Wireless Communication Modeling for Safety Related Systems

P.K. Pendli, M. Schwarz, H.D. Wacker, and J. Boercsoek

***Abstract*—**This paper deals with the modeling of wireless communication for safety related systems. To achieve safe wireless communication for safety related systems, the wireless channel is modeled by taking into account both bit errors and erasures (loss of information) that occur during wireless transmission of the information. To reduce the bit errors and to detect the erasures, a coding method for transmitting the code word is suggested in this paper. With this coding method, parameters such as bit error, probability of undetected error are reduced and the bit erasures that occur due to fast fading and channel losses are detected confidently.

The safety methods as defined according to the European standard EN 50159-2 are taken into consideration and their implementation to achieve safe wireless communication for safety related systems is explained in this paper. The mathematical derivations to calculate the probability of failures per hour (PFH) values for wireless communication with the suggested coding method are derived. With the derived PFH equation, safety integrity level (SIL) achieved for a particular wireless technology can be determined. Finally, the SIL levels achieved for Bluetooth technology are shown.

***Keywords*—** Safety Related Systems, Safe Wireless Communication, Safety Methods, Wireless Communication Modeling.

I. Introduction

IN industries, communication between the field bus/devices, PLC's/Controllers and System/Applications is normally achieved by industrial wired communication protocols such as PROFIbus, Profinet, INTERBUS, CAN and Ethernet. To achieve safe communication for safety related systems, these protocols have been further developed as PROFIsafe, Profinet Safety, INTERBUS Safety, CAN Open Safety and Safe Ethernet [1]-[5]. These safe protocols provide higher reliability, higher SIL (Safety Integrity Level) levels and safe communication.

At present in research institutes, industrial applications, automation, automotive industries, health care and medical applications the interest is increasing to use wireless communication technologies in place of wired communication technologies [6]-[10]. Of course, wired communication cannot be completely replaced, but to have the advantages of wireless communication such as network architecture flexibility, mobility, economical advantages, and based on the application requirements, the demand to use wireless communication technologies is largely growing [11].

To achieve safe wireless communication, safety related systems demands the wireless communication links to be reliable, timely delivery of the information without failure, real-time performance, robustness, optimized performance, optimized throughput, latency, power consumption, range of all these together or a combination of any of these. These demands depend on noise, interference and fading effects of the wireless communication channel which in turn depend on the parameters such as SNR (Signal to Noise Ratio), BER (Bit Error Ratio), Bit Erasure and Probability of undetected error. These parameters determine the PFH (Probability of Failure per Hour) value and based on this value, the SIL level achieved is determined.

For wireless communication, due to noise, interference and fading effects SNR is reduced, BER, Bit Erasure and Probability of undetected error are more and which cannot be avoided, but techniques should be implemented to reduce them so that the most accepted SIL level (SIL3 (for industrial applications)) for safety related systems is achieved.

In order to utilize a particular wireless communication technology for safety related systems i.e. to achieve safe communication, the technology has to be analyzed and further developed. Wireless communication channel should be modeled so that bit errors and bit erasures are taken into account and the measures to reduce the bit errors and to detect the bit erasures that occur during wireless transmission of the information should be implemented. In this paper, modeling of the wireless communication channel for safety related systems is presented. The safety methods as defined according to the European standard EN 50159-2 [12] are explained. As an example, Bluetooth technology implemented to achieve safe wireless communication for safety related systems is explained and the SIL levels achieved are shown.

The structure of this paper is as follows: section 2 explains wireless transmission with its advantages, security and safety issues and measures that are needed to overcome these issues. The implementation of safety methods as safety measures is

P. K. Pendli is with the Department of Computer Architecture and System Programming, University of Kassel, Wilhelmshoeher Allee 71, 34121, Kassel, Germany (e-mail: p.pendli@uni-kassel.de).

M. Schwarz is with the Department of Computer Architecture and System Programming, University of Kassel, Wilhelmshoeher Allee 71, 34121, Kassel, Germany (e-mail: m.schwarz@uni-kassel.de).

H. D. Wacker is with the Department of Computer Architecture and System Programming, University of Kassel, Wilhelmshoeher Allee 71, 34121, Kassel, Germany (e-mail: Hansd.wacker@uni-kassel.de).

J. Boercsoek is the chair of the Department of Computer Architecture and System Programming, University of Kassel, Wilhelmshoeher Allee 71, 34121, Kassel, Germany (e-mail: j.boercsoek@uni-kassel.de).

explained. Section 3 explains safe packet with safety layer implementation. Section 4 explains wireless communication modeling with mathematical derivations to achieve safe wireless communication for safety related systems. In section 5, the conclusions of this paper are presented.

II. Wireless Transmission, Advantages Issues and Measures

At present in portable, mobile computing and communicating devices such as smart phones, smart pads, cameras, printer, fax machine etc, transmission of the information with wireless communication i.e. with radio transmission is achieved successfully. In Industries, for example wireless communication between field-bus/devices and PLC/Controllers is also used, but the communication is not safe for safety related systems or applications.

