INTERNATIONAL JOURNAL OF CIRCUITS, SYSTEMS AND SIGNAL PROCESSING
DOI: 10.46300/9106.2020.14.128 Volume 14, 2020

Investigation of a safety parameter observer for wireless communication

Michael H. Schwarz
Dept. Computer architecture and System programming
University Kassel
Kassel, Germany

Larissa Gaus
Dept. Computer architecture and system programming
Universität Kassel
Kassel, Germany

Josef Börcsök
Dept. Computer architecture and system programming
Universität Kassel
Kassel, Germany

***Abstract*—This paper investigates the possibilities to monitor the degree of disturbances of a wireless communication and to use this information to calculate online the necessary safety parameters in order to estimate the probability of failure per hour (PFH) and the safety integrity level (SIL). Depending of the degree of disturbances, addition actions are performed with the intention of keeping the current safety level. A hardware set-up is introduced to get process data and to evaluate the results.**

Keywords: Signals, Signal Processing, Safety parameters, Systems, Systems Theory, Process Control, Control, Hamming distance, GPC

I. Introduction

In process control, communication is one of the essential components as process data have to be sent from sensors to the control unit to be processed and the control unit sends data to the actuators to force an action. Such communication is often based on wired cable and field bus protocols. The behaviour of wired cable is known and it possesses a certain withstand against noise if properly shielded. However, not all cables resist all kind of noise and new technologies appear that pave their way into industrial automation areas [3], [4]. Industry 4.0 and IoT are the two new areas which push wireless solutions in the area of automation and process control. Wireless communication has advantages over wired communication. First of all, copper cable and optical fibre both are expensive, they have to resist harsh industrial environment such as high and low temperature, humidity, contaminated or aggressive air or gas, vibrations and many others. Wireless communication does not have those problems (the wireless station in the same way as the field bus station but not the communication line) [3], [4], [12].

A wireless station has to be put somewhere and powered up, no cables are used, but they have also some drawbacks. The signals of a wireless communication can be easier perturbed, noise is a much severe problem. An obstacle between two wireless stations can simply stop the communication. Security aspects [9], [11] get also in the focus, as wireless communication can be blocked by jammed signals or a different foreign station can mimic a proper station and can send falsified data (if the protocol is known), or at least it can disturb the communication with the true stations. Fig. 1 illustrates the problems that can occur [3], [4], [12].

This paper is part of the project MEPHYsto which is funded by the German federal state Hessen through the programme Distr@l. We thank Distra@l for the financial support, with the project-nr.: Distra@l 493 20_0021_1.

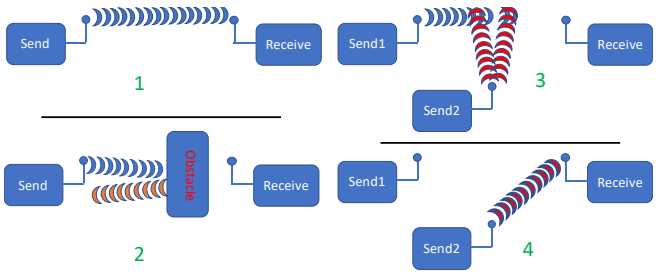

Fig. 1: Wireless communication with 4 scenarios

Additionally, in cyber physical systems, the idea is that every single piece possesses information about itself and its construction, which can be read when needed, but every broadcasted signal can also be read by others [9], [12].

As disturbances can severely affected the quality of the transmitted signals and therefore influence the reliability of a wireless communication, which can result in permanently chancing safety parameters and at the end in a variation of the safety integrity level. Although, the safety integrity level is an unsigned integer between {1...4}, and no 2.3 SIL exist, but it is still good to know, when the SIL decreases or when it is just about to cross the bottom line to a lower safety level [3], [5].

Fig. 2 illustrates the changes in a safety integrity level and also the idea to use the current information to predict the future behaviour and then to use this information to hinder the level loss with additional actions. Diagnostic procedures are well established for hardware systems, whether safe or not, to detect faults in components and either to inform the remaining system about the problem or to switch it off. When it comes to communication, the components are monitored but not the communication itself and there is the most variability of performance in safety expected. Consequently, the transmitted data should be monitored and the number of errors can be used to calculate its reliability and trends can be estimated to state its future behaviour.

