as seen in Figure 1 due to proliferation of Industrial IoT systems connecting to enterprise IT networks and even Internet. An attack initiated from the IT network by malicious adversaries can put harm on the OT systems and damage can be increased by directly targeting safety function in the OT network. Triton malware is an example of such an attack which targeted safety instrumented system of an oil and gas petrochemical facility in 2017 [3]. Although attackers were not able to disable the safety function that can result in lost lives of people, they were successful at putting the systems into emergency stop state harming availability. Occurrence of such attacks targeting functional safety for industries will increase unless proper security protection is in place to handle malicious actions by threat agents aiming to exploit security vulnerabilities in these systems as mentioned in literature [4].

We can mention two main threat sources that can adversely affect security of a functional safety system. First one stems from the vulnerabilities of safety system itself. In the design phase, improperly constructed decision flow can trigger unwanted actions resulting from human manipulations with the adversarial intention in the operating phase. Such vulnerabilities can be named as misuses of the safety system that mostly relate to behaviours like disregarding the intended use of systems and intentions to overcome safety precautions. The second one stems from insufficient security considerations in safety communication protocol or software, which expose vulnerabilities that attackers can exploit to put harm by preventing correct functioning of the safety related system. In our study, we focus on the latter one and make our investigation of possible attack scenarios on smart manufacturing domain introduced by security weaknesses and explain how they can impact the safety system. We present a threat taxonomy for the first time in literature to cover security threats targeting directly safety function. This taxonomy also includes vulnerabilities which may arise from insecure supply chain of the devices and software vulnerabilities in the safety control system. We also present several attacks against functional safety in IoT-based smart manufacturing environments.

II. Security perspective on functional safety

Until recently, most of the industry standards have regarded security [5] and safety [1] in industrial automation as concepts to handle separately. Objectives in safety-oriented standards mostly consider protecting people from any harm caused by OT environment while security-oriented standards focus on protection of the IT system against attacks coming from malicious actors in the IT domain. However, as we already mentioned, while it might be reasonable in the past to take functional safety and security as distinct topics, this approach is not valid anymore in the IoT and Industry 4.0 era since mutual dependencies are increasing and attack surfaces are widening. Recent studies and standardization activities depict

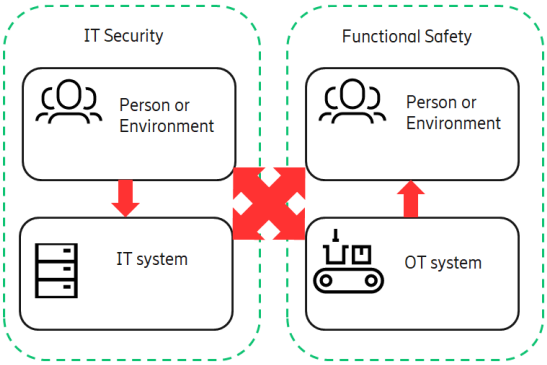

Fig. 1. Safety - Security relationship

the need for co-handling of these concepts as [6] presents a consolidated framework for both safety and security. Before we explain how such studies can provide support for securing functional safety, we first describe a generic smart manufacturing use case on which we will investigate potential vulnerabilities and threats in Industrial IoT.

A. Smart manufacturing Industrial IoT use case

In a typical industrial IoT setting for smart manufacturing, OT network is isolated from the enterprise IT network and from Internet with firewalls through a demilitarized zone (DMZ) to allow controlled flow of information between enterprise and industrial network. Safety related systems are located in the OT network together with the automation control system that is used to control IoT devices so-called Equipment Under Control (EUC) such as a robot arm or AMR (Autonomus Mobile Robot). EUC is controlled by a software named Control Program running on a hardware device, Controller. Safety-related actions of EUC is controlled by another software named Safety Program. Safety Program runs on a dedicated hardware named Safety Controller. Besides these, safety system in a manufacturing scenario includes two other main components: (i) Safety Sensor(s), either attached to EUC or separate and (ii) Safety Actuator(s), either attached to EUC or separate. An Engineering Workstation is used to make configurations and updates on parameters or code of the Safety Program and Control Program. Setting for a generic smart manufacturing safety function is depicted in Figure 2.

