Adoption of Miniaturized Safety-Related Systems for Industrial Internet-of-Things Applications

Ali Hayek(✉), Samer Telawi, Christian Bieler, and Josef Börcsök

Chair for Computer Architecture and System Programming,
University of Kassel, Wilhelmshoeher Allee 71, 34121 Kassel, Germany
ali.hayek@uni-kassel.de

Abstract. Nowadays the internet is considered as given in almost any consumer electronic application. Internet connections are now extended to physical objects and are able to connect the living environment with computers, laptops, tablets and smartphones. We are dealing here with the Internet of Things. However, it is only the beginning of the Internet of Things revolution and today the development process has entered a new stage, where Internet of Things includes more and more industrial devices. Of course, using Internet of Things in such application fields faces the challenge of balancing the flexibility of internet communication and the robustness of industrial applications. In this paper, a concept of the adoption of a miniaturized safety-related solution on a single chip for industrial Internet of Things applications is introduced. An example application is presented to prove the feasibility of the introduced concept.

Keywords: Internet of Things · Safety systems · Systems-on-Chip · Wireless network

1 Introduction

Intelligent computer systems, peripheral devices of any type such as mobile devices, sensors, machines and vehicles are networked with each other and with the external environment by means of the Internet of Things (IoT). The analysis of the IoT data offers many opportunities for companies to exploit, such as taking faster decisions, better optimization and refinement of their business processes, revealing new applications and even the development of new business models. IoT thus offers enormous potentials for almost any technical field as energy technology, industrial automation and factory, medical technology, automotive industry as well as production and logistics.

Against this background, IoT applications can mainly be divided into two categories. On one hand, there is IoT applied to consumer electronics (CIoT), and on another hand, there is the industrial IoT (IIoT). CIoT devices represent consumer-oriented applications such as big and small household appliances that are usually communicating with small data volumes and low data rates but they are not used in safety or mission critical applications. Whereas, IIoT devices represent industry-oriented applications, e.g. machines and robots in an industrial environment in which

N. Mitton et al. (Eds.): InterIoT 2016/SaSeIot 2016, LNICST 190, pp. 116–126, 2017.
DOI: 10.1007/978-3-319-52727-7_13

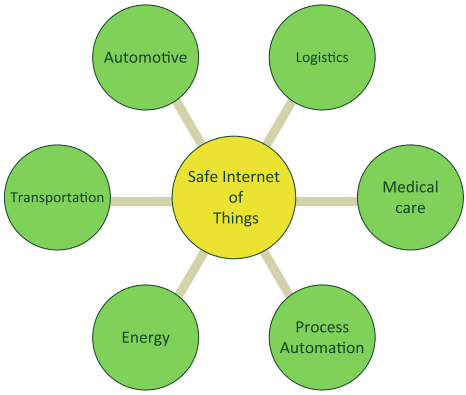

Fig. 1. Application fields of the Safe Internet of Things

they communicate with higher data volumes and rates. Furthermore, IIoT applications have normally to be classified as safety and reliability critical. In this context Fig. 1 provides an overview of the most important fields that can involve IIoT devices in safety-related applications (Safe Internet of Things).

According to the most common definition, the IoT is a network of physical things, which are different embedded electronic parts such as sensors, microcontrollers and communication interfaces to collect and exchange data [1]. Moreover, adopting these things is getting more widely in the industrial environments to fulfill more critical tasks that are related to monitoring performance and safety of workers, machines or any other important factor in the industrial environment. Furthermore, enormous efforts have been conducted to safely monitor and manage the industrial environments such as the research work conducted by Alcaraz and Lopez [2, 3], in which they introduce a system that utilizes many technologies, and the wireless sensors are a main part of these solutions. In order to provide a safe sensory data, which is the main effort of this research work, the wireless sensory system must comply one of the safety-related architectures adopted in the safety-related digital systems [4, 5].

Consequently, such a linkage between safety-related systems and IoT devices is not well-engineered yet; and this requires implementing a safety-related architecture for the whole path of the captured data, starting from the sensors to the end point to which the data is transmitted. Some challenges, as system size, costs and ensuring the high level of safety and resilience, have still to be mastered. In this work, consistently with our own research work about the realization of on-chip safety systems a concept is presented, which focuses on the realization of applying miniaturized IIoT systems to safety-related applications. The objective in this context is to establish miniaturized as well as robust, flexible and efficient systems for the use in IIoT devices.

