Safety-Related Wireless Communication via RF Modules for Industrial IoT Applications

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

Department of Computer Architecture and System Programming,
University of Kassel, Wilhelmshöher Allee 71-73, 34121 Kassel, Germany
{samer.telawi,ali.hayek,j.boercsoek}@uni-kassel.de

Abstract. The major trend of *IoT* concept in the recent years is this technology being widely engaged into the industrial applications where the principles of critical safety are the essential concerns. Moreover, the great advantages and the rapid development of wireless communication technologies have driven them to form the backbone of *IoT* applications. Therefore, these wireless technologies must comply additional safety-related requirements in order to make their great features available for industrial applications. This research work is a complement work to the research introduced by Hayek et al. [1] and it describes a conceptual design of a safety-related wireless communication protocol based on *RF* technology, that fulfills the needed requirements as well as implements the safety approaches defined in the related safety standards to achieve all enhancements that make this technology suitable to be used in industrial internet of things applications.

Keywords: Frequency band · Frequency Hopping Spread Spectrum
Gateway · Industrial Internet of Things · Jamming
Safe communication · Safety integrity level · Safety-related
Sensor node · Threats · Wireless sensor networks

1 Introduction

The terminologies of smart and intelligent devices or systems that are being expanded and integrated in our daily life's details, such as smart homes, intelligent monitoring and transportation, represent systems that connect our physical world more than we ever imagined possible. These systems are commonly associated with the concept Internet of Things *(IoT)*, where through the utilization of different sensors types, the entire physical environments are coupled and connected closely in order to transmit a massive amount of sensory data via communication technologies. In such sophisticated systems used to provide intelligent monitoring, management and control, many embedded devices are interconnected to transmit the required information and instructions via distributed sensor networks. Consequently, a Wireless Sensor Network *(WSN)* defines the

G. Fortino et al. (Eds.): InterIoT 2017/SaSeIoT 2017, LNICST 242, pp. 96–112, 2018.
https://doi.org/10.1007/978-3-319-93797-7_12

large number of interconnected sensor nodes that are equipped with a big range of sensors to detect and capture different factors as well as physical conditions and phenomena such as temperature, pressure, humidity, gas, human body pointers, motion, vibration, etc.

However, the term Internet of Things was introduced by Kevin Ashton in 1999 [2] which recognizes all the objects that are uniquely identified and have their own virtual existence in an "internet-like" structure. There are tremendous possibilities for these objects, so they can be anything starting from large buildings, vehicles, planes, machines, any type of products, to humans and animals or even a specific part of their bodies.

As a matter of fact, both *IoT* and *WSNs* were developed in parallel, and while *IoT* does not require or assume any specific kind of the available communication technologies, the wireless technology have the capabilities to play the major and most important role in *IoT* applications. Furthermore, the *WSNs* are recognized as a revolutionary approach for capturing and gathering environmental data that is used to structure efficient and reliable systems. Moreover, their features such as flexibility, fast deployment of devices comparing with wired networks, rapid development, and availability of the inexpensive miniaturized low power consumption components like microprocessors, radios and sensors that are integrated together to form System on Chip *(SoC)*, lead to involve and integrate *IoT* in the smallest objects installed in any kind of environments and applications. This integration is the major evolution which drives *WSNs* to become the backbone and the key technology for *IoT*.

However, the wide utilization of industrial internet of things *(IIoT)* in different fields, where the safety of human is a critical issue, requires safety-related communication. Nowadays, variety of efforts focus on this promising field to have the advantages of wireless communication in the industrial applications and provide more sophisticated, reliable, and safe approaches that meet the safety requirements of different relevant international standards. This research work introduces a new approach to achieve the safe wireless communication based on providing hardware redundancy which requires redundant communication channels, in addition to the conceptual protocol that meets the standardized safety requirements and manages the redundant channels. This proposed approach targets the safety-related *IIoT* applications.

The next two subsections of this paper provide an overview about the key concept of *IoT* which is the wireless communication networks, also a review of the related research works is introduced. Section 2 of this paper roughly reviews the standardized requirements of safety related communications and how to integrate them in wireless communications. Section 3 explains how to overcome different challenges of the wireless sensor networks. Section 3.2 introduces the conceptual safety-related wireless protocol and Sect. 4 includes a summary of experiments and tests in addition to the conclusion of this research work.

1.1 Wireless Sensor Networks

Commonly, *WSNs* identify the type of sensor networks that utilize the wireless communication, and consist of a base station (gateway) and sensor nodes that capture the physical parameters or events and convert them into a digital representation giving us the ability to monitor the physical environment around us. A sensor network can be composed of one or a large number of sensor nodes partially distributed and deployed closely to the phenomenon or the event to be monitored. Consequently, the purpose of these nodes is to collect the relevant sensory data and route them back to the sink which will utilize this data.

