IOT Challenges: Functional Safety

Vytaras Juraska
Electronics Engineering (7^{th} Semester)
Hamm-Lippstadt Hochschule
Lippstadt, Germany
vytaras.juraska@stud.hshl.de

***Abstract*—in this paper main focus is emphasizing the importance of functional safety in the field of Internet Of Things (IOT), while also analyzing the today's standardised requirements, which each IOT device has to follow.**

I. Introduction to Internet of Things (IOT)

The Internet of Things (IoT) [1] is upcoming and constantly evolving technology which allows different devices (which in IoT field are considered as "things") to communicate through the Internet connection. Currently, IoT is known to use more and more of Artificial Intelligence techniques, which helps processing data gathered by different sensors and predict the next action accordingly. In terms of various fields, where IoT is being widely implemented, are as follows: manufacturing, agriculture, education, commercialization, smart homes, auto cars, medical and so on.

In fact, IoT is such a vastly adapted technology, that general purpose IoT technologies for some cases are not suitable enough, hence various of application specific IoT fields are in constant development (e.g. Internet of Medical Things (IoMT), Internet of Underwater Things (IoUT) along with others) [2]. For instance, a specific IoT for environmental water monitoring would have different requirements from a specific IoT for medical monitoring, which would require much higher and more precise requirements for real-time data transfer and security.

Another important topic about IoT is its safety and security, which at current state is exposed in concerning levels [3]. Internet already introduces a magnitude of security issues, such as cyber-attacks, malware, etc. One of the examples in bad security practice happened in 2016 with an insulin pump. According to the references [3], the specified device users experienced impersonation issues by third party, which had the possibility to cause malfunction of the equipment, leading to a possibility of risking a human life, since it is, in fact, a medical device, which is crucial to some users. Surprisingly, manufacturers did not take any actions, rather advised users in correct usage of the device. In this case, this should not be the case - human error handling a device, which is meant for an average patient, can not lead to device failure. Thus, manufacturers must apply specific Secure by Design practices, which would take functional safety seriously already from the design phase of development.

A. General Applications of IOT

1) Personal: This would include personal health, such as[1]:

- Remote Patient Monitoring - one of the most common applications, monitoring vital variables of a human body like heart rate, blood pressure, temperature and so on. Generally, its purpose is for patients, who can not visit a healthcare facility - vitals could still be monitored and medical advice could be handled accordingly. Automatic analyzing helps to inform healthcare professionals about an upcoming problem, which creates an opportunity to stop an upcoming issue before the situation gets worse;
- Glucose Monitoring - for a significant amount of people across the world with diabetes, glucose monitoring has been not the most simplest process. Traditionally, it had to be tracked and checked manually, hence the patients received the results only after executing the initial manual test, which creates problems for people with widely fluctuating glucose levels. Current IoT device allows for continuous, automatic monitoring of glucose, which can also alert the patient, if the levels are too low and track the data automatically[2].
- Hand Hygiene Monitoring - a device, which informs a user upon the inspection, if their hands are clean. This is practical especially at unique times like the current crisis situation, where hand cleanliness is an important aspect. Traditionally, there has not been a quick and effective way to check it automatically, but this solution with the availability of sensors and their IoT communication, can achieve acceptable results[3].

There are many various examples of application, but generally, personal use can extend even to ways of social interaction, hence the possibilities in this field are limitless.

2) Home: Electronic appliances integrated with IoT redefine communication between user and devices. Every electronic appliance, such as lights, air conditioning, security cameras, refrigerator, oven and so forth can be connected to the internet quite simply. Integrating a smartphone into the scenario and the customer now can remotely control almost any electronic appliance there is.

[1]https://ordr.net/article/iot-healthcare-examples/
[2]https://www.niddk.nih.gov/health-information/diabetes/overview/managing-diabetes/continuous-glucose-monitoring
[3]https://biovigil.com/

In one of the references [4], authors mention some application examples:

- Ambient intelligence-based lightning system has an integrated intrusion detection, which will detect intrusion and give alert to the nearby police station, by acquiring exact geographical location;
- Gas or smoke detection system, which sends an e-mail or SMS to fire department.

Home environment field has also many benefits from the IoT integration to everyday technology.

3) Industrial: Not surprisingly, the industry also benefits greatly from the technology of IoT, since most industrial machinery are using a bulk of various sensors, with which communication is crucial[4]. Here are some areas of application, as an example of where this technology is being used and for what purpose:

- Remote automated equipment management and monitoring is one of the main Industry IoT use-cases, which allows to have a centralized system, to execute a crucial task of equipment maintenance. The remote characteristic also implies, that this technology can be adapted to maintain more than one geographical location at a time;
- Predictive maintenance is a system integrated with IoT, which sends alerts, when the machinery are in dire need of maintenance before a crisis occurs.
- Quality control is another massive application, from raw materials to the built product - with the help of various sensors, AI and precise real-time calculations IoT technologies help analyze the product, record each analysis of the product and inform engineers at which part the product maintain quality, and if error happened, at which point it was detected.