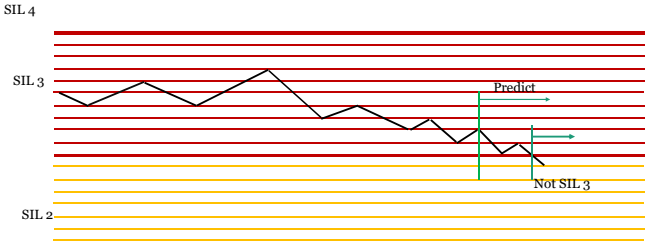

Fig. 2: Illustration of monitoring and predicting the safety integrity

The remaining paper is structured as follows: Section 2 describes the black channel approach and new methods to be used. Section 3 describes the controlled process and the following presents the controller. The set-up is presented in Section 5 and initial tests in Section 6. Conclusions and future work are presented in Section 7.

II. Safety Parameters

The idea is not to design an entire new wireless protocol, as this one would have a difficult stand to be accepted in industries. The generic method is to use a "black channel approach" [6]. The schematic of a black channel method is shown in Fig. 3.Which means that a standard protocol is used and data sequence is modified by the safety protocol [10]. When viewing the protocol from the lower layers of the 7-layer ISO model, it looks like as a normal protocol.

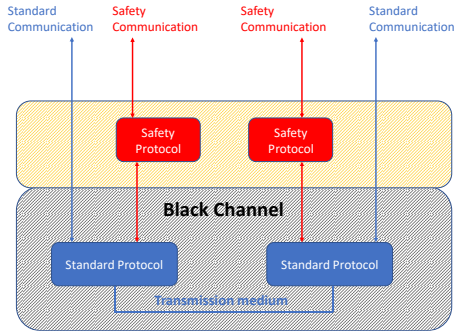

Fig. 3: Black Channel Approach

In field bus systems it is mostly the 7th layer also known as the application layer that interprets the data differently as illustrated in Fig. 4 .

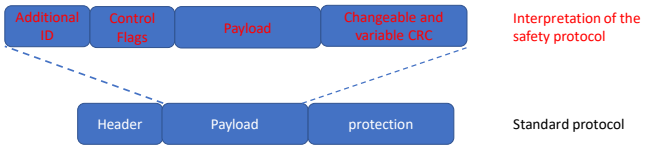

Fig. 4: Payload interpretation

The flags which are necessary to control and understand the meaning of the payload is derived next.

A. Probability of Errors per Hour

The IEC 61508 defines the different levels which are in relation to the probability of error per hour (PFH). Those levels are classifying the safety integrity level (SIL). The calculation is normally based on a risk analysis [5].

Table 1: Relation of SIL and PFH upper bounds

SIL	SIL/PFH	
	PFH of safety function	***PFH of safety communication channel***
4	$< 10^{-8}$	$< 10^{-10}$
3	$< 10^{-7}$	$< 10^{-9}$
2	$< 10^{-6}$	$< 10^{-8}$
1	$< 10^{-5}$	$< 10^{-7}$

It is generally recommended that the safety communication channel should not exceed 1% of the maximum permitted PFH of the achieving SIL [6]. Table 1 shows the relation of the PFH values and the SIL classification [5].

B. General Erasure Channel

The channel model of the digital transmission can be described by the *Generalised Erasure Channel* (GEC) [17]. This model considers two elements for inputs {0,1} and three elements for the output {0, 1, e}, where the input is the sending device and the output is the received value by the receiver. The element *e* indicates that an input whether 0 or 1 is vanished or erased [17].

$$P(e|0) = P(e|1) = \zeta \tag{1}$$

$$P(0|1) = P(1|0) = \eta \tag{2}$$

$$P(0|0) = P(1|1) = \theta \tag{3}$$

From this definition the Bit Error Rate (BER) ε and the Bit Loss Rate (BLR) φ can be explained. BER is the number of falsified bits per second and the BLR is the erased bits per second.