The advantage of wireless communication for safety related systems are that the wireless networks provide flexible standard interconnection with wired or different wireless systems [11], flexibility of extending the network easily [13], self-reconfiguration of the network with minimal implementation and maintenance costs and mobility to wireless users or systems in the network [13]. For application like Automatic Guided Vehicles, and for applications in chemical and manufacturing plants, where chemicals, vibrations or moving parts could damage cables, wireless communication is the best solution [13]. In some situations to install cables, breaking walls is the only option left; in such cases, wireless communication provides economical advantages. Costs of wiring are reduced with almost zero cabling costs [13]. These advantages can be considered as the disadvantages of wired communication technologies.

A. Wireless Communication Security and Safety Issues

Security and safety issues are the two major problems that have to be overcome and they should be particularly taken into consideration, during modeling and analysis of the wireless communication architecture. Developing appropriate wireless communication architecture to achieve safety and security measures is extremely important for safety related systems.

Securing wireless communication is to provide confidentiality of the information. For systems with wireless communication due to eavesdropping, the requirement to achieve security plays a major role. Due to the broadcasting nature of the wireless communication, it is difficult to achieve secured wireless communication, as it makes easy to eavesdrop on the ongoing communication.

Security for wireless communication can be achieved by applying security measures at the physical layer, Media Access Control (MAC) or the application layer of the communication protocol stack. There are many research papers explaining the methods to achieve security. For example, at the physical layer security measures depend on the characteristics of the wireless channel such as noise, interference and fading effects, and they can be achieved by inherited spread spectrum techniques such as FHSS or DSSS schemes, or through the design of smart antennas, or through the key distribution for access control or key management schemes [14]-[19].

At MAC, higher layers or the application layer security can be achieved by applying appropriate encryption and authentication mechanisms. For example, MAC security measure can be achieved by the authentication of MAC address, higher layers or the application layer security measures are achieved by encryption techniques such as Cryptography, Internet Protocol Security (IPSec), IP tunneling (encapsulation), Hash function etc. [14]-[19].

This paper is mainly concerned to overcome safety issues or to achieve safe wireless communication for safety related systems.

B. Safety Measures with Safety Methods

During wireless transmission of the information, transmission errors and erasures are of great importance to safety related systems. EN 50159 is the European standard for "Railway applications - Communication, signaling and processing systems" and part 2 of the document specifies safety related communication in open transmission systems [12], [20]. This standard lists the causes of transmission errors and erasures that occur during wireless transmission of the information through the wireless channel. The causes include repetition, loss or deletion, insertion, wrong chronological sequence, data falsification and transmission delay [12].

To overcome these causes, in the same EN 50159-2 document, safety measures with safety methods against the transmission errors and erasures are listed [12]. The safety methods include sequential numbering, timestamp and timeout, acknowledgement, identification, data safety and redundancy with cross comparison. These safety methods are discussed in detail in the references [12], [20].

III. Safe Packet and Safety Layer Implementation

To achieve safe wireless communication for safety related systems with a particular wireless technology, the technology has to be analyzed for the safety methods implemented. These safety methods can be implemented in the standard packet as safe packet. If the implemented safety methods by a particular wireless technology are not sufficient, these methods can be implemented independently as a separate safety layer on the top of the protocol layer. The safe packet and safety layer implementation are explained in this section.

A. Standard and Safe Packets

Fig. 1 shows the transmission of a standard packet and a safe packet with the safety methods implemented. In the safe packet, the implemented safety methods perform the following actions to overcome the transmission errors and erasures.

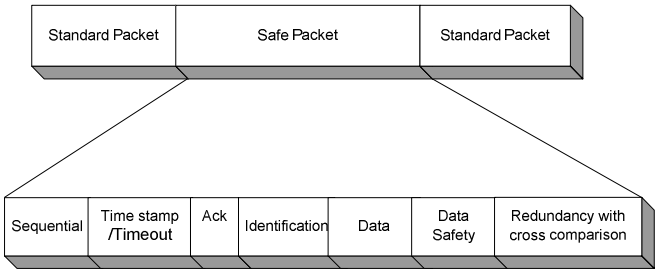

Fig. 1: Standard and safe packet with safety methods

Safe packet with safety methods [12], [20]:

1) Sequential numbering: This method assigns a sequence number to each packet so that the numbering is incremented from packet to packet in a defined way.
2) Timestamp (Ts) and Timeout (To): Time stamp method adds time stamp to each packet, which contains the time at which the transmitter creates a packet for transmission and timeout sets the limit for transmission.
3) Acknowledgement: This method acknowledges the transmission after the successful reception of a packet.
4) Identification: This method identifies the transmitter and receiver by recognizing a specified identifier added to the packet.
5) Data safety: This method tests the data content of a packet for correct transmission at the receiver, for example Cyclic Redundancy Check (CRC) and Hamming code.
6) Redundancy with cross comparison: This method testes the redundant data transmission for correctness in order to overcome retransmission, loss, insertion and wrong sequence errors.

