Bluetooth for Safety Systems

Pavan Kumar Pendli, Michael Schwarz, Hans Dieter Wacker & Josef Boercsoek

Department of Computer Architecture and System Programming

University of Kassel, Kassel

email: kumar@uni-kassel.de, m.schwarz@uni-kassel.de,

Hansd.wacker@uni-kassel.de, j.boercsoek@uni-kassel.de

***Abstract*— In nearly every factory floor and industrial setting, communication links carry vital information between machinery, control, and monitoring devices. Safety related or safety critical systems demand that communication links are safe, reliable and the transmitted information is timely delivered without fault and errors. Additionally, real-time performance, robustness, optimized performance, optimised throughput, latency and power consumption issues are to be considered. This paper presents an approach exploiting Bluetooth short-range radio technology with an additional safety layer to achieve safe communication for safety systems. Additionally, this paper presents a mathematical description to show that this approach meets the requirements of safety systems by achieving Safety Integrity Level 3 (SIL3) according to the standard IEC 61508.**

***Keywords* – Bluetooth, Bluetooth protocol stack, Safety systems and Safety layer.**

I INTRODUCTION

In recent years, wireless communication has been an active area of research. A large number of government and industry initiatives, health care & medical fields, research efforts and standard activities have aimed at enabling wireless and mobile networking technologies [1]-[5]. There are diverse set of wireless access technologies available from satellite networks, to wide area cellular systems, from wireless local loop and PCs to wireless LANs and WPAN's. Bluetooth a WPAN technology is analysed in this paper for safety related systems. As standard Bluetooth communication is not suitable, a safety layer is developed, so that Bluetooth technology can be used for safety related systems.

Bluetooth Special Interest Group (SIG), which was formed in 1998 by mobile telephony and computing leaders like Ericsson, IBM, Intel, Nokia, and Toshiba are working on Bluetooth technology and believe that it can revolutionise wireless connectivity for personal and business mobile devices, enabling seamless voice and data communication via short-range radio links. The technology allows users to connect a wide range of devices easily and quickly, without the need for cables, expanding communication capabilities for mobile computers, mobile phones and other mobile devices, both inside and outside of the office [6].

Bluetooth is initially designed keeping in mind short-range wireless data/voice transmissions, ad-hoc networks and cable replacement purposes. It also provides to some extent reliability for applications. The technology was not designed for safety related, safety critical and real time industrial applications, where the messages are often short but typically demanding more reliable, robust, secured, safe, time critical and faster transmission.

Much of the research work on Bluetooth technology is done to improve throughput and reliability of Bluetooth communication, to provide secured communication against security threats, to improve Bluetooth RF transceiver design for low power consumption, to analyse Bluetooth performance, to provide faster data transmission and to improve the polling time [7]-[12]. This paper investigates Bluetooth technology to achieve safe communication for safety related systems. The implemented safety methods by the standard Bluetooth technology are analysed and as they are not sufficient to provide safe communication, a separate safety layer is designed for this purpose. The mathematical equations for the calculations of safety are also derived with the proposed GEC wireless channel model and the new approach for wireless data transmission to reduce the bit errors, probability of undetected error and the bit erasure (loss of information) present in the wireless channel. The calculations show that with Bluetooth

communication SIL3 is achieved which is the most accepted value for safety systems.

The structure of this paper is as follows: section 2 gives a brief overview of the Bluetooth protocol stack with lower and upper layers. Section 3 gives the values of Safety Integrity Level (SIL) for safety systems. Section 4 explains the implemented safety methods by the standard Bluetooth technology and baseband layer SIL calculations performed for different Bluetooth ACL (Asynchronous Connectionless) packets. In section 5, the modelling of a wireless channel with new approach is explained, in section 6 the safety layer is designed at the L2CAP (Logical Link Control and Adaptation Protocol) layer of the Bluetooth protocol stack to achieve fail-safe communication using Bluetooth technology for safety related systems and finally conclusions in the last section.