Safety related systems in smart manufacturing detect any safety-related incidents through safety sensors and take preventative counter actions through safety actuators before any hazardous event occurs. Possible safety actions might be performing an emergency full stop, slowing-down the speed of rotating components or any other fail-safe mode action previously defined in Safety Program code. In order to detect dangerous events and take timely action, communication among components of an SRS such as transfer of measurement data from safety sensors to safety controllers and action commands from safety controllers to safety actuators are critical. Protocols like Profisafe allows application level handling of

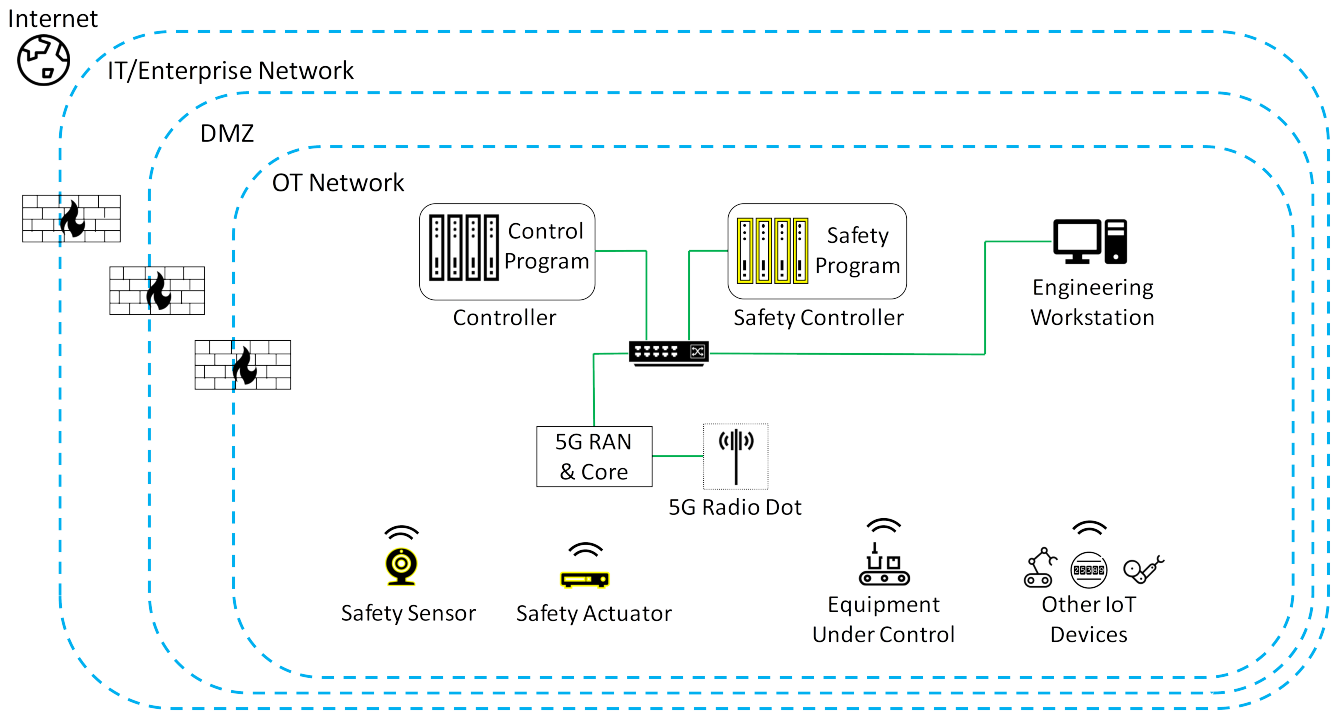

Fig. 2. Smart manufacturing setting

all possible faults and hazards infiltrated by the underlying communication network with the objective of keeping error probability in such critical packet transmissions under certain limits [7]. Therefore, almost all kinds of wired and wireless industrial communication technologies including Profinet and Profibus [8], Wi-Fi, Bluetooth and 5G can be used in the underlying communication channel of a safety system as long as a proper safety protocol is in place. In our IIoT setting depicted in Figure 2, we assumed a non-public 5G network connectivity for wireless IoT devices and cabled connectivity over Profinet for OT devices like Controller and Safety Controller.