The paper is organized as the following. Section 2 provides an overview of the state of the art of safety-related systems and on-chip safety systems. Section 3 serves to introduce the concept of adapting an on-chip safety system to IIoT applications. Initial results are presented through the use of an example application in Sect. 4. Finally, a summary and an outlook serve to round off this paper.

2 Safety Systems

2.1 Introduction

The relevance of safety-related systems is given by an increasingly growing level of safety awareness in many technical areas leading to strengthened requirements for standardized safety-related systems that can be applied to various fields of applications. Moreover, this relevance is reflected in the technical trend towards safety systems that are increasingly flexible and efficient in a way that they correspond to the current state of the art which can be provided for industrial applications. Furthermore, economic considerations do play a major role because they put stringent demands on the development of safety-related systems. These systems have to meet the key requirements, such as safety and reliability, in addition to that they require several further characteristics like miniaturized size but nevertheless they also require maximum performance and lower costs as well as the highest level of flexibility and portability at the same time. The latter aspect is particularly important due to the connection with applications in the field of Industry 4.0 and the IIoT.

In recent years, based on the previously mentioned background, more new technological platforms have been increasingly used to realize safety-related systems. Conventional hard-wired controllers have been replaced by electronic and programmable controllers. The current trend in this field is characterized by two important aspects: One aspect is to make use of the technical progress that results from the development within the field of semiconductor technology and the other aspect is to allow that given state of the development an appropriate corresponding state of standardization. In fact, the safety-related electronic systems have undergone a significant development over the last few years. A decisive milestone in this area has been achieved, especially with the release of the second edition of the standard IEC 61508 [6] and the associated introduction of safety-related systems involving on-chip redundancy. Safety-related systems with two redundant channels can now be developed on one single chip and certified in accordance with standard IEC 61508.

The following subsections provide a rough overview of the standard IEC 61508 and its development. Subsequently, a brief outline is given about on-chip safety systems that are proposed to be used for the realization of the introduced concept.

2.2 Safety Standard IEC 61508

In this section a brief insight into the safety standard IEC 61508 is introduced. The standard IEC 61508 is limited to electrical/electronic/programmable electronic safety-related systems – short form E/E/PE. It is divided into seven parts and deals with the general requirements for the development process of safety-related systems at hardware and software levels. Furthermore, the standard serves to define key terms like functional safety or safety integrity level (SIL), which serves for a classification of safety-related systems. The safety-related systems are classified into four levels SIL 1 to SIL 4. It applies here that the higher the SIL, the safer the system under consideration. In addition, the standard provides different parameters to be used for a

quantitative evaluation of various safety architectures. Finally, examples and operating instructions for the determination of the safety integrity level as well as for the way to use the different architectures, procedures and measures are provided by the standard.

For the on-chip safety systems that are proposed in this research work, the second edition of that standard of the year 2010 is of great significance. Among other things, the on-chip redundancy, which provides the possibility to develop safety-related systems on a single silicon substrate for SIL 3 applications, was introduced in this edition.

2.3 On-Chip Safety Systems

Besides the key requirements like networkability, reliability and robustness, further requirements do also play a significant role for IIoT applications, especially in the case of the embedded applications, where the compact system size and reduced power loss at an optimized performance, represent the key factors for technical and economic considerations. The conventional technique, which was used for safety-related systems, has considered these factors solely in a very limited way. Therefore, only when the on-chip redundancy in the IEC 61508 was introduced; a safety-related basis has been established for that. At that point the standard provides a roadmap for the development of safety-related systems on a single silicon chip. In fact, since the introduction of that standard, the trend was towards an integration of complete control systems on the smallest silicon areas. Several semiconductor manufacturers and safety experts like Texas Instruments, Freescale or Yogitech have also brought dozens of such solutions to the market ever since, and an overview on the previously existing safety chips is provided in [7]. For the purpose of realizing systems with on-chip redundancy measures, methods and modelling techniques, that should serve to guarantee the technical safety, have to be provided at all levels of development. These comprehensive measures have to be taken on the modelling level as well as on the chip design level. In [8] a summarized overview of these required measures is introduced. In the following subsection, an example is given, which is based on an own previously published architecture, and it serves to illustrate how a safety controller works on a chip. The introduced architecture serves as a basis for the research concept that is presented in this paper.