II BLUETOOTH PROTOCOL STACK

Bluetooth protocol stack determines how the communication between the devices using Bluetooth technology is possible and it is the core of the Bluetooth specification, which defines how the technology works [6]. It consists of lower layers and upper layers with Host Controller Interface (HCI) as an interface between them. The lower layers of Bluetooth protocol stack are Radio layer, Baseband, and Link Manager called together as a Bluetooth controller and the upper layers consists of L2CAP, RF Communication (RFCOMM) and Service Discovery Protocol (SDP) called together as Host System as shown in Figure 1.

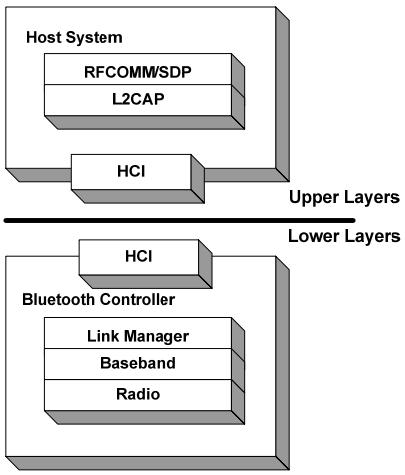

Figure 1: Bluetooth protocol stack.

The radio layer describes the physical characteristics of the components of the Bluetooth's transceiver. Baseband layer manages physical channels and physical links, and is responsible for properly formatting data for transmission to and from the radio layer. The baseband layer also manages synchronous and asynchronous links, handles packets, does paging, and inquiry procedures for the available Bluetooth devices in the range. Apart from these services baseband layer also provides other services like error correction, data whitening, hop selection security and some safety methods explained in the following sections. L2CAP provides connection-oriented and connectionless data services to upper layer protocols with protocol multiplexing capability, segmentation and reassembly operation and group abstractions. L2CAP permits higher-level protocols and applications to transmit and receive L2CAP data packets up to 64 kilobytes in length. L2CAP supports only ACL links; therefore, it is defined only for data traffic such as file, audio/video transfer. For detailed description of the functionalities of each layer, refer Bluetooth specification [6].

III SIL LEVELS FOR SAFETY SYSTEMS

Safety related or safety critical systems are systems in which failures/errors leads to hazardous situations like death, injury or environmental damage, examples are such as industrial process control systems, process shutdown systems, railway signalling equipment, automotive controls, medical treatment equipment, faulty electrical devices *etc*. For such systems, the standard IEC 61508 and IEC 61511 have defined four different SIL's with two different modes, low mode and high mode for measuring the risk reduction for SIS (Safety Instrumented Systems) as shown in Table 1 [13].

SIL	PFD (Λ) (Low Demand)	PFH (Λ per hour) (High Demand)
SIL1	$\geq 10^{-2}$ to 10^{-1}	$\geq 10^{-6}$ to 10^{-5}
SIL2	$\geq 10^{-3}$ to 10^{-2}	$\geq 10^{-7}$ to 10^{-6}
SIL3	$\geq 10^{-4}$ to 10^{-3}	$\geq 10^{-8}$ to 10^{-7}
SIL4	$\geq 10^{-5}$ to 10^{-5}	$\geq 10^{-9}$ to 10^{-8}

Table 1: Safety Integrity Levels.

In Table 1, the Probability of Failure on Demand/ Probability of Failure per Hour (PFD/PFH) values are given by the symbol Λ (lambda) and these values determine the SIL level.

IV BLUETOOTH PROTOCOL STACK IMPLEMENTATION FOR SAFETY

The general Bluetooth Basic Rate (BR) mode baseband packet format is as shown in Figure 2. It consists of access code (68/72 bits), the header (54 bits), and the payload (0-2745 bits) [6]. The header consists of 3-bit logical transport address (LT_ADDR) for identification of the sender and receiver, 4-bit packet type (TYPE) for packet type identification, 1-bit flow control bit (FLOW) for flow control over the ACL link, 1-bit for acknowledgement indication (ARQN), 1-bit sequence number (SEQN) for sequential numbering scheme and an 8 bit header error check (HEC) for securing the header.