Through this underlying communication channel, there is a continuous messaging between Safety Program running on Safety Controller and Safety Sensor/Actuator. Safety Program periodically polls Safety Sensors, which send their measurements about the safety-related ambient conditions such as temperature or pressure. Measurement values are compared to pre-set threshold values in the Safety Program. If the received sensor measurement is out of the range dictated by the threshold values, a potentially dangerous situation is detected and Safety Program sends the control command to the Safety Actuator to perform the action to mitigate damage to people, equipment or environment. If this whole process composed of sensing, deciding and actuating steps is not correctly and timely performed by the safety system, unwanted consequences can occur. Therefore, security of the overall process for functional safety as described here should be protected.

B. Trust boundaries

As depicted in Figure 2, the interaction of the OT system with enterprise network and with public networks including Internet creates a considerable change in trust boundaries in the sense that entities in either side of different networks are not trusted to each other. In other words, an attack might be launched to OT network from IT network or vice versa. In our study, we limit our focus on threats targeting the OT network which might come either from the OT network itself or another network like IT and Internet.

C. Threat Landscape

1) Assets: According to the smart manufacturing setting depicted in Figure 2, we can list the assets to be protected as below. Please note that our threat analysis in this paper is focused on safety related assets rather than assets performing generic control function.

- Equipment Under Control
- Safety Actuator
- Safety Sensor
- Safety Program
- Safety Controller
- Safety Protocol Messages
- Control Program
- Controller
- Engineering Workstation

2) Threat Actors: In a safety control system, agents posing threats can be either humans or equipment itself. Humans may present malicious activities intentionally or may introduce

inadvertent mistakes. We have identified possible threat actors as listed below based on categorization approach in [9]. Although all of these actors may impair the system, our main focus is on intentional malicious actors when we provide a deeper investigation of threats in the following subsection.

Careless Employees (causing errors): In an industrial environment, employees can be an important threat source without posing malicious intent. Common security threats may originate from unwanted mistakes for both OT and IT systems, like downloading the wrong program to a controller, or plugging an infected device into the system. These simple actions may cause major consequences if they cause systems to operate beyond safe parameters.

Disgruntled Employees: Current or former dishonest employees may present severe security and safety threats since they have insider information about the organization's control system and industrial network. They are motivated with grudge or financial gain. Previous cases show that insider attacks have targeted industrial automation systems like employees making direct changes to the Manufacturing Operating System's source code. It is possible that we observe such insider attacks targeting safety related software directly in near future.

Hackers Seeking Political or Financial Gain: An intellectual asset can be a profitable target for hackers. An attacker may simply want to harm reputation of the manufacturer or may seek to disrupt an industrial operation for financial, competitive or political reasons.

Actors performing Industrial Espionage: It is a form of espionage with the main purpose of gaining intelligence on opponent organization(s) to harm their reputation or target intellectual assets to discover their trade secrets.

Cyber terrorists: Infrastructures like nuclear plants, power grid and nation-wide critical smart manufacturing sites are the potential targets for this kind of actors seeking to disrupt, infect or cripple such critical infrastructures.