2.4 On-Chip Safety Architecture

The presented architecture is based primarily on 1oo2D architecture (one out of two with Diagnosis). The 1oo2D architecture according to standard IEC 61508 consists of a simple redundant architecture including two channels and additional diagnosis. In a 1oo2D architecture a dangerous failure can only occur if both channels do create a dangerous failure. The system can fail, only if a dangerous error has occurred in both channels. As a mean of increasing the flexibility of this architecture, it is extended by a communication processor, which serves as a black communication channel. This channel is not interacting with the safe system (interference free communication channel). Figure 2 illustrates a block diagram of this architecture which is represented in the green box on both sides of the figure. The design, which is in accordance with

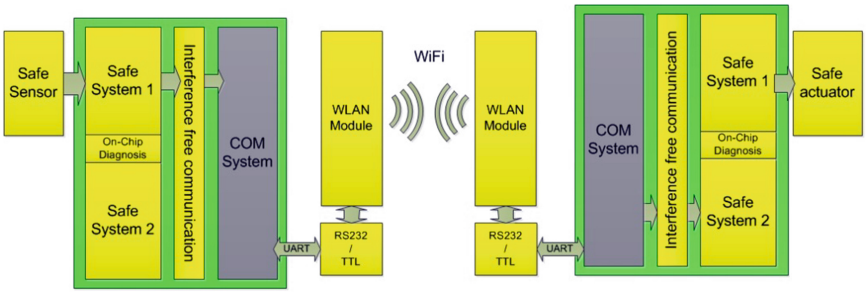

Fig. 2. Block diagram of the IIoT-Enabled on-chip safety system

IEC 61508 second edition representing a safety solution with on-chip redundancy has already been implemented and published in [9].

3 IIoT-Enabled Safety System

3.1 System Architecture

As already been outlined in the previous sections, the basic idea of the current concept is to use an on-chip safety system for safety-related IIoT applications. In this context, the focus is led on using a flexible and miniaturized safety system, which is appropriate for applications that place stringent demands on particularly the system size and costs.

Figure 2 above serves to illustrate a block diagram dealing with a possible implementation of the research project. This implementation adopts the Safe-Device-to-Safe-Device communication model and the on-chip safety system represents the heart of it. The most important features of this on-chip system are the ability to process safe inputs like input sensory data and to allow safe outputs such as actuator data. In this case, the communication of IoT applications is conducted via wireless LAN. At this point, the communication could also be realized via Ethernet or any other wireless communication like RFM radio modules; a concept that utilizes RFM modules will be presented later on. In addition, any communication model of IoT could be adopted such as Device-to-Cloud model or Device-to-Gateway model with respect to safety-related aspects [10]. The following sections deal in more detail with the single components of the introduced system.

3.2 Target on-Chip Safety System

The target on-chip safety system is a miniaturized SIL 3 compliant architecture which integrates all features of a PLC on a single chip. This reduces the number of required components for safety applications and improves system dependability. A more detailed description of this architecture can be found in [9]. Figure 2 gives a general overview about the system architecture of the safety PLC, which consists of two subsystems: a redundant system (1oo2D safe system) and a single-core system intended

for communication (COM system). Both subsystems are connected via interference-free channel. In addition, both processor systems may trigger an interrupt in the other sub-system. Both subsystems contain processor cores with their own data and program memories, digital inputs and outputs, as well as diverse communication interfaces. The COM system acts as black channel for safe communication between the safe system and the devices of safety-related applications, through utilizing its communication interfaces such as serial interfaces and Ethernet.

3.3 WLAN Module

The ESP8266 WLAN module [11] is used in this research work, and it has been successfully marketed in different versions by the company Espressif for some time. The modules typically consist of the system-on-chip SoC ESP8266EX, an external Flash RAM and an antenna or an antenna interface. The modules mainly differ according to the number of interfaces that are available to the exterior. The smallest configuration ESP8266-01 including 8 pins is used for the present research work. It is also important to note at that point that WLAN modules of other manufacturers or other wireless communication interfaces can also be used.