Wireless sensor node integrates many capabilities such as sensing, on-board processing, communications, and storage together on a very small miniaturized board [3]. With these enhancements, a wireless sensor node can often play different roles in addition to the main role of capturing sensory data, such as in-network analysis which requires collaborating with other nodes in order to propagate the sensory data toward the base station, and fusion of its own sensory data with the data of other nodes. Sensor node in *WSNs* can have different variations, in that, it can be a simple sensor node to monitor a single physical factor or a complex device that combines many sensing techniques e.g., acoustic, optical, magnetic. Moreover, they can utilize different communication capabilities and technologies like ultrasound, infrared, or radio frequency.

WSNs have two different types according to their routing structure which is affected by the geographical distribution [3]:

(i) Single hop (Star Topology)
(ii) Multi hop (Mesh Topology)

Accordingly, *WSNs* offer many great advantages, such as reducing the mass and volume by eliminating cables, the wireless components can be embedded in different materials, the cost effective and rapid deployment of sensor nodes, the ability to penetrate many materials without the need of actual physical penetration, and in some applications the wireless might provide a redundant layer for functions that is insensitive to failures in the system structure. Hence, providing developers and designers with more flexibilities and abilities that might be very important in some industries like avionics systems, vehicles, and energy.

1.2 Related Work

WSNs have inspired the system designers to introduce a tremendous applications. Some of them are futuristic like the research work introduced by Alena et al. [4] which investigates and evaluates the *ZigBee* technology and its capabilities to be used in avionics and aerospace industry, while a large number of them are in use and practically useful. The applications in the latter category show a remarkable diversity according to the ability of *WSNs* in providing a continuous real-time autonomous data acquisition, a combined data from a wide variety of sensors, an improved data accessibility, a better data management, and the analysis of data to predict and prevent unlikely events. Such applications are noticeable in different fields of industries as the following:

(i) Home automation or smart home.
(ii) Emerging smart energy markets: like the smart network project to monitor the electricity usage of homes, which is carried out by *WEL Networks* the electricity distribution company in *New Zealand* [5].
(iii) Monitoring of underground working Environment: to detect and capture the environmental factors of the coal mines introduced by Tejashri et al. [6], and Raghram et al. [7].
(iv) Transportation: to monitor the physical environment of the railways introduced by Victoria et al. [8].
(v) Monitoring of human activities and health as in the work provided by Lu et al. [9].
(vi) Monitoring of nature such as active volcanoes, forests in order to protect them from fire as introduced by Jadhav et al. [10], weather, etc.
(vii) Monitoring of pipelines (water, oil, gas), structural health, supply chain management, etc.

Nonetheless, the mentioned research works introduce systems involved with the safety of human life; which is the most important concern; they only focus on showing the efficiency of using *WSNs* in such applications and they evaluate different factors and parameters of the systems, such as network topologies, communication quality, power management, and routing algorithms. Besides, these systems are not safety-related even those that are proposed to be used in hazardous working environments, conversely, the systems that are engaged in a critical environments and whose failure might endanger the human safety or the environment itself must be safety-critical systems, thus the systems must fulfill the safety requirements that consist of functional part and safety-integrity level *(SIL)* part which determines the required level of risk reduction [11–13], likewise, achieving a safe communication.

Meanwhile, many noticeable efforts are involved in introducing different approaches to provide safe wireless communication for industrial or human safety relevant applications, such as the *SafeCOP ECSEL* project that provides an approach to the safety assurance by use of safe wireless communication. This project implements the defined requirements in the well known standards e.g. *IEC 61508* [11], and *ISO 26262* [14] to achieve the safe communication. Furthermore, a remarkable effort is introduced by Pendli et al. in which the researchers provided a complete approach with all mathematical models and analysis for utilizing the *Bluetooth* technology and implementing the defined requirements in the mentioned standards to achieve the safe communication that can be used in safety-related systems [15,16].

However, the efforts that aim to achieve a safe wireless communication comply the safety requirements defined in different standards by adding a new safety-layer to the stack of the involved communication protocol, in that they mainly focus on implementing those requirements at the software layer. This research work introduces an approach to fulfill the safe communication by providing a hardware redundancy as well as the required improvements to the protocol to manage the safety communications and the redundant channels.

The next section provides an overview about the safety standards and fundamental requirements that are needed to be considered and integrated to achieve the safe wireless communications. These standards identify the challenges that form the sources of failures and errors in wireless communications, in addition to the proposed procedures and policies to overcome and manage these sources of errors.

2 Safety-Related Wireless Communications

Regarding the increased demand on safe communication for safety-related systems in industrial applications, the necessity to develop the available industrial network technologies that do not provide safe communication such as *Profinet*, *Interbus*, *Profibus*, *Ethernt* and *CAN-Open* comes into a considered meaning. Consequently, to achieve a safe communication these technologies have been developed and new versions have been issued accordingly as *Profinet-Safety*, *Interbus-Safety*, *Profibus-Safety*, *Safe-Ethernet* and *CANOpen-Safety*. These safety protocol fulfill the special requirements for safety-related industrial applications such as high reliability, high safety integrity level up to *SIL 3*. Nevertheless, the great advantages of the wireless communication it cannot totally replace the previous industrial wired technologies. But when the wireless communication become a mandatory requirement for some applications that need mobility or special physical structures in which the physical penetration for the cables is not likely, this technology must be analyzed to implement the safety methods according to the European standard *EN 50159-2* [17]. In that, two major issues must be taken into account in order to adopt the wireless communication in industrial safety-related applications, that are security and safety.