C. Relation of Probability of undetected Error and PFH

The probability of undetected errors P_{ue} for transmissions protected by a linear Code *C* can be stated as follows [17]:

$$P_{ue}(\zeta, \eta, \theta, C) = \sum_{l=1}^{n} A_l \cdot \eta^l \cdot \theta^{n-l} \tag{4}$$

where A_l is a number of code words of weight *l*. ζ, η and θ are already defined and finally, *n* refers to the block-length.

Then, the transitions probabilities ζ, η and θ can be given as detailed in [16]:

$$\zeta = \varphi \tag{5}$$

$$\eta = \varepsilon \cdot (1 - \varphi) \tag{6}$$

$$\theta = (1 - \varepsilon) \cdot (1 - \varphi) \tag{7}$$

Using these equations with (4) results in:

$$P_{ue}(\varepsilon, \varphi, C) = (1 - \varphi)^n \cdot P_{ue}(\varepsilon, C) \tag{8}$$

After some calculations as presented in [3], [4], this results finally in:

$$PFH = 36 \cdot 10^4 \cdot v \cdot (1 - \varphi)^n \cdot P_{ue}(\varepsilon, C) \tag{9}$$

For the mathematical derivation of the online SIL estimations it is referred to [3], [4]; in this paper only the relevant equation will be shortly introduced:

The estimation of BER can be given by:

$$\gamma_b = \frac{E_b}{N_0} \tag{10}$$

Where γ_b is the signal-to-noise ratio per bit E_b is the mean energy per bit and N_0 is the noise spectral density.

The estimation of BLR starts with [17]:

$$\frac{C_{W,\gamma_b}}{W} = \log_2\left(1 + \frac{C_{W,\gamma_b}}{W}\,\gamma_b\right) \tag{11}$$

Where C_{w,γ_b} defines the channel capacity and W desribes the bandwidth. The calculations finally result in [3], [4]:

$$2^{a^x} = 2 \cdot a^{x \cdot \gamma_b} \tag{12}$$

With the substitutions of:

$$x = \frac{(1-\varphi)}{W} \tag{13}$$

and

$$a = 2 \cdot \varepsilon^{\varepsilon} \cdot (1-\varepsilon)^{(1-\varepsilon)}. \tag{14}$$

The probability of undetected error P_{ue} can be estimated as an upper bound with a worst-case approach. The inequality of upper bound for $P_{ue}(\varepsilon, C)$ was derived by [18] for all $0 \leq \varepsilon \leq ½$:

$$P_{ue}(\varepsilon, C) \leq \frac{72}{121} \cdot \frac{\sqrt{2\pi n}}{2^r \cdot d!} \cdot n^d \varepsilon^d + 2^n \left(\sqrt{\varepsilon}\right)^j \tag{15}$$

with

$$j = n \qquad \text{if } n \geq 3 \text{ and even}$$

and

$$j = n - 1 \qquad \text{if } n \geq 4 \text{ and odd.}$$

Where $d = d_{min}$ is the minimum distance of the code C, ε is the value of BER and n is the length of the message while r defines the length of the checksum. The final argument for P_{ue} gets:

$$P_{ue}^{*} = \frac{72}{121} \cdot \frac{\sqrt{2\pi n}}{2^r \cdot d!} \cdot n^d \varepsilon^d + \left(2\sqrt{\varepsilon}\right)^n \tag{16}$$

A detailed derivation can be found in [3], [4]. When combining (16) and (9), the this results in:

$$PFH = f(v, n, r, d) = 36 \cdot 10^4 \cdot v \cdot (1-\varphi)^n \cdot \left(\frac{72}{121} \cdot \frac{\sqrt{2\pi n}}{2^r \cdot d!} \cdot n^d \varepsilon^d + \left(2\sqrt{\varepsilon}\right)^n \right) \tag{17}$$

The function consists of 6 variables: v, k, r, d, φ and ε. BLR φ and the BER ε are parameters that are measured and cannot be directly influenced. The speed of transition v can be changed depending on the system under control. The remaining parameters, are those that can be really influenced. The Hamming distance d, can be changed when changing the CRC from one transition to the next. This has to be indicated in one of the flags that the CRC is changed. The parameter r changes when length of the CRC deviates due to a change of the Hamming distance d when BER or BLR increases for example. The payload k is the last parameter that will be adjusted depending on BLR φ and BER ε. With an increase in noise the messages will be shorter, when the noise decreases the messages can be longer [3], [4].