B. Safety Layer with Safety Methods

To utilize a particular wireless communication technology for safety related systems, the technology for the implementation of the safety methods as discussed above should be analyzed. One method to implement these safety methods for safety related systems is to consider the communication channel as a so-called ‘‘Black Channel’’ [21].

The concept of ‘‘Black Channel’’ means that all safety-related functions will be designed outside on the top of the communication layers. The safety measures to avoid transmission errors and errors will be designed in a separated safety layer that is situated between communication protocol and the application layer as shown in Fig. 2.

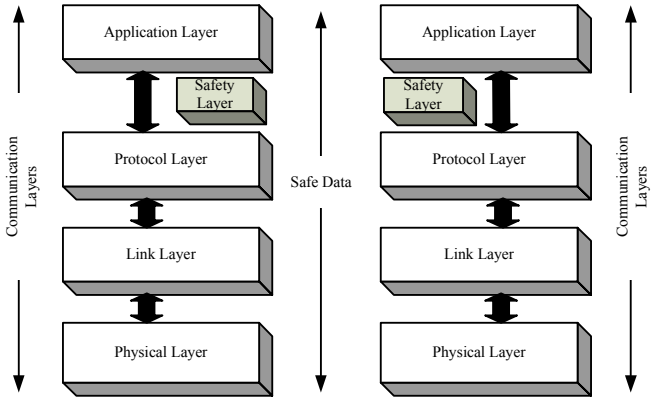

Fig. 2: Communication layers with safety layer

The implemented safety methods in the safety layer should be independent to the standard safety methods. For example, for a particular wireless technology, if the implemented data safety method is a 16-bit CRC at the lower packet layer of the communication protocol stack and if this CRC is not sufficient to achieve safe wireless communication, the data safety method has to be implemented with a 32-bit CRC code at the safety layer. The implemented safety method should be independent to the standard 16-bit CRC.

With this principle, an existing communication system can be used as it is and the data transmitted from upper/lower layers is considered to be safe data. Such solutions also exist for several wired field bus protocols e.g. PROFIsafe, Profinet Safety, INTERBUS Safety, CAN Open Safety and Safe Ethernet [1]-[5].

IV. Wireless Communication Modeling and Derivation

For Wireless communication, modeling both the bit errors and bit erasures (loss of information) that occur during the wireless transmission of the information should be taken into account and the wireless channel should be modeled accordingly. During the modeling of the wireless channel, it should be made sure that the bit errors are reduced and the bit erasures are detected, so that safe wireless communication can be achieved for safety related systems.

For mathematical derivations and calculations, for wired communication there are two parameters that are taken into consideration, Bit Error Ratio (BER) given by the symbol (ε), and probability of undetected error (P_{ue}) [22], [23]. For wireless communication, due to loss of information, a third parameter bit erasure is introduced given by the symbol (φ). With wireless communication, these parameters are normally high which makes the communication unsafe.

Avoiding errors and erasures in a wireless communication is not possible, but the errors can be reduced and the erasures can be detected, for this purpose a coding method is described in this paper to reduce the bit errors, P_{ue} and to detect the bit erasures that occur during wireless transmission of the information.

A. Wireless Communication Channel Model

To take into consideration the bit error and erasure effects, the wireless communication channel is modeled in this paper as a serial concatenation of BSC channel and BEC channel. The example of BSC channel is taken as a Gaussian channel and BEC as defined by author Peter Elias [24] as Elias erasure channel as shown in Fig. 3.

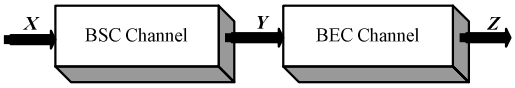

Fig. 3 BSC-BEC channel model

In Fig. 3 BSC is considered as a channel, which corrupts a binary signal by reversing each bit with a fixed probability. The erasure channel is a very simplified model of a fading channel where parts of the code word are completely erased (bits are lost rather than corrupted) by a deep fading of the channel. This type of channel model corresponds to the large bit error ratio due to noisy channel (BSC channel) and fading of the signal due to erasure channel (BEC channel). For real wireless communication systems, it is very important to consider both the effects of noisy and erasure channels.

The channel output of this model is given as $Z = X + AY$, where A is the fading or erasure coefficient. The transition probabilities for the BSC noisy channel and erasure channel are given as:

$$P(1|0) = P(0|1) = \varepsilon, \quad P(0|0) = P(1|1) = 1 - \varepsilon \quad \text{(Noisy-channel)} \tag{1}$$

$$P(e|0) = P(e|1) = \varphi, \quad P(0|0) = P(1|1) = 1 - \varphi \quad \text{(Erasure channel)} \tag{2}$$

With this channel model and with single code word transmission, as the bits are lost (erased) it is difficult to determine if the single bit received as 0 (from transmitted input bits (0,1)) is the original bit (uncorrupted), an error (corrupted), or lost (erasure) bit due to noise, interference and fading effects of the wireless communication channel.