D. Possible threats and attacks in our scope

In this section, possible attack scenarios based on security vulnerabilities of the safety function system components and communication ongoing in the smart manufacturing use-case are identified. With the objective of identifying a comprehensive list of attacks, we have developed a threat taxonomy as depicted in Table I, particular to functional safety related security threats. This taxonomy is based on European Union Agency for Network and Information Security (ENISA) documents in Cybersecurity Assurance for Industry 4.0 [10]. We focused on three selected threat categories that are related to technical attacks originated from malicious intentional parties and discarded other categories covering non-technical (legal, disaster, etc.) and accidental threats. Our taxonomy is composed of threats which are relevant for attacks targeting particularly functional safety.

To determine attacks applicable for our generic smart manufacturing scenario, we scanned all threats listed in our taxonomy and determined seven attacks matched with the categories in the taxonomy table. These attacks are selected based on prioritization in [11] where experts evaluated general threats for smart manufacturing to rank severity of critical attack scenarios on a scale of five from (1) low to (5) critical. All seven attack scenarios on functional safety that we included below are ranked as either critical or high severity in [11] indicating how high is the potential impact of such attacks on functional safety. In our threat analysis, attacks originated by internal malicious actors and external attackers are both taken into consideration.

- Attack 1 (Manipulation of Hardware): Unauthorized physical access of any malicious party to the devices belonging to the safety control system may present a threat to take control of a safety-related asset like Safety Program. This attack can be launched via direct access to the device over following interfaces:
  - An interactive screen or control panel
  - Switches or buttons for device configuration
  - Removable memory cards, e.g altering the memory card content
- Attack 2 (Manipulation of Software): Attacks are possible on assets which can be used to configure and parameterize the safety systems like Engineering Workstation. Malicious modifications of safety programs, safety parameters or any other software/hardware on safety controller, safety actuator and safety sensor can be done to adversely affect the operation of functional safety.
- Attack 3 (Man-in-the-middle): There can be attacks that aim malicious intervening with cyclic communication between Safety Controller (Safety Program), Safety Actuator and Safety Sensor. Attacker may aim to obstruct, destruct or modify
  - Safety Program polling messages from Safety Controller to Safety Sensor
  - Safety-related measurement messages from Safety Sensor to Safety Controller
  - Safety Program control messages from Safety Controller to Safety Actuator

  Adversaries can launch different kind of attacks on these messages. For instance, an attacker can prevent exchange of critical safety protocol messages and cause expiration of timers on safety devices or controller, which results in switching to failsafe mode when not needed. Also, an adversary can launch a replay attack by retransmitting the messages, a data tampering attack by changing messages, a time delay attack by injecting extra time delay into measurements or identity spoofing attack by masquerading legitimate entity to fool the receiver of the message.
- Attack 4 (Bruteforce): Attacks can be performed on the Safety Controller over network via its remote programming or monitoring interfaces. Similar to the reported weaknesses in IoT devices, safety controllers are also prone to weak authentication and authorization practices. If they are accessible remotely, any type of attacker may try to break authentication, for instance, by using

TABLE I
THREAT TAXONOMY FOR FUNCTIONAL SAFETY

Category	Threat	Attacks
Nefarious activity/ Abuse	Denial of Service	Obstruction of Safety Protocol Messages
		Disruption of Safety Protocol Messages
		Exhaustion of OT network resources
		Exhaustion of Safety Program resources
	Malware	Trojan horse injected into Engineering Workstation
		Virus/Worm injected into Safety Program
	Manipulation of HW & SW	Manipulation of Safety Program code
		Manipulation of Safety Program parameters
		Manipulation of Safety Controller firmware
		Manipulation of Safety Sensor code and firmware
		Manipulation of Safety Actuator code and firmware
	Manipulation of information	Manipulation of Safety Sensor measurement
	Targeted attacks	Compromising targeted Safety Controller from particular vendor
		Manipulating targeted Safety Program code written in particular control language
	Brute force	Cracking Safety Controller configuration password
		Cracking Engineering Workstation password
Eavesdropping/ Interception / Hijacking	Man-in-the middle attack / Session hijacking	Modification of Safety Protocol Messages
		Replay of Safety Protocol Messages
		Reordering of Safety Protocol Messages
	Network reconnaissance	Collecting critical information from OT network about Safety Program, devices and protocols
Failures / Malfunctions	Malfunction of a sensor / actuator	Malfunction due to unsecure firmware of Safety Sensor
		Malfunction due to unsecure firmware of Safety Actuator
	Malfunction of a control system	Malfunction due to unsecure firmware of Safety Controller
	Software vulnerabilities exploitation	Exploitation of OS / SW vulnerability in Engineering Workstation
		Exploitation of SW code vulnerability in Safety Program
		Exploitation of improper / unsecure configuration of Safety Controller
		Exploitation of improper / unsecure configuration of Engineering Workstation
	Failure or disruption of service providers	Insecurities originating from vendors and service providers in OT network