II. Introduction to Functional Safety

As mentioned before, IoT is a field, which has accumulated big interests in various of applications. Some applications are crucially important, where a single failure could cause undesirable and devastating results, good example was given, referring the insulin pump device. Generally, IoT is being implemented in a lot of fields, so having a standardised method of risk-free products in every application is a complicated matter, since every application, as mentioned before, can be so unique, that the general requirements might not fit the product as much as specific requirements.

To understand how complex risk prevention implementing IoT is - in the reference [5] a topic of security and functional safety specifically in industrial IoT applications is investigated. These two terms have shared goals of preventing a product or a system from risks, but they do have unique differences, which have to be understood.

A. Meaning of Functional Safety

The word safety is ”defined as the state of being free from unacceptable risk, which causes direct or indirect harm to human health, environment or property” [5], hence the importance of safety is prevention from physical harm. Regarding functional safety, it is a term, which mostly relates to software applications, where correct operation of the system prevents from physical harm at acceptable levels, by reassuring successful communication and control, when it is required.

B. Meaning of Security

Security risks are concerning on deliberate malicious intents, where when exploited - vulnerabilities can affect both physical and cyber world.

C. Comparison between Safety and Security

Functional safety is focusing on protecting purely physical world assets (human health and life, environment and equipment) from dangers of Operational Technology (OT) malfunctions, while Information Technology (IT) security is all about protecting the information of all IT related assets. Previously security and safety were two different subjects, being operated in their own separate domains, but generally, these two systems have a strong connection with each other (Figure 1).

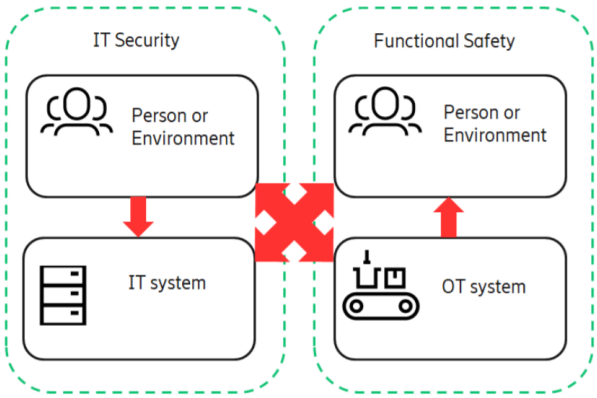

Fig. 1. Inter-connectivity of OT and IT [5]

There are cases, especially in IoT applications, where bypassed security of IT can directly affect OT. For an example - Triton Malware, a malicious attack in 2017, which targeted safety of oil and gas petrochemical facilities, which ended up in putting systems into emergency stop. Fortunately, the outcome was just lost availability of equipment, but this is a good example of how important it is to consider both risk-preventing systems, when developing and designing security and safety.

III. Characteristics of Functional Safety

Knowing, that functional safety focuses for machinery and equipment hazard control, couple of important characteristics have to be analyzed to get a wider understanding of this specific field.

[4]https://nexusintegra.io/7-industrial-iot-applications/

A. Machinery Safety Functions

Mostly, the machinery is implemented with a detection system, which checks if there is a person on any other environmental asset, which has to be insured with risk-prevention. One of the examples of it is an entrance door with an interlock, for which to open, the safety relay has to check the robot safety system, if it is safe for someone to enter the area (Figure 2). This example would provide suitable level of risk reduction in terms of functional safety and also satisfy such requirements as safety reaction time, since the door would not open, if a threat is a possibility.

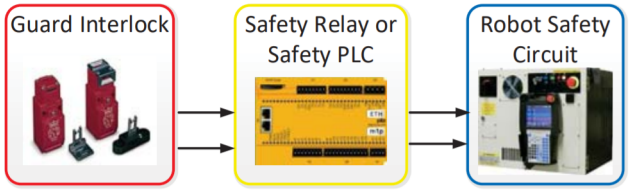

Fig. 2. Safety block functions in machinery applications [6]

B. Safety Integrity Level

To compare, analyze and understand the amount of required functional safety, specific levels have to be considered, which would help creating a specific goal for safety, to be able to achieve better quality of safety. In the case of Safety Integrity Level the variable in consideration is average frequency of dangerous failure per hour, which is defined as probability of failure on demand (PFD). Two international different standards cover the requirements of safety, which help analyze this variable: ISO 13849 and IEC 61784.

IV. Standardised Requirements

A. IEC 61508

Rely on the document of References [7] and [8].