To reduce the bit errors and to detect the bit erasures a method of transmitting the code word bits twice with its inverted bit as a set of 2 bits [25] i.e. 0 bit transmitted as {0,1} and 1 bit transmitted as {1,0} is suggested in this paper.

B. Graphical Representation

The graphical representation of such channel model with code word bit transmitted twice with its inverted is shown in Fig. 4.

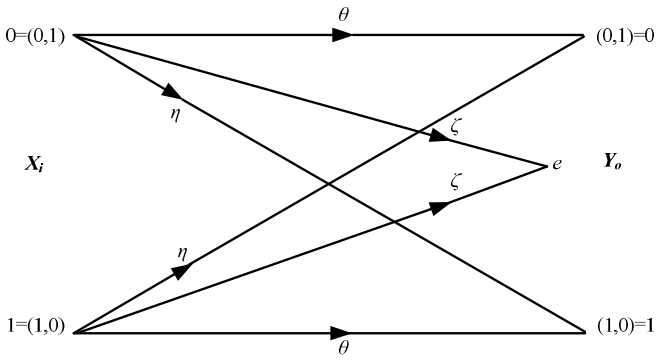

Fig. 4 Graphical representation of a BSC-BEC channel with code word bit transmitted twice with its inverted

The coded input symbols (0,1) for 0, (1,0) for 1 are either received as output symbols 0, 1 and *e*. In Fig. 4, θ represents the probability of a bit correctly received, ζ represents the probability of a bit erasure and η represents the probability of a bit inverted or complemented.

C. Transmission over BSC and BEC Channel

To calculate the total transition probabilities, the transmission of symbols is assumed to be firstly via a BSC noisy channel and then through the BEC erasure channel as shown in Fig. 5, by assuming there are two transmitters and two receivers for the transmission and reception of code word bits.

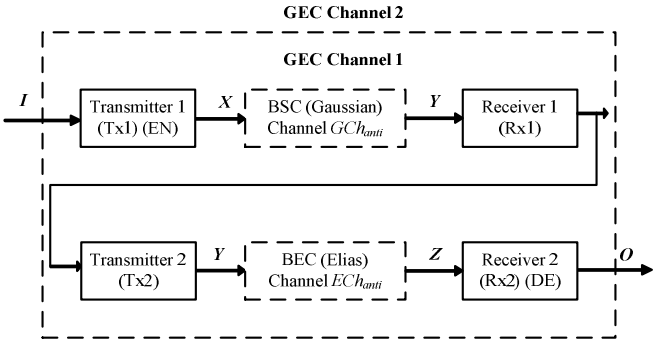

Fig. 5 BSC-BEC channel with code word bits transmitted twice with its inverted

In Fig. 5 each incoming code word bit represented by an input alphabet $I = \{0,1\}$ is further encoded (EN) by transmitter 1 (Tx1) as given by the alphabet $X = \{(0,1), (1,0)\}$. The alphabet *X* is transmitted by the transmitter 1 over the BSC (Gaussian) noisy channel, which results as a GEC (Generalized Erasure Channel) [26] channel 1 at the input of the receiver 1 given by the alphabet $Y = \{(0,1), (1,0), (0,0), (1,1)\}$. The alphabet *Y* is then transmitted by the transmitter 2 over the BEC (Elias) channel, which results as a GEC channel

2 at the input of the receiver 2 given by the alphabet Z = {(0,1), (1,0), (0,0), (1,1)}. The alphabet Z is decoded (DE) as the output symbol as O = {0, 1, e} as shown in Fig. 5 and Table I .

In Table I, it is shown that the transmission of the code word bits twice with its inverted over the BSC and BEC channel results as a GEC channel. Therefore, the wireless communication model for safety related systems is considered as a GEC channel model. The resulting transition probabilities calculated are also shown in Table I.

Table I
Transition Probabilities with codeword bits transmitted twice with its inverted over the BSC-BEC Channels.