The module ESP8266-01 represents the smallest module of the ESP8266 WIFI family. The structure is roughly presented in Fig. 3 which shows its components that are consisting of a 32 bit RISC SoC (Tensilica L106) with integrated analog/RF transceiver, Flash RAM memory and an antenna that is integrated on the board. The module is produced by Espressif in China. Having a size of 5 × 5 mm for the SoC and 1.5 × 2.5 cm for the module it involves rather low manufacturing costs. Due to its low power consumption of a maximum of 215 mA and less than 1 mA in stand-by mode, furthermore, its small size and high performance, the module is not only suited for being used as a WLAN module but also for being used as complete solution for IoT applications. The firmware can be freely programmed and only 20% of the possible computational power is consumed during the WIFI operation. Consequently 80% of the performance is theoretically available for user applications. Version ESP8266-01 provides to the user, alongside with the SoC, an external Flash and an antenna, 8 pins,

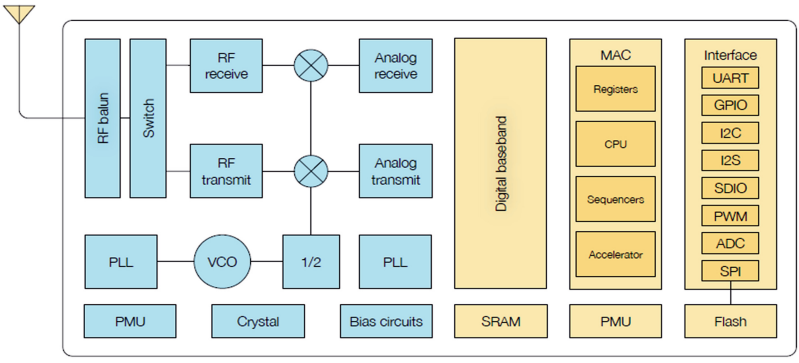

Fig. 3. Block diagram of WLAN module ESP8266EX [11]

too. The pins are required for the power supply, reset, chip-enable, firmware programming and the communication via UART. The firmware is externally loaded via SPI from Flash and it can be reprogrammed by the use of the UART interface.

4 Communication Network and IoT Application

The main purpose of the example application in this paper is to present a prototype platform for processing safe sensor data using a miniaturized safety system and transferring this data via wireless communication to other IoT devices. As already mentioned in the previous section, the safety system consists of a redundant processor system with integrated diagnostic units, and a communication system that serves as a black interference-free communication channel. The data that have been read out is processed and delivered to the RS232/TTL converter through a serial UART interface of the communication system. The converter regulates the voltage so that it will go down to 3.3 V and it forwards the data to the used WLAN module. As soon as one complete line has been transmitted, the WLAN module is going to respond with an echo and a reply. The communication system will then be in a position to verify whether the data were transferred correctly.

4.1 Example Test Design

Besides the module ESP8266-01, power supply, an RS232/TTL (15 V/3.3 V) converter and the system that communicates with the chip, are necessary for the experimental setup. Moreover, a button is used for the reset. An AMS1117 3.3 with 3.3 V is used for the power supply of the WLAN module and an AMS1117 5.0 with 5 V of Advanced Monolithic is used for the RS232-TTL converter. The RS232/TTL converter is an MAX2323 module from the company Maxim and has to be operated with 5 V. It should be noted that all modules share a common ground so that disturbances can be

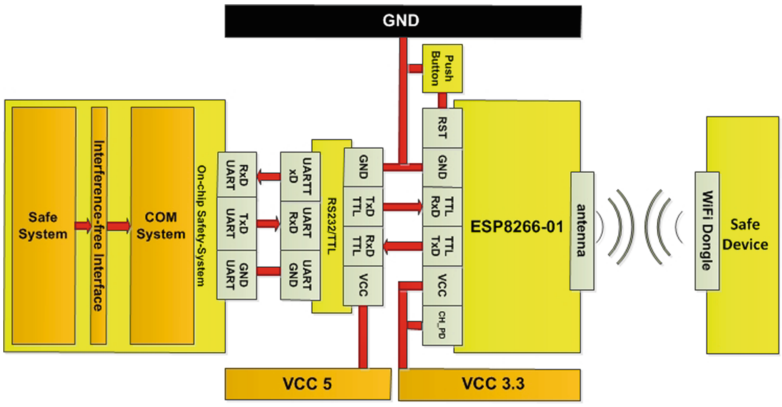

Fig. 4. Block diagram of a simple test design

prevented. The RxD/TxD signals are connected crosswise at the modules. The Baud rate is set to 115200Bd at all systems.

As soon as the system is switched on, the ESP8266-01 can be configured. The standard firmware runs with the AT-Instruction-Set. A connection between the safety system and the module has to be established via the UART interface. By entering "AT\r\n" it is tested whether the module is ready. If the answer "AT\r\nOK\r\n" is received, the system will be ready. Further information on additional commands can be found in the ESP8266 AT Instruction Set Version 1.5.4 on the website of Espressif [12]. The WLAN module can be configured as station, access point or as both at the same time. Figure 4 illustrates the block diagram of a simple test design.