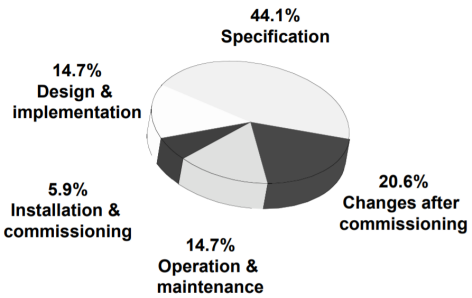

Fig. 3. Main control system failure causes [7]

B. ISO 13849

Rely on the document of Reference [8] (also the document AN9025, which has the introduction to this standard).

C. IEC 61784

V. Background of FuSa

Which standards are important, general background.

VI. Example Issues and Unique Solutions

Some examples of how IOT Functionality can go wrong and what was or might be done to avoid the problems. Rely on the Reference [6]

One of the examples could be Medical IOT System (Reference [3]).

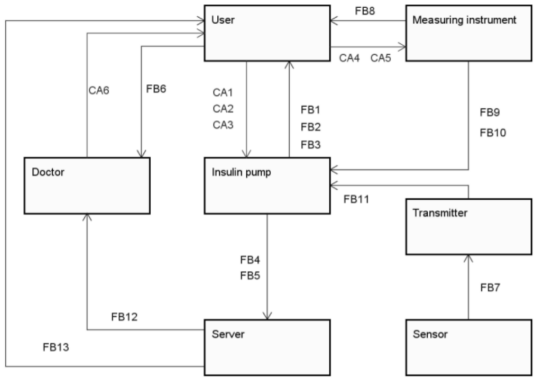

Fig. 4. Example control structure in IOT application to medical field [3]

VII. Advantages of Functional Safety

VIII. Disadvantages of Functional Safety

IX. Summary and Conclusion

Summary of paper and conclusion to the whole topic in one.

X. Affidavit

I, Vytaras Juraska, herewith declare that I have composed the present paper and work by our self and without use of any other than the cited sources and aids. Sentences or parts of sentences quoted literally are marked as such; other references with regard to the statement and scope are indicated by full details of the publications concerned. The paper and work in the same or similar form has not been submitted to any examination body and has not been published. This paper was not yet, even in part, used in another examination or as a course performance.

References

[1] S. M. Alzahrani, "Sensing for the Internet of Things and Its Applications," in *2017 5th International Conference on Future Internet of Things and Cloud Workshops (FiCloudW)*. Prague: IEEE, Aug. 2017, pp. 88–92. [Online]. Available: http://ieeexplore.ieee.org/document/8113776/

[2] K. L.-M. Ang and J. K. P. Seng, "Application Specific Internet of Things (ASIoTs): Taxonomy, Applications, Use Case and Future Directions," *IEEE Access*, vol. 7, pp. 56 577–56 590, 2019. [Online]. Available: https://ieeexplore.ieee.org/document/8707089/

[3] T. Hayakawa, R. Sasaki, H. Hayashi, Y. Takahashi, T. Kaneko, and T. Okubo, "Proposal and Application of Security/Safety Evaluation Method for Medical Device System that Includes IoT," in *Proceedings of the 2018 VII International Conference on Network, Communication and Computing - ICNCC 2018*. Taipei City, Taiwan: ACM Press, 2018, pp. 157–164. [Online]. Available: http://dl.acm.org/citation.cfm?doid=3301326.3301330

[4] S. J. Ramson, S. Vishnu, and M. Shanmugam, "Applications of Internet of Things (IoT) – An Overview," in *2020 5th International Conference on Devices, Circuits and Systems (ICDCS)*. Coimbatore, India: IEEE, Mar. 2020, pp. 92–95. [Online]. Available: https://ieeexplore.ieee.org/document/9075807/

[5] E. Tomur, U. Gulen, E. U. Soykan, M. Akif Ersoy, F. Karakoc, L. Karacay, and P. Comak, "SoK: Investigation of Security and Functional Safety in Industrial IoT," in *2021 IEEE International Conference on Cyber Security and Resilience (CSR)*. Rhodes, Greece: IEEE, Jul. 2021, pp. 226–233. [Online]. Available: https://ieeexplore.ieee.org/document/9527921/

[6] S. Robinson, "Living with the Challenges to Functional Safety in the Industrial Internet of Things," in *Living in the Internet of Things (IoT 2019)*. London, UK: Institution of Engineering and Technology, 2019, pp. 35 (6 pp.)–35 (6 pp.). [Online]. Available: https://digital-library.theiet.org/content/conferences/10.1049/cp.2019.0160

[7] R. Bell, "Introduction to IEC 61508," p. 10.

[8] T. Meany, "Functional safety and Industrie 4.0," in *2017 28th Irish Signals and Systems Conference (ISSC)*. Killarney, Co Kerry, Ireland: IEEE, Jun. 2017, pp. 1–7. [Online]. Available: http://ieeexplore.ieee.org/document/7983633/