unchanged default passwords or applying a brute force attack. Similar attacks can be performed on the Engineering Workstation.

- Attack 5 (Software vulnerability / Malfunction): Vulnerabilities in built-in security features of safety devices (actuator, sensor or controller) can be exploited because of weak credential management, firmware update from untrusted source or lack of side channel protection. Similarly, operating system vulnerabilities in Engineering Workstation or software code vulnerabilities in Safety Program can cause attackers to gain access to the critical safety assets in OT network allowing malicious manipulation.
- Attack 6 (Malware / Targeted attack): Malware injected into Safety Program either directly or indirectly via Engineering Workstation can allow attackers to manipulate safety program code in such a way that it does not command switching into fail-safe mode when there is potentially dangerous situation or it commands to do so when there is no such situation. The former attack causes physical harm on humans, equipment or environment while the latter results in unavailability. Such attacks can utilize advanced techniques to target a particular vendor's hardware and software.
- Attack 7 (Denial of Service): Injection of a high volume of packets in the OT network or flooding of malicious traffic to overload system resources in Safety Program by attackers can cause disruption in timely operation of the overall safety function.

III. SECURITY BEST PRACTICES ON FUNCTIONAL SAFETY

In this section, we briefly present safety and security related standards and publications of standardization bodies. Then, we provide some best practices to address security requirements and mitigate the threats mentioned in Section II.

A. Standardization

We may categorize the relevant standards in smart manufacturing into three groups where the focus is only on safety, only on security, and both on safety and security.

a) Safety Standards: IEC 61508 [1] describes a functional safety standard for electrical and electronic elements that provide safety functions for the EUC. The standard provides requirements for a system to be designed, implemented, operated and maintained to achieve the required safety integrity level (SIL) that is applicable to all industries. IEC 61784 provides a set of standard documents to design devices used in communication and process control in manufacturing. Specifically, IEC 61784-3-3 [8] provides an overview of PROFIsafe, which relates to transmission of safety-related messages considering the functional safety requirements defined in IEC 61508.

b) Security Standards: ISA/IEC 62443 [5] standard document is related to current vulnerabilities and possible mitigation methods in industrial automation and control systems. IEC 62443 has several series which cover different parts of

the security aspects such as: (i) IEC 62443-2-4: Security program requirements for Industrial Automation and Control Systems (IACS) service providers, (ii) IEC 62443-3-3: System security requirements and security levels, (iii) IEC 62443-4-1: Product development requirements, (iv) IEC 62443-4-2: Technical security requirements for IACS components.

c) Safety and Security Standards: There are also standards that take safety and security at the same time into account for industrial automation. IEC 63069 standard provides a framework for safety and security with a sector agnostic approach [6]. It provides common application of *IEC 61508 (all parts)* and *IEC 62443 (all parts)* standards by providing a general guidance on how to handle safety and security analyses and resolve conflicts arising from conflicting countermeasures within the life cycle of the system. Also, IEC 63074 provides guidance on the use of *IEC 62443 (all parts)* where security threats and vulnerabilities could effect functional safety of the system. There are also some working groups that investigate security and safety in manufacturing. One example is ISA-99 WG7 that works on a framework to align safety and security in industrial automation and control systems. Another working group is IEC TC65 AHG1 that is an ad-hoc working group in IEC aiming to build a framework for coordinating safety and security.