Although the safety standards and analysis frameworks of data communication were originally intended for wired network, they can also be implemented and applied to the wireless communications referring that the wireless communications do not produce any new types of errors, but the only differentiation is in the probabilities of errors [18]. The next subsection provides a rough summary about the required safety issues and standards to overcome the failures and errors produced by the wireless communications in order to achieve the safe communication.

2.1 Fundamental Requirements for Safety-Related Communications

The distributed nature of industrial Internet of things applications requires more effective and uninterrupted communication methodologies between all sensor nodes. Therefore, additional safety layers are added to fulfill the necessary special requirements that are fault tolerant and safety. When implementing safety-related applications, it is important to utilize two safe hardware ends that are the source and destination nodes in addition to the safe protocol. Moreover, all standards for functional safety demonstrate that the reliability of such systems is achieved by adopting redundancy in addition to the technical and non-technical

measurements for fault detection of the safety system, but redundancy is not sufficient to achieve faults free systems while this can be impaired by the random failures of single components, in that the best approach is to control these unavoidable failures based on a redundancy that does not lead to the failure or it can diagnose the failures so early [19,20].

The main challenges of a safe communication can be categorized according to their type into two categories [19,20]:

(i) Functional requirements of the process: this category concerns many factors such as the response time of the safety-related system controller, the amount of data that are needed to be processed and the operation mode of the application whether it should operate in a high or low demand mode.
(ii) Qualitative measures against failures: the most important issues in safety-related systems are the transmission errors, such as repetition of a message, loss of a complete message, insertion of an unwanted message due to an error, wrong sequence of messages, data corruption and delay.

Similarly, the standards of safe communications such as *EN 50159-1* and *EN 50159-2* describe the suitable defense methods to control and overcome the previews challenges. Table 1 shows descriptions of the threats and corresponding defense methods.

Furthermore, the concept of data integrity is considered as the most important challenge in the safety-related systems, thus this integrity can be assured using the redundancy method which assumes that both sender and receiver have two communication channels, and the received messages are compared to check the correctness of transmission. Hence, detecting any difference between the two copies of the same message represents an error. Adopting this hardware redundancy method eliminates and detects many threats such as retransmission, packet loss, malicious insertion and wrong sequence. Consequently, this hardware redundancy must implement one of the four defined architectural models [19–21], and these models that are presented in Fig. 1 describes how the channels are connected and the communication is managed over the adopted redundancy model through across different layers of the communication stack.

(i) Model *A* represents a single channel of controller for both safety-related end nodes.
(ii) A complete redundant system is described in model *B*, in which the safeguard and the transmission layers are designed dual. This model is adopted for this research work.
(iii) Model *C* corresponds to Model B with a single-channel transmission medium. The transmission layers and the safeguards are existed in both safety channels of the safety-related end node.
(iv) Model *D* presents two-canal link layers via a single-channel of transmission layer, and both link layers have the ability to access the transmission layer independently.

So far, the presented methods were introduced to provide safety for wired communication, but while the wireless communication does not produce any new

Table 1. Description of the defense methods against threats [22]

Defense method	Description	Threat
Sequence number	Each message is identified by a consecutive number	Repetition, deletion, insertion, incorrect sequence
Time stamp	Each message has the sending time	Repetition, incorrect sequence, delay
Source and destination identifier	Source and destination addresses are included in the message	Insertion
Acknowledgments	Receiver send sends a positive or negative acknowledgment	Insertion
Identification	Identity check must be done for all network members before the system starts up	Insertion
CRC cyclic redundancy check	CRC is calculated for the message bits and included with it	Corruption
Encryption	Apply authentication and add the cryptographic code into the message	Corruption, malicious attacks
Membership control	The network members monitor each other	Inconsistency
Atomic broadcast	To ensure that all sent messages are delivered in the same order to all receivers	Inconsistency
Hamming distance to addresses and message identifiers	To detect the case of single bit failure in the address or in the message identifier	Insertion

type of errors, these methods are capable to be adopted in the wireless communication technologies. Regarding the different physical transmission medium used in wireless communications more threats need to be considered, and the next subsection overviews these threats with the correspondence defense methods.