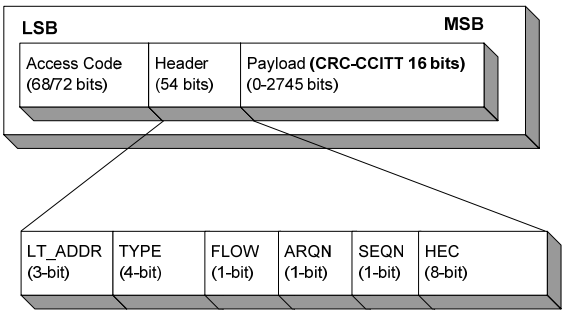

Figure 2: Bluetooth baseband layer packet format.

With these fields in the header, some of the safety methods like identification, flow control, acknowledgement and sequential numbering specified in the document EN 50159-2 [14] are achieved, to avoid the data transmission errors and erasures that occur due to the list of failures as listed in the same document EN 50159-2. With the payload protected by a 16 bit CRC-CCITT data safety method is achieved.

With stop-and-wait ARQ (SW-ARQ) or an unnumbered ARQ scheme concept at the baseband layer, Bluetooth provides very poor throughput performance. At the L2CAP layer there are configurable options which can be configured such as maximum transmission unit (MTU), flush timeout (FTO) option, quality of service (QoS) and retransmission and flow control option. With retransmission and flow control option configured, some buffering can be introduced at the transmitter and the protocols like go-back-N (GBN-ARQ) and selective-repeat ARQ (SR-ARQ) are implemented, from which sequential numbering is further improved. With QoS option configured, flow control method is further improved. With MTU and FTO options configured, safety control methods timestamp and timeout are achieved.

For the 16-bit CRC-CCITT payload protection scheme used at the baseband layer, graph is plotted as shown in Figure 3 for different Bluetooth ACL packets to determine the SIL level:

For the calculation of SIL level, the following equations are used [15]:

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

where Λ is the PFH value given by the equation (1), P_{ue} is the probability of undetected error with ε as bit error ratio and C as the linear code of CRC protection scheme used. The number of safety related messages per second is given by v=R/n (R is the data rate, n is packet length), m represents the number of communicating devices, taken its value as 2 for calculations and 1% introduced to avoid the safety communication errors.

The P_{ue} is given by the formulas [16]:

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

or in terms of dual code as [17]:

$$P_{ue}(\varepsilon, C^{\perp}) = 2^{-r} \sum_{l=0}^{n} B_l \cdot (1-2\varepsilon)^l \cdot (1-\varepsilon)^n \qquad (3)$$

Here,
A_l is the weight distribution of linear code C, B_l is the weight distribution of linear dual code $C^{\perp}$ with number of codeword's of Hamming weight l and ε is the bit error ratio.

For Hamming codes, the formulas to enumerate A_l or B_l are derived in reference [18], but no general formula is known for shortened Hamming codes. The weight distribution of the dual of a shortened Hamming code can be computed with a method called direct method as explained in reference [19]. By computing weight distributions of dual codes at a given ε, P_{ue} for shortened Hamming codes can be determined but the computing requires mathematical calculations or an algorithm to be designed [17]. Instead of computing A_l or B_l for Hamming or shortened Hamming codes, the P_{ue} calculations are performed with upper bound equation (4) given as [20]:

$$P_{ue}(\varepsilon, C) \le \frac{72}{121}\sqrt{2\pi}\frac{\sqrt{n}}{2^r}\frac{1}{d!}n^d\varepsilon^d + R_n \qquad (4)$$

Here,

$$R_n(\varepsilon) \le \left\{ \begin{matrix} \left(2\sqrt{\varepsilon}\right)^{(n)}, n \ge 3 \,\&\, even \\ 2\left(2\sqrt{\varepsilon}\right)^{(n-1)}, n \ge 4 \,\&\, odd \end{matrix} \right\} \qquad (5)$$

where r is the number of parity bits, d is the hamming distance and the remainder term R_n is given by the equation (5). Equation (4) is valid for proper codes for which $P_{ue}(\varepsilon,n)$ increases monotonically with ε values $\in$ [0, 0.5] at a payload length n.

The graph BER vs. PFH is drawn in Figure 3 at the baseband layer for different Bluetooth ACL packets.