Tx1 DE (I)	EN (X)	Rx1 EN (Y)	Tx2 EN (Y)	Rx2 EN (Z)	DE (O)	Transition Probability
0	(0,1)	(0,1)	(0,1)	(0,1)	0	$(1-\varepsilon)^2\cdot(1-\varphi)$
0	(0,1)	(0,1)	(0,1)	(0,0)	e	$(1-\varepsilon)^2\,\varphi$
0	(0,1)	(1,0)	(1,0)	(1,0)	1	$\varepsilon^2\cdot(1-\varphi)$
0	(0,1)	(1,0)	(1,0)	(0,0)	e	$\varepsilon^2\cdot\varphi$
0	(0,1)	(0,0)	(0,0)	(0,0)	e	$(1-\varepsilon)\cdot\varepsilon\cdot(1-\varphi)$
0	(0,1)	(0,0)	(0,0)	(0,0)	e	$(1-\varepsilon)\cdot\varepsilon\cdot\varphi$
0	(0,1)	(1,1)	(1,1)	(1,1)	e	$\varepsilon\cdot(1-\varepsilon)\cdot(1-\varphi)$
0	(0,1)	(1,1)	(1,1)	(0,0)	e	$\varepsilon\cdot(1-\varepsilon)\,\varphi$
1	(1,0)	(1,0)	(1,0)	(1,0)	1	$(1-\varepsilon)^2\cdot(1-\varphi)$
1	(1,0)	(1,0)	(1,0)	(0,0)	e	$(1-\varepsilon)^2\cdot\varphi$
1	(1,0)	(0,1)	(0,1)	(0,1)	0	$\varepsilon^2\cdot(1-\varphi)$
1	(1,0)	(0,1)	(0,1)	(0,0)	e	$\varepsilon^2\cdot\varphi$
1	(1,0)	(0,0)	(0,0)	(0,0)	e	$\varepsilon\cdot(1-\varepsilon)\cdot(1-\varphi)$
1	(1,0)	(0,0)	(0,0)	(0,0)	e	$\varepsilon\cdot(1-\varepsilon)\,\varphi$
1	(1,0)	(1,1)	(1,1)	(1,1)	e	$(1-\varepsilon)\cdot\varepsilon\cdot(1-\varphi)$
1	(1,0)	(1,1)	(1,1)	(0,0)	e	$(1-\varepsilon)\cdot\varepsilon\cdot\varphi$

In Table I, each code word bit transmitted via BSC (Gaussian) channel with error is given by ε^2, with no error is given by $(1-\varepsilon)^2$ and each code word bit transmitted via BEC (Elias) channel with erasure is given by φ and with no erasure is given by $(1-\varphi)$. The overall transition probability for each bit of the code word with error and erasure is given as the product of the transition probability via BSC (Gaussian) and BEC (Elias) channel.

The probability that a bit transmitted and received is represented by P (bit $_{\text{received}}$ | bit $_{\text{transmitted}}$) and is given by the following equations:

$$P(0\,|\,0)=(1-\varepsilon)^2\cdot(1-\varphi) \tag{3}$$

$$P(1\,|\,0)=\varepsilon^2\cdot(1-\varphi) \tag{4}$$

$$P(1\,|\,1)=(1-\varepsilon)^2\cdot(1-\varphi) \tag{5}$$

$$P(0\,|\,1)=\varepsilon^2\cdot(1-\varphi) \tag{6}$$

$P(e\,|\,0)$ and $P(e\,|\,1)$ are given by the summation of the probabilities of receiving (0,0) or (1,1) for the input symbol 0 (resp. 1) received at the output alphabet Z and detected as an erasure symbol e i.e.

$$\begin{aligned}P(e\,|\,0)&=(1-\varepsilon)^2\cdot\varphi+\varepsilon^2\cdot\varphi+\varepsilon\cdot(1-\varepsilon)\cdot(1-\varphi)+\\&\quad\varepsilon\cdot(1-\varepsilon)\cdot\varphi+\varepsilon\cdot(1-\varepsilon)\cdot(1-\varphi)+\varepsilon\cdot(1-\varepsilon)\cdot\varphi\\&=(1-2\varepsilon+\varepsilon^2+\varepsilon^2+2\varepsilon-2\varepsilon^2)\cdot\varphi+2\varepsilon\cdot(1-\varepsilon)\cdot(1-\varphi)\\&=\varphi+2\varepsilon\cdot(1-\varepsilon)\cdot(1-\varphi)\end{aligned} \tag{7}$$

$$\begin{aligned}P(e\,|\,1)&=(1-\varepsilon)^2\cdot\varphi+\varepsilon^2\cdot\varphi+\varepsilon\cdot(1-\varepsilon)\cdot(1-\varphi)+\\&\quad\varepsilon\cdot(1-\varepsilon)\cdot\varphi+\varepsilon\cdot(1-\varepsilon)\cdot(1-\varphi)+\varepsilon\cdot(1-\varepsilon)\cdot\varphi\\&=(1-2\varepsilon+\varepsilon^2+\varepsilon^2+2\varepsilon-2\varepsilon^2)\cdot\varphi+2\varepsilon\cdot(1-\varepsilon)\cdot(1-\varphi)\\&=\varphi+2\varepsilon\cdot(1-\varepsilon)\cdot(1-\varphi)\\&=P(e\,|\,0)\end{aligned} \tag{8}$$

i.e. the resulted GEC channel model is symmetric as the transition probabilities are equal i.e. $P(0\,|\,0) = P(1\,|\,1)$, $P(1\,|\,0) = P(0\,|\,1)$, and $P(e\,|\,0) = P(e\,|\,1)$.