2.2 Safe Requirements for WSNs

Due to the broadcasting nature and the deployment of wireless sensor nodes, they are exposed to different types of threats that might affect the confidentiality, integrity and availability of sensory data. These threats are categorized based on the affected layer of the wireless communication protocol stack and the objectives into the following:

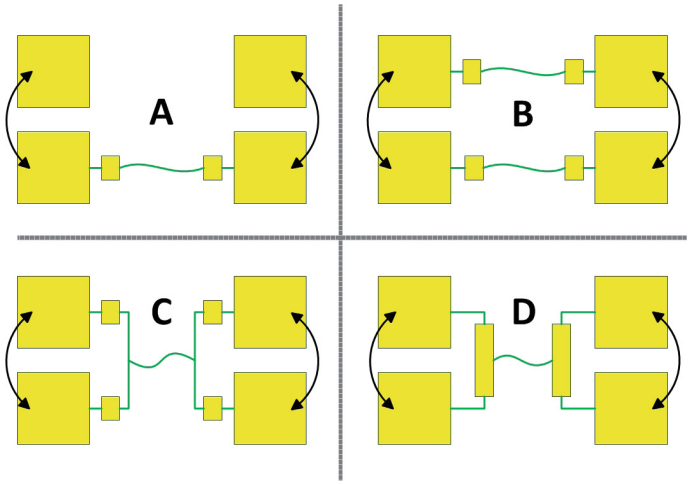

Fig. 1. Communication models

(i) Sabotage attack: *WSNs* are widely distributed making them an easy targets for different types of attacks. The first type called passive attack in which the attacker listens to the channel and steals the packets that may include important information, thus they only seek information without disturbing the communication or damaging the network, and this attack targets the higher layers of the protocol stack. The defense methods against this type of threat are encryption and keys management algorithms [3,23].

(ii) Denial of service attack: usually this type targets the physical layer which contains the operating frequencies, the capability to turn ON/OFF the transceiver and channel selection. However, the most spread type of such attack is jamming that disturbs the transmission communication by inserting a severe intervention to occupy the channels and block the receivers. Jamming attack either continuously emits a high energy signal on the channel in that always found busy by the sender, or transmits regular packets to force the receiver to receive junk packets all the time [24]. Hence protection against jamming attack requires an efficient prevention mechanism like Frequency Hopping Spread Spectrum *(FHSS)* where the data packets are transmitted with different carrier frequencies bands at different intervals of time. Therefore, the two parties have to go through a negotiation phase in order to agree on the switching sequence before the real data transmission starts [25].

(iii) Interference and multi-path: *RF* interference is the main reason for packet errors while it disrupts the ability to interpret received packets, also the existing of reflecting metals in the environment at which the wireless nodes are deployed is the main reason for duplicating the messages. It is possible to overcome these threats by using addressing and sequence number in addition to select the right carrier frequency band that has no interference.

The mentioned methods have to be implemented according to the required *SIL* applying the approaches defined in the standard *IEC 61508* that regards the probability of failure of the whole hardware of the system. These approaches will be defined in more details next section.

3 Concept of Safe Wireless Communication Using RF Modules

This section introduces in more details the proposed design of the safety-related wireless communication system for *IIoT* applications. The first subsection includes a short review about some required basic concepts, characteristics and approaches that are involved in achieving the target system according to the standard *IEC 61508-2*. The second subsection introduces the hardware components as well as the software design and how the safety requirements for safe communication are managed in both software and hardware. Finally, the last section summarizes some experiments conducted by the researchers to test the conceptual system.

3.1 Safety-Related Concepts and Approaches

The digital systems designed to operate in safety-critical environments must comply some functional, nonfunctional, and technical conditions; in particular fail-safe architecture, reliability and fault-tolerance. The reliable system requires to implement hardware redundancy which integrates more components than required to perform the same function. In case of failure in one component the system will switch into a defined safe-mode after activating the correspondence replacement of the failed component. The fail-safe architecture is the frame which holds the previous concepts, and the safety structure *X out of Y* in which *Y* stands for the existed number of independent paths; the path is a group of hardware components responsible to perform specific function; while *X* is the minimum necessary number of paths for the system to operate correctly. Consequently, the adopted structure of the investigated system in this research work is *1oo2* where one of the two channels is sufficient for the safety function to fulfill its task [12,13].

Designing of the communication system is a combination of hardware and software. Therefore, the methods of *IEC 61508-2 (hardware)* and *IEC 61508-3 (software)* should be satisfied to achieve a safe communication. The standard *IEC 61508-2* addresses that when implementing a safety function that requires any form of data communication the probability of undetected failure of the communication process must be calculated considering the previously mentioned threats. This probability is taken into account when estimating the probability of dangerous failure of the safety function. Moreover, two approaches were defined in this standard:

(i) *White channel:* all the subsystems hardware as well as software used in safe communication should meet the relevant requirements of *IEC 61508*.