The optimum is part of a nonlinear optimisation method. For initial tests, only a linear change of k, r, d is considered.

III. Process Description

In this section, the process under control via the wireless communication is described, which is a tank model that is setup in software as a digital twin [15].

A tank that can be filled with liquid should be modelled as shown in Fig. 5. The tank has one inlet (I_I) valve and can be described with (18). Additionally, the tank possesses an outlet valve (I_O) that can be described with (19). The volume can be calculated by calculating the difference between input and output and summed up, which is done in (20). The tank itself is a simple model but can often be found in process industries [15].

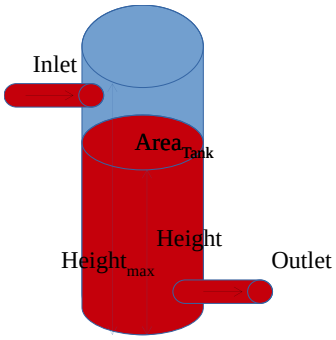

Fig. 5: Schematic of a tank model

The inlet value can be defined as the volume flow:

$$I_I = \frac{Volume}{time} = \frac{V}{t} = \frac{A \cdot h}{t} = A_I \cdot v_I \tag{18}$$

The outlet value can be defined as the volume flow:

$$I_O = \frac{Volume}{time} = \frac{V}{t} = \frac{A \cdot h}{t} = A_O \cdot v_O \tag{19}$$

The current volume of the tank can be calculated as follows:

$$\int_{t_0}^{t_1} (I_1 - I_O)\, dt = \int_{h_0}^{h_1} A \cdot dh \tag{20}$$

The current height can be determined by:

$$H_{current} = \frac{\int_{t_0}^{t_1} (I_1 - I_O)\, dt}{A_{Tank}} \tag{21}$$

The current effluent velocity can be calculated using the Torricelli equation:

$$v_{current} = \sqrt{2 \cdot g \cdot h_{current}} \tag{22}$$

Using (19) and (22) results in:

$$I_O = \dot{V} = A_{valve} \cdot v_{current} = A_{valve} \cdot \sqrt{2 \cdot g \cdot h_{current}} \tag{23}$$

The outlet area is the diameter of the outlet valve and can be controlled from entirely open via a fraction of the diameter to fully closed.

IV. Controller Structure and Tuning

A. Controller

The basic idea of *Generalised Predictive Control* (GPC) is to calculate a sequence of future control signals to minimise a cost function defined over a predicted horizon.

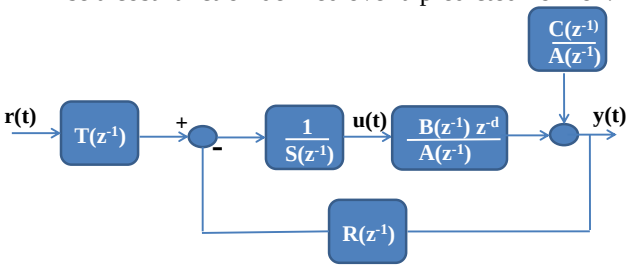

Fig. 6: Closed-loop GPC system

The cost function often is a quadratic function of the measured system output and some predicted reference instances over a predicted horizon plus the quadratic sum of

the control effort [1], [2], [8], [13]. The basic idea of a GPC controller is presented in Fig. 6

The plant model is identified in discrete transfer function form using the backward shift-operator z^{-1}:

$$P(z^{-1}) = \frac{z^{-d}B(z^{-1})}{A(z^{-1})} \quad (24)$$

Where:

$$B(z^{-1}) = b_1 z^{-1} + b_2 z^{-2} + \cdots + b_n z^{-n} \quad (25)$$

$$A(z^{-1}) = 1 + a_1 z^{-1} + a_2 z^{-2} + \cdots + a_n z^{-n} \quad (26)$$

If white noise is assumed, the C polynomial is set to 1, otherwise:

$$C(z^{-1}) = 1 + c_1 z^{-1} + c_2 z^{-2} + \cdots + c_n z^{-n} \quad (27)$$

The output of the process can be written as:

$$A(z^{-1})y(t) = B(z^{-1})z^{-d}u(t-1) + Cz^{-1}\frac{e(t)}{\Delta}$$

$$\text{With } \Delta = 1 - z^{-1} \quad (28)$$

GPC employs the first value of a minimised sequence to the system. The optimisation function often consists of the form:

$$J(N_1, N_2, N_u, \lambda) = \sum_{j=1}^{N_u} (\lambda(j)[\Delta u(t+j-1)]^2) + \sum_{j=N_u}^{N_2} [\hat{y}(t+j|t) - r(t+1)]^2 \quad (29)$$

where ŷ(t+j|t) is the minimised sequence data up to time *t*. N_1 and N_2 are the minimum and maximum costing horizon. N_1 is often set equal to the dead time. N_u is the control horizon and λ is a weighting factor. In order to solve the optimisation problem, the following *Diophantine* equation has to be considered [1]:

$$C(z^{-1}) = \Delta E_j(z^{-1})A(z^{-1}) + z^{-j}F(z^{-1}) \quad (30)$$

and finally, the predicted process output can be calculated as:

$$\hat{y}(t+j|t) = G_j(z^{-1})\Delta u(t+j-d-1) \quad (31)$$
$$F_j(z^{-1})y(t)$$

with:

$$G_j(z^{-1}) = E_j(z^{-1})B(z^{-1}) \quad (32)$$

Equation (32) can be further modified, when splitting it into a future (in red) and past (in blue) section [1]:

$$y(t+j) = Gu \quad (33)$$
$$+F(z^{-1})y(t) + G(z^{-1})\Delta u(t-1)$$

The last two terms [1] are only depending on past values and the subsequent expression is often used in literature:

$$y = Gu + f \quad (34)$$

where f is called the free response. Inserting (34) into (28) and calculating the gradient, results in the mathematical term [1]:

$$\Delta u = \frac{G^T}{(G^T G + \lambda I)}(r - f) \quad (35)$$

Only the first row of the matrix is of interest and only the first element of this row is applied to the process system [1].

B. *Tuning method*

This paper concentrates on using the obtained model parameters to get suitable parameters for the controller. The method is based on experience rather than on analytical computation. The first parameter to be selected is N_1 (lower cost horizon). In literature, this parameter is often set equal to the dead time. This is sensible, then any control signal has an effect on the process after the dead time elapsed [13], [14].

It appears that the control horizon N_u does not get much attention in the literature. Experiments demonstrated that an incorrectly chosen control horizon can destabilise a system. Good solutions were obtained when Nu was set equal to the dead-time of the process [13], [14].

Because the upper cost horizon should be at least equal to control horizon, N_2 should be at least equal to the dead-time of the process. However, the system response improves, when N_2 was selected three times N_u [13], [14].

Finally, the weighting factor λ has to be selected. Therefore, the first parameter of the B-polynomial is used. The value of the parameter is shifted until it is between [0.9 9]. Normally, this results in a gentle control effort. The final tuning method can be summarised as follows, where the coefficients are split in their digits and exponents [13], [14]:

$$G(z^{-1}) = \frac{b_1 10^{\pm x_{b1}} z^{-1} + \cdots + b_n 10^{\pm x_{bn}} z^{-n}}{1 + a_1 10^{\pm x_{a1}} z^{-1} + \cdots + a_n 10^{\pm x_{an}} z^{-n}} \quad (36)$$

$$N_1 = d$$
$$N_2 = 3d$$
$$N_u = d$$
$$\lambda = (b_1 10^{\pm x_{b1}}) * 10^{\mp x_{b1}} \in [0.9,9]$$

V. System Setup

A. *Data bits interpretation*

In the previous sections the different necessary flags and data bytes were defined and explained. For the initial setup the following definitions are made as shown below in Fig. 7:

Fig. 7: Protocol interpretation

Parameter *ID* is a identifer for a communication node and a number for the control loop, if a communication node handles more as one loop. The safety flags are software switches that can enable different safety features as shown in