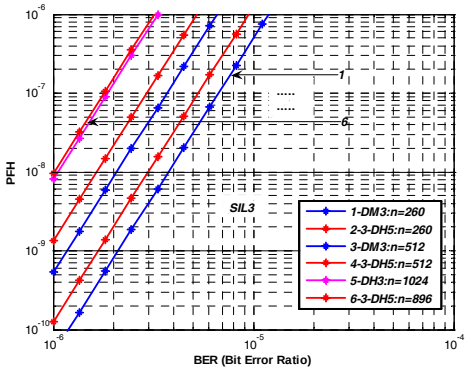

Figure 3: Bluetooth baseband layer packets BER vs. PFH for n=206 to 1024 bits.

The graph is plotted for payload length from n=260 to 1024 bits, as the 16-bit CRC-CCITT code is proper at these values. SIL levels are achieved with the required PFH values for different Bluetooth ACL DM3 (Data Medium), DH3 (Data High) and 3-DH5 packets as shown in Figure 3, but to achieve these SIL levels a BER $\leq 10^{-5}$ or for SIL3 a BER of 10^{-6} is required, which is not a practical value for any wireless or Bluetooth communication.

From these results, it is shown that the CRC-CCITT used for payload protection is not sufficient to use Bluetooth communication for safety systems. Therefore, the data safety method has to be further improved. In the safety control methods listed in the document EN 50159-2 [14] the method redundancy with cross comparison is also not implemented by the standard Bluetooth technology, which is implemented here with a new approach.

V WIRELESS CHANNEL MODEL

As the wireless communication has both errors and erasures present in the wireless channel, the channel is modelled as a Generalised Erasure Channel (GEC) model, which takes into account both the errors and erasures present in the channel. As the bits are lost, it is very difficult to decide if a single bit received as 0 has been transmitted uncorrupted or result of the fading of the channel, so a new method with transmission of each information bit twice with inversion is proposed in this paper.

The GEC wireless channel model is as shown in Figure 4.

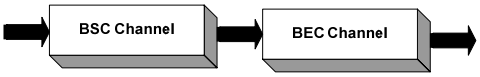

Figure 4: GEC wireless channel model.

In this model both the effects of a Binary Symmetric Channel (BSC) channel and Binary Erasure Channel (BEC) channel are taken into consideration.

The graphical representation of this model with the information bit transmitted twice with inversion is as shown in Figure 5.

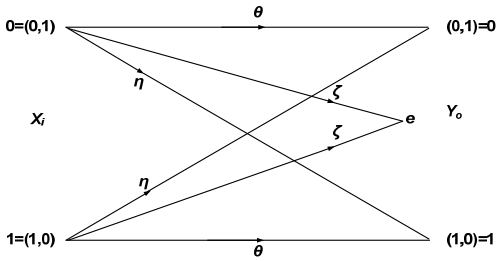

Figure 5: GEC wireless channel model graphical representation.

In Figure 5, η represents probability of error symbol, θ as probability of no error symbol and ζ as probability of erasure or loss of information symbol. X_i represents the input symbol and Y_o represents the output symbol. To detect the bit erasures and to reduce the errors present in the wireless channel, the original information bits are transmitted twice with inversion, i.e. 0 bit is transmitted as {0,1} and 1 transmitted as {1,0} and the erasure is represented by symbol e. At the receiver, the received dual bits are checked for antivalence; if it is the case then the original information bits are extracted and accepted. With this method, the bit errors are reduced and the bit erasures are detected confidently. The calculation of transition probabilities η, θ and ζ with this method, when the information bits are transmitted through a single GEC wireless channel are given as in equation (6) with ε as bit error ratio and φ as bit erasure:

$$\begin{aligned} \eta &= \varepsilon^2 \cdot (1-\varphi) \\ \theta &= (1-\varepsilon)^2 \cdot (1-\varphi) \\ \zeta &= \varphi + 2 \cdot \varepsilon(1-\varepsilon) \cdot (1-\varphi) \end{aligned} \tag{6}$$

The probability of undetected error of the GEC channel is given by [22]:

$$P_{ue}(\zeta,\eta,\theta,C) = \sum_{l=1}^{n} A_l n^l \theta^{n-l} \tag{7}$$

and by substituting equation (6) in (7) P_{ue} is given as:

$$P_{ue}(\varepsilon,\varphi,C) = (1-\varphi)^n \sum_{l=1}^{n} A_l \varepsilon^{2l} (1-\varepsilon)^{2(n-l)} \tag{8}$$

VI BLUETOOTH SAFETY LAYER

The new method to reduce the bit errors and to detect the bit erasures is implemented as a separate safety layer at the L2CAP layer of the Bluetooth protocol stack as shown in the Figure 6.