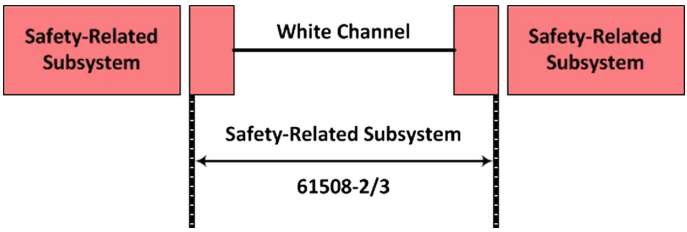

Fig. 2. White channel approach [22]

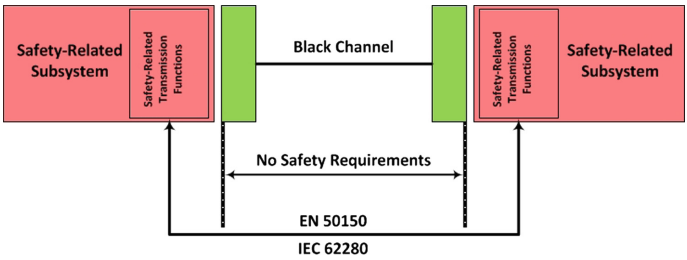

Fig. 3. Black channel approach [22]

Figure 2 shows a block diagram for the concept of a white channel that is adopted in this research work.

(ii) *Black channel:* the required measures to provide a safe data communication are implemented in the subsystems that represent the sender and the receiver. Thus, there are no safety requirements on other part of the safety-related communication systems. The concept of black channel approach is shown in the term of block diagram in Fig. 3. This is the approach of standards *EN 50159-1,-2*, *IEC 62280* and it was extended in *IEC 61508* to include the calculations of probability of dangerous failures.

The next subsection provides a detailed overview about the target safe communication system, in that the utilized hardware components are introduced and how they are integrated together in order to fulfill the safety requirements and implement the adopted standardized approach in order to achieve the safe communication functionality.

3.2 Conceptual Safe Wireless Communication System

This research work utilizes a *SIL 3* safety-related chip which integrates two subsystems together, the first subsystem is the safety system and it includes two processors in order to achieve the *1oo2* safe-architecture as well as a hardware comparator between these two processors that is responsible to provide diagnosis functionality, in that achieving an enhanced safe-architecture which is *1oo2D*. Furthermore, the second subsystem in this chip is the com system that

includes only one processor and it is responsible to provide the safe part of this chip with the required communication interfaces with the external environment implementing the approach introduced in Fig. 3. All of these components are integrated together on a single chip to form a System on Chip.

Accordingly, in order to provide the physical wireless transmission medium for the safety-related chip, the *RFM69* modules are used where they provide many features drive them to be suitable solution for high performance sensor networks, such as the extremely low-cost solutions, very small size, low mass, narrow-band and wide-band communication modes, the major parameters of *RF* communication are programmable, lower power consumption, two transmission modes (continuous and packet), *SPI* communication interface, and the most important that is the module provides some built in functions that fulfill the safe requirements [26].

Furthermore, in order to complete the structure of the wireless sensor node an acceleration sensor is used and combined with the safety-related chip. Thus, any type of sensors can be used even the node can combine more than one type of sensors to be able to detect more than one factor of the monitored environment. However, regardless what sensor type is used to build up this node, these sensors must be structured according to *1oo2* safe-architecture.

This research work starts with the simplest structure of the wireless sensor network that consists of only two ends, the gateway and the sensor node. As mentioned previously in order to achieve a safe communication both ends must be safety-related designed, in that the hardware redundancy is achieved by implementing the *1oo2* safe-structure along the path from the source to the sink according to the white channel approach shown in Fig. 2. The detailed design of this conceptual system is presented in Fig. 4 that shows the safety architecture of both safety-gateway and safety-node in addition to the safe wireless communication. According to the white channel approach this whole system consists of three safety-related subsystems:

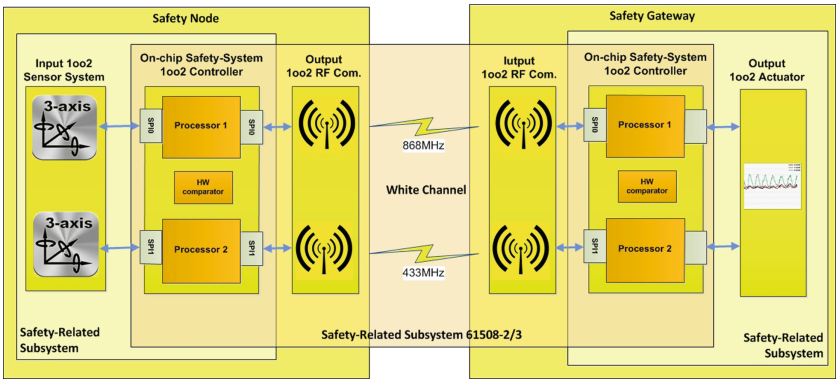

Fig. 4. Structure of the safe wireless communication system

(i) The first subsystem exists in the safety node and it includes the safety-related sensor system and the safety-related controller which is implemented in the utilized safety-chip. Each sensor is interfaced with a specific processor in the controller via an independent *SPI* interface fulfilling the *1oo2* architecture to obtain a safe sensory data.
(ii) The second subsystem exists in the safety gateway and similarly it includes the safety-related controller that is connected to some safety-related actuator via some interface.
(iii) The third subsystem exists in both safety ends and it includes the communication parts of both sides. This communication part consists of two *RFM69* modules connected via *SPI* interfaces independently to each processor in the controller according to safe-architecture *1oo2*. Besides, one *RF* module operates at frequency band of 868 MHz and the second one operates at 433 MHz to implement; with cooperation of the *RF* modules on the other end; a redundant communication channel. These two communication parts on both ends represent the white channel approach.