Table 2. The *CRC-ID* states the currently used CRC polynomial. Due to a noise increase, a forthcoming change in SIL or a change in the data-length a different CRC is used for protection and the receiver has to know which CRC is used. The relevant CRCs [7] are presented in Table 3, with the maximum length of data-bits for the particular CRC. The parameter *k* defines the data length in bits and is calculated as:

$$k = Maxlength - ID_{bit} - SafetyFlag_{bit} - \\ -CRC_{ID\,bit} - r_{bit} \quad (37)$$

Table 2: Safety flags

Safety Flag	Bit interpretation	
	Bit length	***Comments***
1	1	Enables Consecutive number
2	1	Enable Time Stamp
3	1	Data protection CRC
4	1	Redundant, inverted data

Table 3: Selectable CRCs

Safety Flag	CRCs			
	CRC	***Bit Length***	***Data length***	***Hamming D.***
0000	0x33	6	57	3
0001	0x65	7	120	3
0010	0xe7	8	247	3
0011	0x119	9	502	3
0100	0x327	10	1013	3
0101	0x5b	7	56	4
0110	0x83	8	119	4
0111	0x17d	9	246	4
1000	0x247	10	501	4
1001	0x583	11	1012	4
1010	0xbae	12	53	5
1011	0x212d	14	113	5
1100	0xac9a	16	241	5
1101	0x372b	14	57	6
1110	0x573a	15	114	6
1111	0x9eb2	16	135	6

Table 4: Protocol bits

Section	Protocol	
	Bit length	***Comments***
ID	4	Node and Loop identifier
Safety Flag	4	Enables safety features
CRC-ID	4	Current CRC
k	Varies	Data length in bits
r	Varies	Length of CRC
Data	Varies	Data
CRC	Varies	CRC protection

Parameter *r* defines the length of the bit length of the CRC. In Table 4 the lengths of the different protocol sections are shown. In the current state, only the safety flag for data protection is active, the other three mechanisms will be later implemented.

B. Test environment

The initial tests are setup with two programmable logic controllers from the company Bernecker and Rainer Automation (B+R)®. The two PLCs are two *Powerpanel*® and are connected via Ethernet with the wireless access points. A tank model was developed for the first PLC (Receiver PLC) and the generalised predictive controller was derived with the described tuning method and transferred on the second plc (Controller). The controller value is then packed into the protocol frame as described in the previous section and wireless transmitted to the receiver. The receiver verifies the data and passes the value to tank model. The value performs a reaction and the reaction value is then packed and sent to the controller. The GPC calculates the new value and the procedure starts again. The communication circle is shown in Fig. 8.

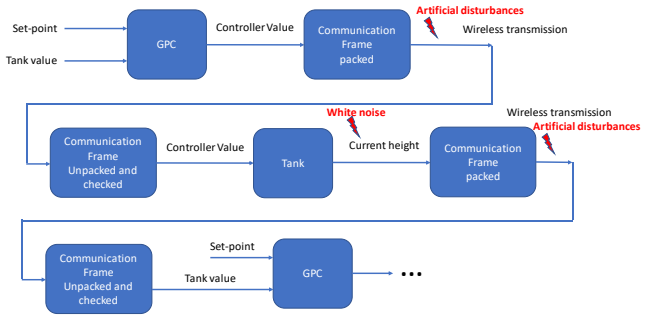

Fig. 8: Control and communication

VI. Initial Tests

Firstly, the control scenario was carried out, to achieve a good control of the tank. To hinder that when the required tank level is reached that always the same value is sent to the tank, artificial white noise was added to mimic real-world situations. The controller has to level out this kind of disturbances.

In the second step, bits are changed and flipped after the value is packed to simulate different disturbances during the transmission and to force the algorithm to change the CRC according to the Hamming distance.

When different data with different lengths has to be sent then the CRC changes but remains in the same Hamming distance category. This was done by sending additional status information.

VII. Conclusions

In this paper a new communication system was set up, that changes its safety features according to the bit error rate and bit loss rate in order to maintain the required safety level. A control scenario was setup consisting of a GPC controller with a tank model placed on two separate PLCs and a communication via a wireless communication.

This paper focuses on the feature that the protection CRC which changes depending on the data load *k*, the required Hamming distances *d* in accordance with the required SIL and PFH value.

A. Future work

This paper was a first step. The safety features according to the flags have to be implemented, especially the redundant, inverted data.