Therefore, the values of θ, η, and ζ in Fig. 4, with each bit of the code word transmitted twice with its inverted bit through a BSC-BEC channel resulting as a GEC channel are given as:

$$\theta=(1-\varepsilon)^2\cdot(1-\varphi) \tag{9}$$

$$\eta=\varepsilon^2\cdot(1-\varphi) \tag{10}$$

$$\zeta=\varphi+2\varepsilon\cdot(1-\varepsilon)\cdot(1-\varphi) \tag{11}$$

D. Procedure for code word Transmission

There are two methods of transmitting the code word bits twice with its inverted bits. In method 1 each bit of the code word is transmitted twice with its inverted bit appended to the original n-bit code word, thereby giving a total of 2n-bit code word given by c as (12). In method 2 the complete n-bit code word is inverted and appended to its original giving a total of 2n-bit code word of different pattern given by c as (13).

$$c=(m_1\overline{m_1},.....m_k\overline{m_k},S_0\overline{S_0},...,S_{r-1}\overline{S_{r-1}}) \tag{12}$$

$$c=(m_1,.....m_k,S_0,...,S_{r-1},\overline{m_1},.....\overline{m_k},\overline{S_0},...\overline{S_{r-1}}) \tag{13}$$

where m_1 to m_k represents the k information bit symbols with its inverted from $\overline{m_1}$ to $\overline{m_k}$. S_o to S_{r-1} represents the r checksum bits with its inverted from $\overline{S_0}$ to $\overline{S_{r-1}}$.

The implementation of the first method depends on the design of the transceiver complexity at the lower layers of protocol stack. If the design is very complex at the lower layers, the second method should be implemented at the upper layers of the protocol stack. In either of the methods, it should be ensured that the coded information bits are transmitted twice with its inverted bits as a 2*n*-bit code word. The 2*n*-bit code word is then transmitted through the serial concatenation of BSC and BEC channel to the receiver.

The receiver only accepts the information bits, if the received original code word and its inverted code word are antivalent and the calculated CRC checksum of the extracted original information bits is same as the received original code word CRC checksum. With this method, bit errors are reduced and the bit erasures are detected confidently as explained in Table I.

E. PFH Derivation for Wireless Communication

The quantity Λ of undetected errors per hour or PFH values is given by the formula [27]-[30]:

$$\Lambda = 3600 \cdot P_{ue}(\varepsilon, \varphi, C) \cdot v \cdot 100 \cdot (m-1) \tag{14}$$

where P_{ue} is the probability of undetected error, v is the number of safety related messages per second given by R / n; R is the data rate with packet length n, m is the number of communicating devices, and the factor 100 is the 1% factor introduced to avoid the safe communication errors.

According to the international standard IEC 61508 and IEC 61511, PFH values determine the SIL levels, and there are four defined different SIL levels SIL1 to SIL4. High demand mode is taken into consideration for calculations and in this mode, SIL1 is achieved when the PFH values lies in the range $\geq 10^{-6}$ to 10^{-5}, SIL2 $\geq 10^{-7}$ to 10^{-6}, SIL3 $\geq 10^{-8}$ to 10^{-7}, and SIL4 $\geq 10^{-9}$ to 10^{-8} [31].

As explained, that the resulted channel model is a GEC channel for wireless communication for safety related systems, the general equation of the P_{ue} for a GEC channel is given as [26]:

$$P_{ue}(\zeta, \eta, \theta, C) = \sum_{l=1}^{n} A_l n^l \theta^{n-l} \tag{15}$$

where A_l is the number of code words of the linear block code C of Hamming weight l.

By substituting θ, η, and ζ from the above calculations (equations (9), (10), (11)) in equation (15)), P_{ue} with the coded information bits transmitted twice with inversion and in terms of ε and φ is given as:

$$P_{ue}(\varepsilon, \varphi, C) = (1-\varphi)^n \sum_{l=1}^{n} A_l \cdot \varepsilon^{2l} \cdot (1-\varepsilon)^{2(n-l)} \tag{16}$$

with $P_{ue}(\varepsilon, \varphi, C)$ derived, Λ or PFH value can be calculated which determines the SIL level as given in the international standard IEC 61508 [31].

In (16) for a particular CRC if the values of the A_l are not knows, it is difficult to calculate these values and especially for shortened hamming codes there are no mathematical equations derived. For this purpose an upper bound P_{ue} inequality has been derived, which is given as [32]:

$$P_{ue}(\varepsilon, \varphi, C) \leq (1-\varphi)^n \cdot \frac{72}{121} \sqrt{2\pi} \frac{\sqrt{n}}{2^r} \frac{1}{d!} n^d \varepsilon^{2 \cdot d} + R_n(\varepsilon^2) \tag{17}$$

Equation (17) is valid for proper codes or codes with natural length of the code.