B. Best Practices

In this subsection, we briefly present security best practices for protecting functional safety based on recommendations and guidelines including the ones developed by the standardization bodies as listed above. These best practices could support proper handling of security requirements for safety function in smart manufacturing and mitigation of potential threats as mentioned in previous section before they lead to a wide range of risks including fatal physical damage to the environment and people.

In a high level, three principles should be considered based on IEC 63069: (i) protection of safety implementations, (ii) protection of security implementations and (iii) compatibility of implementations. Safety functionalities to be implemented should be carefully selected not to adversely affect security implementations. This is as important as utilization of security solutions to protect safety implementations. For example, deploying remote access without any secure solution will damage the overall security deployment, which, in turn, may lead to a safety incident having a considerable damage on human or equipment. Also, selected security solutions should not have an negative impact on the safety system. Consideration of timing aspects of safety systems when choosing a security solution is an example of this compatibility of implementation principle.

In addition to the main pillars of information security, namely, confidentiality, integrity and availability, security for functional safety should address the requirement for prevention of damage to critical physical assets to protect against intended malicious behaviours. According to IEC 63074, the foundational requirements to achieve this can be summarized as follows: Authentication of all entities who have access to the ICS must be ensured. Integrity of ICS data must be ensured against both accidental and intentional manipulation. The data to be stored or communicated in ICS should be confidential using cryptographic protocols. ICS should be divided into partitions to ensure security for each level specifically. Security breaches should be handled via reporting, collecting evidence and taking action against by corresponding authority. The availability of ICS should be assured against denial of services.

As summarized above, industry standards provide a valuable guide on what kinds of policies and practices should be followed to protect the safety function and Industrial IoT systems in general. On the other hand, these standard documents include very little information on how exactly these best practices can be implemented using existing technologies. Another contribution of our paper is depicted in Table II where we provide a mapping of 5G security features to the particular security requirements needed to protect functional safety when 5G is used as the connectivity technology in an Industrial IoT network as we depict in this paper. As seen in the table, network slicing and closed access group features of 5G allows creation of proper security zones and thus prevents potential malicious message flow from a compromised device or network segment to the safety-related system. Besides, assurance on the integrity protection of critical safety messages can be provided by user plane integrity feature of 5G. In addition to integrity protection, communication between main components of a functional safety system including safety program, sensors and actuators should be secured in terms of message and source authentication. 5G allows use of various types of strong EAP-based authentication methods which can be deployed to provide mutual authentication even for IoT devices without a SIM-card. Also, 5G mechanisms for secure credential storage and processing provide strong protection against identity compromise and spoofing.

Before concluding this section, it should be emphasized that all technical security features mentioned above must be implemented and enabled to provide protection. Also, all these technical solutions for securing safety function should be considered for the whole system life cycle and implemented countermeasures should be monitored and improved considering results monitored as well as lessons learned from previous safety-security events.

IV. Related work

One study depicting importance of security in manufacturing domain is [12]. In this work, authors experimented a case study where an engineering workstation was infected with a virus and the manufactured element were different than the design. This study shows that how easy it can be to create a major physical defect via a minor change in cyber domain, which could have a big adverse impact on physical assets.

One of the first studies addressing security of functional safety is done by Åkerberg and Björkman on Profinet and Profisafe [13]. They showed that safety related data communicated in these particular protocols can be modified and this attack cannot be detected by any security mechanism [14].

TABLE II
MAPPING OF 5G SECURITY FEATURES TO SECURITY REQUIREMENTS OF FUNCTIONAL SAFETY

Security Requirements	Relationship to functional safety communication	5G Network Features
Message integrity	Protection against malicious parties aiming to modify critical safety messages intentionally	User plane integrity protection
Message & Source Authentication	Countering against safety protocol messages originating from unauthorized parties	5G-AKA, EAP-AKA, EAP-TLS Mutual authentication (5G private network and IIoT application)
Access Control	Isolation of safety-related from non-safety OT devices and networks	Network slicing Closed access groups

They proposed so-called security modules and showed that their implementation could prevent man-in-the-middle attacks on Profinet protocol [15]. They made another demonstration of their work by proof-of-concept implementation on Profinet, Profisafe and WirelessHART [16].