However, each end in the presented design can be viewed as a sequence of input-controller-output. Thus, for safety node the *1oo2* sensor system represents the input, the safe part of the safety-related chip represents the *1oo2* controller, the *RF* communication represents the *1oo2* output. Likewise, for safety gateway the *RF* communication represents the *1oo2* input, the safe part of the safety-related chip represents the *1oo2* controller, and the safe actuators represent the *1oo2* output.

Figure 5 presents a prototype of the introduced system where all involved hardware components are integrated together and the *RFM69* modules are

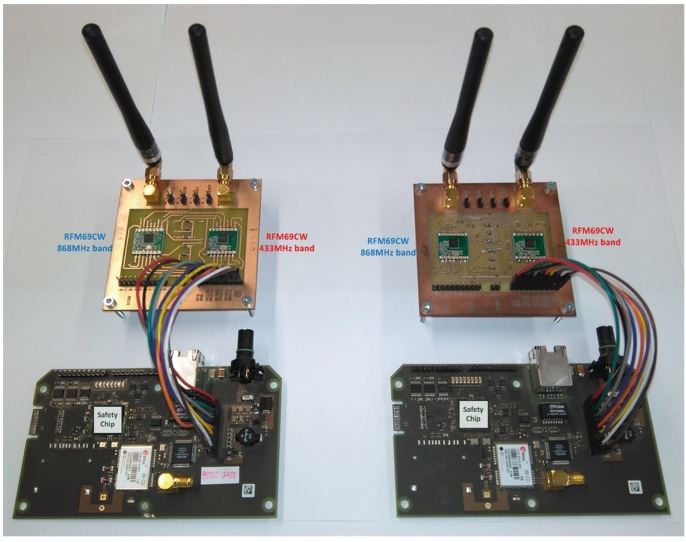

Fig. 5. Prototype of safe wireless communication system

mounted to a board with correspondent antennas, in addition the second board includes the safety-related chip and the acceleration sensors. Besides, the two boards are interfaced together via *SPI* using wires.

Table 2. Frequency bands ranges [26]

Frequency band	Min	Max
433 MHz	424	510
868 MHz	862	890

However, the denial of service attack based on jamming is one of the most important challenges that this system must overcome using one of the proposed defense method such as frequency hopping in which the underlying basics are to change the carrier frequency to assure that the data is transmitted over one frequency band for a short time. Therefore, the frequency band of the transceiver should be divided into channels and the communication protocol will hop between these different channels with respect to the hopping period and the sequence pattern of the channels. However, this research work utilizes two *RF* modules operate at two different frequency bands 433 MHz and 868 MHz where their possible frequencies are shown in Table 2, so these two bands can be divided into different number of frequency channels based on the utilized step which can be one of the next values 200 kHz, 1 MHz, 5 MHz, 7 MHz, 12 MHz, 20 MHz, 25 MHz [26]. Thus the suitable number of channels and the hopping period will be determined based on experiments while many issues should be considered such as response time, processing load, and complexity.

Regarding, the previous issues and the great built-in functionalities of *RFM69* modules, the challenges and the requirements that this system must overcome and comply accordingly are managed and distributed between hardware and software as presented in Table 3.

Furthermore, the wireless communication protocol for this simple network structure where only two ends are involved, should follow different phases before the transmission of safe sensory data starts. However, at the beginning when the wireless sensor node is powered up it is considered as an orphan and autonomous node while it is not a member yet of any network, then this node should broadcast a join request packet with a predefined identification code to enable the wireless gateway to recognize this node and answer back with an acceptance and a specific *ID* of this node. Next the node accepts the *ID* and acknowledges the operation to move into the next phase that is negotiation about the parameters of this communication channels and so on. Regarding the existence of two frequency bands, the protocol can follow different scenarios to structure the network like broadcasting on one channel or two channels at a specific frequency.

While the *RFM69* is designed to build the data packet automatically after the processor writes payload data into the *RF* module buffer and triggers the transmit mode, in that any other functionality like sequence number or message