F. Bluetooth Technology SIL levels

For Bluetooth technology, a separate safety layer is implemented on the top of the L2CAP layer of Bluetooth protocol stack [33]. In this safety layer CRC32c (Castagnoli) [34] is implemented as data safety method and the code word transmission procedure is implemented as redundancy with cross comparison safety method.

With this implemented safety layer and with the PFH derivation as explained, SIL levels achieved for Bluetooth technology are shown in Fig. 6.

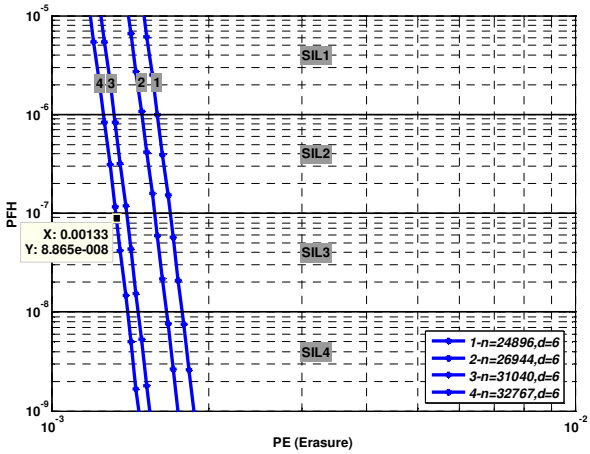

Fig. 6 PFH vs. PE with code word bits transmitted twice with its inverted at a BER 10^{-1}.

Fig. 6 shows that at BER of 10^{-1} (higher and practical value for wireless communication), code word length n = 32767 bits with Hamming distance 6, PE $\leq 1.33 \times 10^{-3}$, a safety integrity level of SIL3 is achieved (plot 4), which is the most common accepted and required value for safety related systems in industrial applications.

V. Conclusion

Due to the advantages of wireless transmission, safe wireless communication plays a significant role for safety related systems in industrial, medical and other safety related applications. For this purpose, the implementation of safe

packet with safety methods and the safety layer implementation are explained in this paper. To reduce the bit errors, P_{ue} and to detect the bit erasures that occur during wireless transmission of the information, a code word transmission with its inverted bits is suggested. For this transmission procedure, mathematical equations are derived and from which SIL levels for a particular wireless technology can be determined. Based on these equations, SIL levels achieved for Bluetooth technology are calculated. As SIL3 is the most acceptable value in industrial safety related applications, this level achieved with Bluetooth technology is shown.

For a particular wireless technology to achieve safe wireless communication for safety related systems, the technology has to be analyzed for the safety methods implemented. If the implemented safety methods are not sufficient, a separate safety layer has to be implemented independent to the standard safety methods as explained in this paper. For the calculations to determine the SIL levels, the derived PFH equation together with P_{ue} derivation as explained in this paper can be used.

REFERENCES

[1] PROFIsafe, "Test Specification for Safety-Related PROFIBUS DP Slaves, V3.0," Nov. 2005.

[2] Profisafe (2012, November), "Technology-Profisafe," Available: http://www.profibus.com/technology/profisafe/

[3] Phoenix Contact (2012, November), "Safety Basics, Interbus-Safety," Available: http://www.phoenixcontact.com/global/technologies/40872_42836.htm

[4] CiA (2012, November), "Technology-CANopen" Available: http://www.can-cia.org/index.php?id=513

[5] F. Handermann, "Communication with SafeEthernet," *Praxis Profiline- Industrial Ethernet*, HIMA Paul brandt GmbH, Apr. 2002.

[6] A. Jarmo, H. Marita, and T. Malm, "Safety of Digital Communication in Machines," *VTT Research Notes 2265*, Espoo, 2004.

[7] D. Miorandi, , E. Uhlemann, V. Stefano, and W. Andreas, "Wireless Technologies in Factory and Industrial Automation – Part I," *IEEE Transactions on industrial informatics*, May 2007.

[8] Y.Bo, Y. Liuqing, and C. Chia-Chin, "ECG Monitoring over Bluetooth: Data Compression and Transmission," *IEEE Wireless Communications and Networking Conference (WCNC)*, Apr. 18-21, 2010.

[9] M. Kamel, S. Fawzy, A. El-Bialy, and A. Kandil, "Secure remote patient monitoring system; Systems and Biomedical Engineering Department," *IEEE Conference on Biomedical Engineering*, Apr. 2011.

[10] H. Sheng, M. Schwarz, and J. Boercsoek; "New Concept to Develop a Safety Sensor Network for Continuous Noninvasive Blood Pressure Monitoring," *17th IEEE International Conference on Emerging Technologies and Factory Automation*, Krakow, Poland, Sep. 2012.

[11] Cirronet, Inc, "Wireless Communication for Industrial Applications," Cirronet Inc, Oakbrook Parkway, Norcross, GA 30093 USA, 2002.