Novak et. al. presented a general approach for a safe and secure Building Automation Control system by extending pre-design phase with additional security steps [17]. They addressed commonalities between security and safety and suggested use of cryptographic operations to ensure safety and security at the same time. There are two recent papers which address security and safety in process and manufacturing industry respectively [18], [19]. Both of these studies present practical attack scenarios for industrial use cases. However, they do not provide a taxonomy of security threats affecting safety.

In addition to studies covering practical aspects of securing functional safety, there are also works in academic literature presenting a more conceptual view on the relationship between security and safety such as [20], [21] and [22]. These studies present formal methodologies on how to perform a combined risk analysis to address safety hazards and security threats by exploiting common features and by resolving conflicts.Yet, none of them cover security attacks on functional safety.

One interesting work where authors present a taxonomy of security challenges that could also have safety impacts is [23].The paper provides how IoT can be adapted in the underground mines for implementing an effective communication and data collection technology in order to enhance safety and productivity. It also provides detailed information about the IoT security challenges and classify them. The threat taxonomy in [23] covers the specific IoT use case for underground mine communication whereas our taxonomy is for security threats impacting safety function in IoT-based smart manufacturing.

V. CONCLUSION

Supported by advancements in IoT technologies in smart manufacturing domain, factories are becoming more connected both within the elements in the factory and also with the outside world too. This connectivity is required and beneficial for the integration of automation and control processes. However, while improving the automation and overall production performance in smart factories, one should be careful about a new attack surface, functional safety, which may have vulnerabilities arising from intersection of IT and OT boundaries. In order to shed a light on this topic, we investigated security issues in functional safety for smart manufacturing using IoT. Our main contribution in this paper is the development of a taxonomy of security threats particular to functional safety in industrial IoT domain. Besides, we identified several attack scenarios with highly severe impact on both physical assets including human life and cyber-assets like availability of an IIoT-based manufacturing system. Finally, we provided a set of best practices aligned with related industry standards and we also showed that how they can be implemented using security features of 5G to mitigate some of the threats identified in our study. Future studies elaborating how such state-of-the art technologies can be leveraged to provide protection for critical functions in IoT applications like safety are needed as well as studies addressing domain specific security requirements. In this context, we're planning to investigate how security attacks targeting safety system vulnerabilities can be mitigated using machine learning.

ACKNOWLEDGMENT

This work was funded by The Scientific and Technological Research Council of Turkey, under 1515 Frontier R&D Laboratories Support Program with project no: 5169902.

REFERENCES

[1] IEC/TR 61508-0, "Functional safety electrical/electronic/programmable electronic safety-related systems," International Electrotechnical Commission, Tech. Rep. 61508, 2005, part 0: Functional safety and IEC 61508.

[2] T. Meany, "Functional safety and industrie 4.0," in *2017 28th Irish Signals and Systems Conference (ISSC)*. IEEE, 2017, pp. 1–7.

[3] A. A. Di Pinto, Y. Dragoni, and A. Carcano, "Triton: The first ics cyber attack on safety instrument systems," in *Proc. Black Hat USA*, 2018, pp. 1–26.

[4] J. Åkerberg and M. Björkman, "Exploring network security in profisafe," in *International Conference on Computer Safety, Reliability, and Security*. Springer, 2009, pp. 67–80.

[5] IEC 62443-4-1, "Security for industrial automation and control systems–part 4-1: Secure product development lifecycle requirements," International Electrotechnical Commission, Tech. Rep., 2018.