4.2 Results and Evaluation

After having introduced the test setup in the previous section, the current section will be dealing with a brief introduction of the first results that have been obtained. An initial feasibility study has been carried out along with the introduced demo design. In this context, a validated Field Programmable Gate Array (FPGA) platform as realized served as prototype platform for the used on-chip safety system. A connection of the WLAN interface to the serial interface of the communication system has been realized and wireless communications with a host computer have been established successfully. Figure 5 shows a photo of the realized prototype.

Thus the first step in realizing the proposed concept was taken. Two crucial aspects have to be emphasized regarding future work. On one hand, there is the miniaturization of the system where the on -chip safety system is integrated together with the WLAN module on the smallest hardware structure, and on other hand there is the important aspect of dealing with the ability to guarantee a safe wireless communication, because without this aspect a complete system safety could not be achieved.

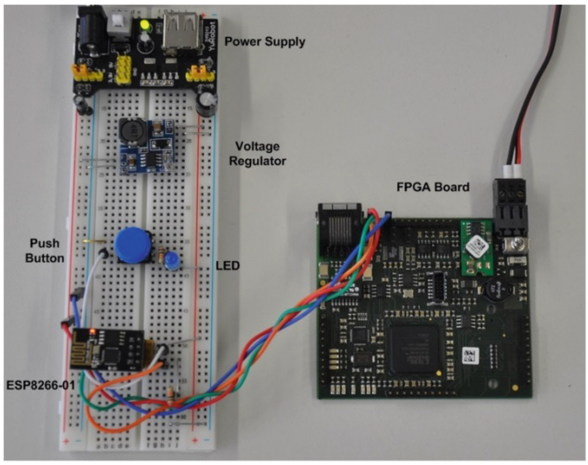

Fig. 5. Hardware prototyping platform with WLAN module and FPGA board

Miniaturization: A first hardware design has been implemented for the miniaturization of the test setup. Figure 6 shows the layout of the target hardware created in Cadence Allegro. The target hardware mainly consists of the on-chip safety system and the connection to the WLAN module. Further important units, among others, are the power supply and its monitoring as well as the circuit of an external Watchdog. Due to the size of 7 cm x 4 cm the realized design serves to provide the optimal platform for wireless, safe networks for IIoT applications. A long-term objective of our research work is to integrate the complete system on a single chip to achieve the first IIoT safety chip solution.

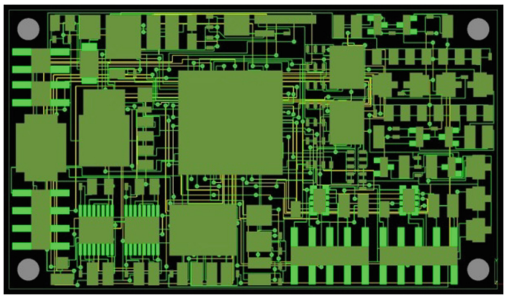

Fig. 6. Layout of an IIoT network

Wireless Safe Communication: For the purpose of ensuring a safe wireless communication, a significant addition to the introduced architecture is required. At first glance it seems as if there are two suitable options to provide conceivable solutions. Firstly, the wireless communication can be realized directly via the safety system, and secondly, it can be carried out in a redundant way via the communication processor. The first variant would imply two WLAN modules or two RF radio modules having two different frequencies, being connected to two serial interfaces or two SPI interfaces of the safety system accordingly. A conceptual diagram of this approach with both suggested communication modules is shown in Fig. 7. The advantage of this variant is that it results in two redundant communication channels that are processed by an equally redundant processor system. The technical challenges to be faced at that point would be the handling of the synchronization and the loss of performance at the safety system.

The second variant would imply two WLAN modules or two RF radio modules being connected to two different serial interfaces of the communication processor accordingly, exactly as shown in Fig. 7 above, but the communication modules will be connected to the communication system rather than to safe System. An appropriate comparison is also carried out there. The advantage of this variant is that the communication is still established via the communication processor and thus the performance of the safety system remains unaffected. However, a disadvantage is represented by the singularity of the communication processor. Diversity of the wireless interfaces e.g. using 2.4 GHz and 5 GHz and multiple comparisons depending on the targeted safety level represents appropriate measures to be adopted to solve this.