The optimisation problem to determine the best CRC for the transmission and when a CRC should be changed has to be further investigated and implemented.

The communication scenario with several access points and different transmission traffic has to be investigated.

REFERENCES

[1] Camacho E.F. Bordans C., "Model Predictive Control", Advanced Textbooks in Control and Signal Processing London, Springer Verlag, 1999.

[2] Clarke D.W. Mohtadi C. Tuffs P.S., "Generalised Predictive Control Part 1: The Basic Algorithm," Part II: "Extensions and Interpretation", Automatic 23(2), pp.137-148, pp.149-160, 1987

[3] Gaus L., Schwarz M. and Börcsök J., "A theoretical approach to a safety-based predictive adaptation of wireless communication channel parameters in harsh environments", Safety in Extreme Environments. Vol. 2, Issue 1, pp. 93-101, April 2020 ISSN: 2524-8170 (Print) 2524-8189 (Online)

[4] Gaus L. Schwarz M.H., Börcsök J., "A Mathematical Approach to a Real-Time Optimization of Safety Parameters in Wireless Communication Systems", 4thWorkshop & Symposium on Safety and Integrity Management of Operations in Harsh Environments, St. John's, NL, Canada, July15-17, 2019

[5] IEC 61508, "International Standard 61508 Functional Safety of Electrical/Electronic/ Programmable Electronic Safety Related Systems". International Electrochemical Commission. Geneva, Switzerland, 2000

[6] IEC 61784-3, "Industrial communication networks – Profiles- Part 3: Functional safety fieldbuses – General rules and profile definitions", International Electrotechnical Commission, Geneva, Switzerland, 2016

[7] Koopman Ph. "Best CRC Polynomials", available at: https://users.ece.cmu.edu/~koopman/crc/, accessed: 06.12.2020

[8] Maciejowski J. "Predictive Control with Constraints", England, Prentice Hall, 2000

[9] Mueller E., Chen X.-L. & Riedel R. "Challenges and Requirements for the Application of Industry 4.0: A Special Insight with the Usage of Cyber-Physical System", Chinese Journal of Mechanical Engineering vol. 30, pp1050–1057, 2017.

[10] Pendli P. K., "Contribution of Modelling and Analysis of Wireless Communication for Safety related Systems with Bluetooth Technology", Kassel, Kassel university press, 2014, ISBN 978-3-86-219-770-5

[11] Sadiku M. N. O., Wang Y., Cui S., Musa S. M, Roy G., "Cyber-Physical Systems: A Literature Review", European Scientific Journal Vol.13, No.36 December 2017 ISSN: 1857 –7881

[12] Schmertosch T. Krabbes M., 2018, "Automation 4.0" (Automatisierung 4.0), Fachbuchverlag Leipzig, im Carl Hanser Verlag,

[13] Schwarz M., Cox C., Börcsök J., "A Filtered Tuning Method for a GPC Controller", IET Irish Signals and Systems Conference 2010, Cork Ireland, pp 180-186, June 23-24 , 2010, ISBN: 978-1-61782-057-1

[14] Schwarz M.H., Cox C.S., Börcsök J., "A model based tuning method for a generalized predictive controller", IEE Irish Signals and Systems Conference 2005 (ISSC2005), Dublin, Ireland, pp.54-591.-2. Sept., 2005

[15] Schwarz M.H., Börcsök J., "Verified Digital Controller Operating on Programming Logic Controllers for Process Control", 4thWorkshop & Symposium on Safety and Integrity Management of Operations in Harsh Environments, St. John's, NL, Canada, July15-17, 2019

[16] Sköllermo T. and Skoglund M., "A Sub band Image Coder for Channels with Both Errors and Erasures", The Thrity-Seventh Asilomar Conference on Signals, Systems & Computers, pp. 1553-1557, 9-12 November 2003

[17] Wacker H.-D. and Boercsoek J., "The Probability of undetected error of some communication channels", Proceedings of the European Safety and Reliability Conference (ESREL 2007), pp. 385-391, June 2007

[18] Wacker H. D. and Boercsoek J., "Binomial and Monotonic Behavior of the Probability of Undetected Error and the 2-r-Bound", WSEAS Transactions on Communication, vol. 7, pp. 188-197, 2008