[6] IEC/TR 63069, "Industrial-process measurement, control and automation framework for functional safety and security," International Electrotechnical Commission, Tech. Rep. 61508, 2019.

[7] PROFIsafe, "System description technology and application," PROFIBUS Nutzerorganisation e. V. (PNO), Tech. Rep., 2016.

[8] IEC 61784-3-3, "Industrial communication networks - profiles - part 3-3: Functional safety fieldbuses - additional specifications for cpf 3," International Electrotechnical Commission, Tech. Rep., 2016.

[9] R. Automation, "Safety through security," Tech. Rep., 2016.

[10] V. Sklyar and V. Kharchenko, "Enisa documents in cybersecurity assurance for industry 4.0: Iiot threats and attacks scenarios," in *2019 10th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS)*, vol. 2, 2019, pp. 1046–1049.
[11] ENISA, "Good practices for security of internet of things in the context of smart manufacturing," European Union Agency for Cybersecurity, Tech. Rep., 2018.
[12] L. J. Wells, J. A. Camelio, C. B. Williams, and J. White, "Cyber-physical security challenges in manufacturing systems," *Manufacturing Letters*, vol. 2, no. 2, pp. 74–77, 2014.
[13] J. Akerberg and M. Bjorkman, "Exploring security in profinet io," in *2009 33rd Annual IEEE International Computer Software and Applications Conference*, vol. 1. IEEE, 2009, pp. 406–412.
[14] J. Åkerberg and M. Björkman, "Exploring network security in profisafe," in *International Conference on Computer Safety, Reliability, and Security*. Springer, 2009, pp. 67–80.
[15] J. Akerberg and M. Björkman, "Introducing security modules in profinet io," in *2009 IEEE Conference on Emerging Technologies & Factory Automation*. IEEE, 2009, pp. 1–8.
[16] J. Åkerberg, M. Gidlund, T. Lennvall, J. Neander, and M. Björkman, "Efficient integration of secure and safety critical industrial wireless sensor networks," *EURASIP Journal on Wireless Communications and Networking*, vol. 2011, no. 1, p. 100, 2011.
[17] T. Novak, A. Treytl, and P. Palensky, "Common approach to functional safety and system security in building automation and control systems," in *2007 IEEE Conference on Emerging Technologies and Factory Automation (EFTA 2007)*. IEEE, 2007, pp. 1141–1148.
[18] M. Noorizadeh, M. Shakerpour, N. Meskin, D. Unal, and K. Khorasani, "A cyber-security methodology for a cyber-physical industrial control system testbed," *IEEE Access*, vol. 9, pp. 16 239–16 253, 2021.
[19] L. Perales Gómez, L. Fernández Maimó, A. Huertas Celdrán, F. J. García Clemente, M. Gil Pérez, and G. Martínez Pérez, "Safeman: A unified framework to manage cybersecurity and safety in manufacturing industry," *Software: Practice and Experience*, vol. 51, no. 3, pp. 607–627, 2021. [Online]. Available: https://onlinelibrary.wiley.com/doi/abs/10.1002/spe.2879
[20] D. Pan and F. Liu, "Influence between functional safety and security," in *2007 2nd IEEE Conference on Industrial Electronics and Applications*, 2007, pp. 1323–1325.
[21] T. Novak and A. Treytl, "Functional safety and system security in automation systems - a life cycle model," in *2008 IEEE International Conference on Emerging Technologies and Factory Automation*, 2008, pp. 311–318.
[22] F. Reichenbach, J. Endresen, M. M. R. Chowdhury, and J. Rossebø, "A pragmatic approach on combined safety and security risk analysis," in *2012 IEEE 23rd International Symposium on Software Reliability Engineering Workshops*, 2012, pp. 239–244.
[23] A. Singh, D. Kumar, and J. Hötzel, "Iot based information and communication system for enhancing underground mines safety and productivity: Genesis, taxonomy and open issues," *Ad Hoc Networks*, vol. 78, pp. 115–129, 2018. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S1570870518303524