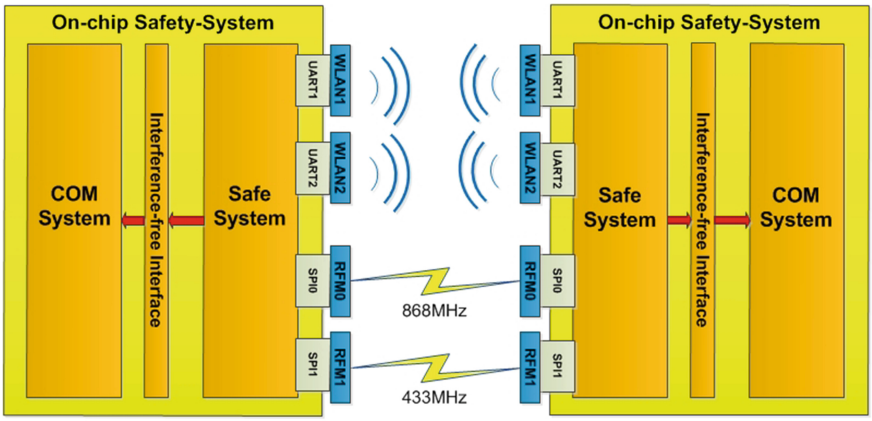

Fig. 7. Example layout of a safe IIoT network

In each case, a feasibly study for those proposed solutions and for other possible solutions will represent the main focus of further research on this topic, in addition to developing a suitable safe communication protocol to each suggested approach.

5 Conclusion

The background of IIoT and Industry 4.0 implies that better networking of industrial devices as well as increasing miniaturization and lower costs of hardware have to be achieved. In this context, the introduced concept presented in this work delivers a contribution to the realization of a miniaturized safety-related platform for the implementation in industrial IoT applications. The solution, which is presented in this paper, comprises the following steps: (1) Introducing an on-chip safety system, (2) Integrating wireless communication, (3) Designing a model for a communication network for safe IoT implementations and using example hardware. The presented solution represents a compact and flexible solution consisting of a miniaturized on-chip safety system and wireless communication for the use in safe industrial IoT applications. The feasibility of the presented example served to demonstrate the enormous potential of the IoT devices for the implementation in safety-related industrial applications. Furthermore, this paper deals with open suggestions for enhancements guaranteeing a safe communication, which are not yet fully developed. They are going to be elaborated and published within the scope of future research activities.

References

1. McEwen, A., Cassimally, H.: Designing the Internet of Things. Wiley, Chichester (2014)
2. Alcaraz, C., Lopez, J.: Diagnosis mechanism for accurate monitoring in critical infrastructure. Comput. Stand. Interfaces **36**(3), 501–512 (2014). Elsevier

3. Alcaraz, C., Lopez, J.: WASAM: a dynamic wide-area situational awareness model for critical domains in smart grids. In: Future Generation Computer Systems, vol. 30, pp. 146–154. Elsevier (2014)
4. Börcsök, J.: Electronic Safety Systems - Hardware Concepts Models and Calculations. Hüthig-Verlag, Heidelberg (2004)
5. Börcsök, J.: Functional Safety - Basic Principles of Safety-related Systems. Hüthig-Verlag, Heidelberg (2007)
6. International Electrotechnical Commission: International Standard: 61508 Functional Safety of Electrical/Electronic/Programmable Electronic Safety-related Systems Part 1–7. IEC, Geneva (1999–2010)
7. Hayek A., Boercsoek J.: Safety chips in light of the standard IEC 61508: survey and analysis. In: International Symposium on Fundamentals of Electrical Engineering (ISFEE), pp. 1–6. IEEE press, Bucharest (2014)
8. Hayek A., Boercsoek J.: Safety-related ASIC-Design in terms of the standard IEC 61508. In: The third International Conference on Performance, Safety and Robustness in Complex Systems and Applications (PESARO), pp. 16–21. IARIA press, Venice (2013)
9. Hayek A., Machmur B., Schreiber M., Boercsoek J.: Safety-related system-on-chip architecture for embedded computing applications. In: European Safety and Reliability Association Annual Conference (ESREL). ESRA press, Amsterdam (2013)
10. The Internet of Things: An Overview, Understanding the Issues and Challenges of a more Connected World (2015). http://www.internetsociety.org
11. Espressif Systems: Espressif Smart Connectivity Platform ESP8266. Espressif Systems Inc. (2013)
12. ESP8266 AT Instructions Set (2013). https://espressif.com/en/content/esp8266-instruction-set