Table 3. Implementation of defense methods against threats

Defense method	Implementation	Description
Sequence number	Software	Monitor the messages received on both channels
Time stamp	Software	Should be synchronized between both ends at startup
Source and destination identifier	Hardware/Software	RFM69 provides 8-bytes for network ID and 1-byte for node ID, more Flags can be added in software
Acknowledgments	Software	Each packet type should have a special Acknowledgment
Identification	Software	Not needed with the simple structure of networks
CRC cyclic redundancy check	Hardware	RFM69 provides 2-bytes for CRC
Encryption	Hardware/Software	Hardware: a symmetric-key block cipher to provide cryptographic, 128-bit long fixed key. Software: encryption models and schemes [23]
Membership control	Software	When there is no available data to transmit
Atomic broadcast	Software	Not needed with simple network structure
Hamming distance	Software	Monitor bit failure in addresses
Keys management	Software	At startup key should be negotiated
Denial of service (Jamming)	Software	Frequency Hopping Spread Spectrum: hopping pattern is negotiated at startup

type should be added into the payload before writing them into the *RF* buffer. Consequently, different types of messages can be defined and recognized based on their unique code, such as joint request, acknowledgment, battery level, sensor message, etc. Moreover, on the receiving side also many scenarios can be followed based on the application requirements, for example the basic scenario is the node should receive the same correct message on both channels otherwise the system must trigger the safe mode. But it might be accepted in case of losing one communication channel for some reason to inform the other end by using the second available channel to recover the lost one by following some procedure like changing the frequency. Furthermore, an important factor need to be considered which is the synchronization among both communication channels, in that many experiments are needed with respect to response time.

3.3 Experiments and Tests

The software part of this prototype for a safe wireless communication system is still under development. Moreover, the utilized safety chip provides a certified *SIL3* software package that includes an operating system and a middle ware to enable the developer to use all the safety functions provided by the chip, in that the application of this protocol is written using this software package. Consequently, some basic experiments were performed to check the capability of this prototype to function correctly, in that the researchers tested each channel independently and the transmission is successfully fulfilled, in addition, the redundant communication is also tested successfully. However, some packet errors were detected, but changing the cycle time of each transmission and improving the code reduced this error rate. Besides, the frequency bands of the redundant channel are detected by utilizing *RTL SDR* radio receiver which captures and converts the analog signal into digital data to be visualized with a supportive software called *SDRsharp* as illustrated in Fig. 6. The left part shows the captured signal for 868 MHz band and the right part shows the captured signal for 434 MHz band. The continuous development process of the software requires more experiments such as permanent monitoring of packet errors, investigating the values of Received Signal Strength Inductor of the receiver *(RSSI)*, testing the frequency hopping functionality, monitoring the behavior and response time in case of errors, and investigating the influence of metal parts on the transmission procedure such as positioning the node inside a metal box.

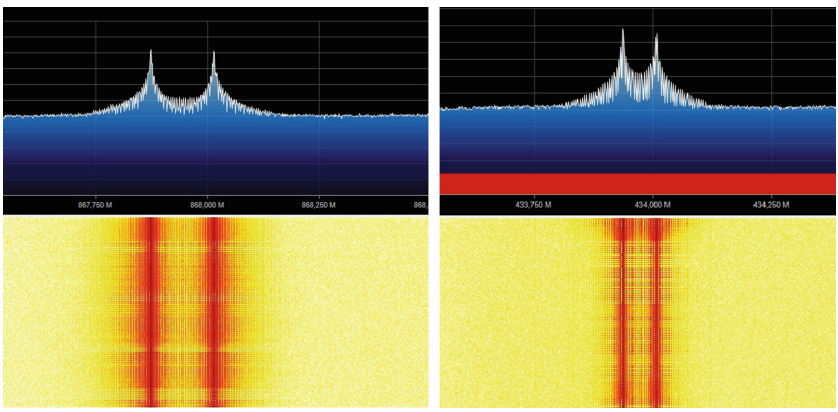

Fig. 6. Frequency bands of redundant communication

4 Results and Conclusion

The introduced prototype has revealed a potential capability to provide a robust safe wireless communication utilizing the *RF* technology which opens a wide range of opportunities for *IoT* to be used in industrial applications especially

with those that are criticized as safety-related applications and where the safety of human life is the major concern, in addition to the efficiency in providing an effective cost system with safe functionality.

Moreover, there are many challenges that can be outlined as a future work for this research such as enhancing the communication protocol to manage the other topologies of the networks such as star and mesh with concerning the ability to handle the mobile sensor nodes that are mounted on some moving objects like robots or vehicles. Furthermore, this prototype introduces the main frame for designing another prototype for a new wireless safety-chip that includes all the components in one miniaturized single chip to form a system on chip, hence making this system a great option for applications such as safe monitoring of human motion.

The unique design of the utilized safety chip that includes three processors; two of them represent the *1oo2* safety-system and the third one represents the com system; opens a new potential opportunity to introduce another design involving the com processor, in that the safe part of this chip will be responsible only for obtaining the safe sensory data while the safe communication functionality will be moved into the com processor that will transmit the same message via the redundant channel, but this approach requires the com processor to perform some other functions like comparing to assure the data integrity. Figure 7 shows a rough design of this new approach.