[12] EN 50159-2, "Safety-related communication in open transmission system," *European committee for electro technical standardization*, part-2, page 44, 2001.

[13] W. I. George, J. Colandairaj, and G. S. William, "An Overview of Wireless Networks in Control and Monitoring; Computational Intelligence," *International Conference on Intelligent Computing (ICIC)*, Proceedings, Part II, Kunming, China, Aug. 16-19, 2006.

[14] M. Di Renzo, and M. Debbah, "Wireless physical-layer security: The challenges ahead," *International Conference on Advanced Technologies for Communications*, Edinburgh, UK, Oct. 2009.

[15] D. Lun, H. Zhu, A.P. Petropulu, and H.V. Poor, "Improving Wireless Physical Layer Security via Cooperating Relays," I*EEE Transactions on Signal Processing*, University of California, Irvine, CA, USA, Mar.2010.

[16] P. Kumar, L. Sang-Gon, and L. Hoon-Jae, "A User Authentication for Healthcare Application Using Wireless Medical Sensor Networks," *13th International Conference on High Performance Computing and Communications (HPCC)*, Tirana, Albania, Sep. 2011.

[17] R. Shrivastava, D.K. Mishra, and A. Jain, "Security at Physical Layer in Wireless Communication," *International Conference on Computational Intelligence and Communication Systems*, IT Dept., IET-DAVV, Indore, India, Oct. 2011.

[18] E.K. Lee, M. Gerla, and S.Y. Oh, "Physical layer security in wireless smart grid," *IEEE Communications Magazine*, University of California, USA, Aug. 2012.

[19] H. Li, S. Gong, L. Lai, Z. Han, R.Q. Qiu, and D. Yang, "Efficient and Secure Wireless Communications for Advanced Metering Infrastructure in Smart Grids," *IEEE Transactions on Smart Grid*, The University of Tennessee, Knoxville, May. 2011.

[20] J. Boercsoek, "Introduction in safety bus systems," Hima, Bruehl, Germany, 2005.

[21] IEC (2003c), IEC 65C/307/NP. Digital data communications for measurement and control-profiles for functional safe and secure communications in industrial networks, New Work Item Proposal, 2003.

[22] H.D. Wacker, and J. Boercsoek, "Redundant Data Transmission and Nonlinear Codes," *WSEAS Transactions on Communications*, 7th May. 2008.

[23] H.D. Wacker, and J.Boercsoek, "Redundant Data Transmission via Different Types of Binary Channels," *7th WSEAS Int. Conf. on Applied Computer & Applied Computational science (ACACOS 08)*, Hangzhou, China, Apr. 2008.

[24] P. Elias, "Error-free coding," *IEEE Transactions on Information Theory*, vol. 4, issue. 4, pp. 29-37, 1954.

[25] H. Jitsukawa, and T. Maruyama, "Method of error detection and correction by majority voting," *European patent application*, Tokyo, Japan, 2000.

[26] H.D. Wacker, J.Boercsoek, and H. Hillmer, "Redundant optical data transmission using semiconductor lasers," *Proceedings of the IEEE/ACS International Conference on Computer Systems and Applications*, pp.1040-1045, 2008.

[27] H.D. Wacker, J.Boercsoek, and H. Hillmer, "Redundant optical data transmission using semiconductor lasers," *Proceedings of the IEEE/ACS International Conference on Computer Systems and Applications*, pp.1040-1045, 2008.

[28] J. Boercsoek, "Safety bus systems," Hima, Bruehl, Germany, 2003.

[29] J. Boercsoek, "Introduction in safety bus systems," Hima, Bruehl, Germany, 2005.

[30] J. Boercsoek, J. Hoelzel and H.D. Wacker, "Probability of Undetected Error with Redundant Data Transmission on Binary Symmetric and Non-symmetric Channels without Memory," WSEAS *Transactions on Communications*, Issue 2, Volume 6, ISSN 1109-2742, 2007.

[31] IEC 61508, "IEC 61508: functional safety of electrical/ electronic/ programmable safety-related systems," IEC, 2000.

[32] P. K. Pendli, M. Schwarz, H. D. Wacker, and J. Boercsoek, "Safe Wireless Communication for Safety Related Systems with Bluetooth Technology" *PSAM 11 & ESREL conference*, Helsinki, Finland, 2012.

[33] P. K. Pendli, M. Schwarz, H. D. Wacker, and J. Boercsoek, "Safe Wireless Communication for Safety Related Systems" 12*th WSEAS Int. Conf. on Circuits,Systems, Electronics, Control & Signal Processing (CSECS 13)*, Budapest, Hungary, Dec. 2013.

[34] G. Castagnoli, S. Braeuer, and M. Herrmann, "Optimization of cyclic redundancy check codes with 24 and 32 parity bits," I*EEE transaction on communication*, vol 41, Jun. 1993.