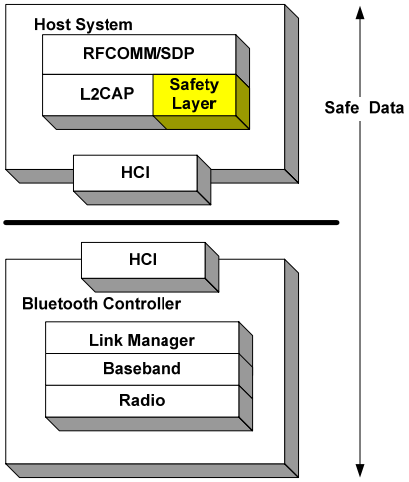

Figure 6: Bluetooth protocol stack with safety layer and safe data transmission.

The information bits protected with the CRC32c (c-Castagnoli) scheme termed as code word is transmitted with the new method proposed in this paper. The data transmitted from the L2CAP layer to

upper layers or lower layers of Bluetooth with the implemented safety layer, by reducing BER and by detecting the erasures occurred in the data transmission via wireless channel is considered safe data.

With the implemented CRC32c scheme and the new method for transmitting the bits twice with inversion, the graph for the PFH values to achieve SIL levels is plotted as shown in Figure 7.

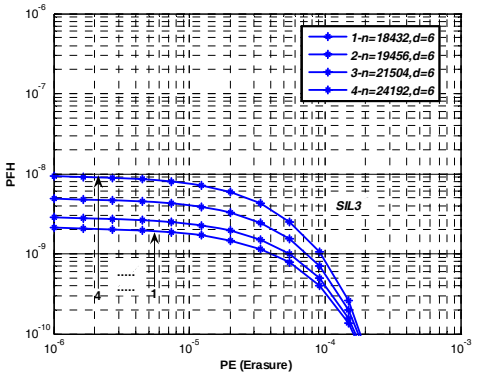

Figure 7: Bluetooth L2CAP PE vs. PFH with double data transmission and inversion, CRC-32/6.

For a BER of 10^{-3} (a practical value for the wireless communication), payload length of n=24k bits with hamming distance d=6, PE (Probability of Erasure) of 10^{-6} a safety integrity level of SIL3 is achieved which is the most acceptable value for safety systems.

For the calculations, P_{ue} upper bound equation (9) is derived and used, where φ is the probability of bit erasure, ε the bit error ratio and $C^{(2)}$ represents the code word being transmitted twice.

$$\begin{aligned} P_{ue}(\varepsilon, C^{(2)}) &\le P_{ue}(\varepsilon^{2}, C) \\ &\le (1-\varphi)^{n} \cdot \\ &\frac{72}{121}\sqrt{2\pi}\frac{\sqrt{n}}{2^{r}}\frac{1}{d!}n^{d}\varepsilon^{2\cdot d} + R_{n}(\varepsilon^{2}) \end{aligned} \tag{9}$$

Here,

$$R_{n}(\varepsilon^{2}) \le \left\{ \begin{matrix} (2\varepsilon)^{(n)}, n \ge 3 \,\&\, even \\ 2(2\varepsilon)^{(n-1)}, n \ge 4 \,\&\, odd \end{matrix} \right\} \tag{10}$$

VII CONCLUSIONS

Standard Bluetooth technology does not provide fail-safe communication and is not suitable for safety related systems. The technology should be further developed for this purpose. With the implemented safety layer protected by a CRC32c scheme and double data transmission with inversion safety is achieved. With the new method proposed, instead of retransmission of the same message again, each bit of the message is transmitted twice with inversion. This introduces a larger redundancy, increases the transmission bandwidth requirements or message delay or both but reduces the probability that all of the original data will be inverted or erased and the erasure goes undetected, providing a safe wireless communication for safety related systems.