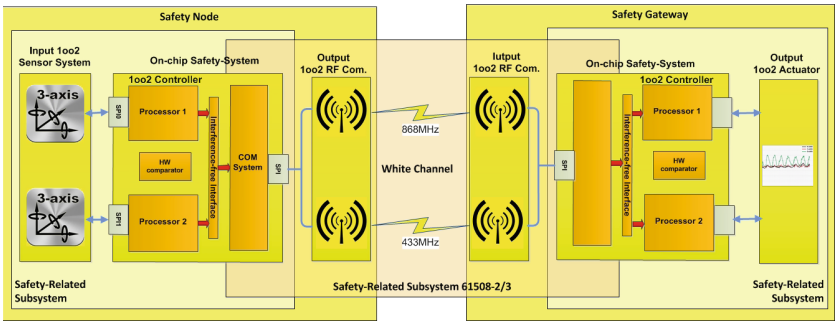

Fig. 7. Safe wireless communication with both parts of the safety chip

References

1. Hayek, A., Telawi, S., Bieler, C., Börcsök, J.: Adoption of miniaturized safety-related systems for industrial internet-of-things applications. In: 3rd EAI International Conference on Safety and Security in Internet of Things, Paris (2016)
2. Shu, Y., et al.: Internet of Things: Wireless Sensor Networks. IEC Market Strategy Board, Beijing (2014)
3. Waltenegus, D., Christian, P.: Fundamentals of Wireless Sensor Networks Theory and Practice. Wiley, Chichester (2010)

4. Richard, A., Ray, G., Jarren, B., Thom, S., Pete, W.: Fault tolerance in ZigBee wireless sensor networks. In: IEEEAC Paper #1480 (2010)
5. Samrtbox project. https://www.wel.co.nz
6. Tejashri, D.D.: Application of the wireless sensor network based on ZigBee technology in monitoring system for coal mine safety. Int. J. Eng. Res. Manag. (IJERM) (2015). ISSN: 2349–2058
7. Raghram, P., Veeramuthu, V.: Enhancing mine safety with wireless sensor networks using ZigBee technology. J. Theor. Appl. Inf. Technol. **37**(2), 261–267 (2012)
8. Victoria, J.H., Simon, O., Michael, W., Anthony, M.: Wireless sensor networks for condition monitoring in the railway industry: a survey. IEEE Trans. Intell. Transp. Syst. **16**(3), 1088–1106 (2015)
9. Lu, J., Van Den Bossche, A., Campo, E.: An IEEE 802.15.4 based adaptive communication protocol in wireless sensor network: application to monitoring the elderly at home. Wirel. Sens. Netw. **6**, 192–204 (2014)
10. Jadhav, P.S., Deshmukh, V.U.: Forest fire monitoring system based on ZIG-BEE wireless sensor network. Int. J. Emerg. Technol. Adv. Eng. **2**, 187–192 (2012). ISSN: 2250-2459
11. IEC 61508: Functional safety of electrical/electronic/programmable electronic safety-related systems. International Electrotechnical Commission (2010)
12. Josef, B.: Electronic Safety Systems Hardware Concepts, Models, and Calculations. Hüthig GmbH and Co. KG, Heidelberg (2004)
13. Josef, B.: Functional Safety. Hüthig GmbH and Co. KG, Heidelberg (2004)
14. ISO 26262 - Road vehicles-functional safety. International Organization for Standardization/Technical Committee 22 (ISO/TC 22) (2009)
15. Pavan, P., Michael, S., Hans, W., Börcsök, J.: Safe wireless communication for safety related systems. In: Recent Advances in Circuits, Systems and Automatic Control (2013). ISBN: 978-960-474-349-0
16. Pavan, P., Michael, S., Hans, W., Börcsök, J.: Wireless communication modeling for safety related system. Int. J. Circ. Syst. Sig. Process. (2014). ISSN: 1998-4464
17. EN 50159–2: Safety-related communication in open transmission system. European Committee for Electro Technical Standardization
18. Howlader, M.K., Dionand, J., Ewing, P.D.: Issues associated with deploying wireless systems in nuclear facilities. In: NPIC and HMIT, Las Vegas, Nevada (2010)
19. Börcsök, J.: Introduction in Safety Bus Systems. HIMA Paul Hildebrandt GmbH + Co KG, Brühl
20. Börcsök, J., Michael S.: Principles of safety bus systems. In: Proceedings of the International Conference on Networking, International Conference on Systems and International Conference on Mobile Communications and Learning Technologies (ICNICONSMCL 2006) (2006)
21. FAET; FAEM III, BIA, Proposal of a Guideline for the Test and Certification of "Bus Systems for the Transmission of Safety Relevant Messages" Stand, 28 May 2000
22. Jarmo, A., Marita, H., Timo M.: Safety of digital communications in machines. In: VTT Industrial Systems (2004)
23. Sklavos, N., Zaharakis, I. D.: Cryptography and security in Internet of Things (IoTs): models, schemes, and implementations. In: 8th IFIP International Conference on New Technologies, Mobility and Security (NTMS), pp. 1–2 (2016)
24. Avionics Department: Electronic Warfare and Radar Systems Engineering Handbook, 4th edn. Wiley, Chichester (2013)
25. Andreas, F.M.: Wireless Communications, 2nd edn. Wiley, Chichester (2011)
26. HOPERF ELECTRONIC: RFM69 ISM Transceiver Module Datasheet V1.1