REFERENCES

[1] N.P.Mahalik, "Fieldbus Technology, Industrial Network Standards for Real-Time Distributed Control", *springer edition*, Berlin, 2003.

[2] J.Alanen, M.Hietikko & T.Malm, "Safety of Digital Communication in Machines", *VTT Research Notes 2265*, Espoo 2004.

[3] R.Zurawski, "The Industrial Communication Technology Handbook", *CRC Press*, Florida, 2005.

[4] D.Miorandi, E.Uhlemann, S.Vitturi & A.Willig, "Wireless Technologies in Factory and Industrial Automation - Part I"; *IEEE Transactions on industrial informatics*, May 2007.

[5] B.Yu, L.Yang & C.C.Chong, "ECG Monitoring over Bluetooth: Data Compression and Transmission", *IEEE/WCNC*, 2010, pp1-5.

[6] Bluetooth SIG, "Bluetooth Specification Version 4.0", *SIG*, vol 0, 2009.

[7] J.Liang, Y.Li & B.Yu, "Performance Analysis and Reliability Improvement of Bluetooth Broadcast Scheme", *IEEE Pervasive Computing and Applications*, 2006, pp 775-780.

[8] T.Margaret & M.K.Aguilar, "An Investigation of Bluetooth Security Threats", *IEEE/ICISA*, 2011, pp 1-7.

[9] L.B.Li, Z.Huang, Y.Jiao, X.Zheng, & S.Wang, "Low power RF transceiver design for Bluetooth applications", *IEEE/ICSICT*, 2008, pp 1552- 1555.

[10] X.Tian & J.Lu "Performance of Bluetooth FH communication system based on general quadratic prime code", *IEEE/ICNIDC*, 2010, pp 145-148.

[11] J.C.Chan & P.W.Tse, "A Novel, Fast, Reliable Data Transmission Algorithm for Wireless Machine Health Monitoring", *IEEE Transactions on Reliability*, 2009, pp 295-304.

[12] D.Contreras & M.Castro "Adaptive Polling Enhances Quality and Energy Saving for Multimedia over Bluetooth", *IEEE Communications Letters*, 2011, pp 521-523.

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

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

[15] J.Boercsoek, J.Hoelzel & H.D.Wacker, "Probability of Undetected Error with Redundant Data Transmission on Binary Symmetric and Non-Symmetric Channels without Memory", *WSEAS Transactions on Communication*, Journal vol. 6, issue 2, ISSN: 1109-2742, 2007, pp 347-353.

[16] S.B.Wicker, "Error Control Systems for Digital Communication and Storage", *Prentice-Hall*, 1995.

[17] J.K.Wolf & R.D.Blakeney II, "An Exact Evaluation of the probability of undetected error for certain shortened binary CRC codes", *IEEE conference*, Qualcomm Inc, San Diego, CA, 1988.

[18] W.W.Peterson & E.J.Weldon, Jr, "Error-Correcting Codes", *M.I.T. Press*, 2nd ed., Cambridge, MA, 1972, pp 64-70.

[19] T.Fujiwara, T.Kasami, S.Kitai & S.Lin, "On the undetected error probability for shortened hamming codes", *IEEE Transaction Communication*, Vol. COM 33, No. 6, June 1985

[20] H.D.Wacker & J.Boercsoek, "Binomial and Monotonic Behaviour of the Probability of Undetected Error and the 2^{-r}-Bound", *WSEAS*, Volume 7, Issue 3, March 2008.

[21] T.Baicheva, S.Dodunekov & P.Kazakov, "Undetected error probability performance of cyclic redundancy-check codes of 16-bit redundancy", *IEEE Proceedings Communication*, Vol. 147, No. 5, Oct 2000.

[22] H.D.Wacker, J.Boercsoek & H.Hillmer, "Redundant optical data transmission using semiconductor lasers", *IEEE/ACS*, 2008, pp 1040-1045.