Modelling of Failures Effect of Open Transmission System for Safety Critical Applications with the Intention of Safety

M. Franekova[1], P. Luley[2], T. Ondrasina[3]
[1]*Department of Control and Information Systems, Faculty of Electrical Engineering, University of Zilina, Univerzitna, 8215/1, 010 26 Zilina, Slovak Republic*
[2]*Department of Control and Information Systems, Faculty of Electrical Engineering, University of Zilina, Univerzitna, 8215/1, 010 26 Zilina, Slovak Republic*
[3]*IRIS IDENT, s.r.o., Mladeznicka 36/E, 974 05 Banska Bystrica, Slovak Republic*
maria.franekova@fel.uniza.sk

***Abstract*—The paper deals with the problem of modelling safety features of open transmission system used within safety-related applications. The basic principles of modelling failures effect to safety of open transmission system and standards used in the process of safety evaluation are summarised in the paper. The practical part is oriented to description of realized Markov's model for determination of random failures effects to safety of safety-related wireless communication system with safety a cryptography codes. The model reflects the safety analysis of failures effect caused by electromagnetic interference in wireless communication channel and random HW failures of transmission system. In the paper there are mentioned the results of simulation of parameters of transmission system and the impact of block length of cryptography code on the resulting of undetected corrupted message are mentioned.**

***Index Terms*—Fault tolerance, reliability, safety evaluation, telecommunication network.**

I. INTRODUCTION

Safety-related systems are characterized by high tolerance against dangerous effects of failures. Consequences of system failures can be measured directly on the system or by the system simulation on model or eventually by theoretical consideration and by calculation. It should be noted that the high safety requirements of safety-related systems cannot be demonstrated only by the test results or by results from the practice (the frequency of occurrence of dangerous state is very small and the value of the mean time among failures far exceeds the value of lifetime of the safety-related system). Safety analysis of the system helps to provide the evidence that the safety requirements are met and the resulting risk is acceptable.

In technical particle there is the term safety seen as one of comprehensive indicators of reliability attribute. This attribute refers to the degree to which a user can relay that the system will operate the way which it should have, that the system will be available in given time and circumstances and that the system is safe. Such combination of attributes of Reliability, Availability, Maintainability and Safety is known under acronym RAMS [1].

Communication system is an essential part of the whole safety-related system. Therefore it is necessary to pay attention on the method of realization of safety analysis respectively on the system synthesis. If we divide the communication system into detailed subsystems then it is necessary during the calculation of total failure rate calculates the failure rate of end device including interface and the failure rate of transmission system consisting of a transmitter, communication channel, receiver and other network elements [2]. The failure rate of end devices is in most cases stated by the manufacturers therefore it is necessary to pay attention only to safety of safety-related transmission system [3]. Nowadays, even for applications with great requirements for safety it is enforced the usage of open transmission systems for example GSM-R technology (communication medium for train control system in development of European Train Control System [4], [5]) respectively other wireless media (Wi-Fi, Bluetooth, ZigBee, WiMaX) within safety-related control systems in industrial automation [6]–[8]. The approach of wireless safety-related systems (W-SRS) development is based on the usage of COTS technologies (*Commercial Off The Shelf*) and on additional safety layers as recommended by railway applications and industrial applications standards [9]–[12]. Additional layers (safety profile) are mainly focused on protection against transmission errors (for their elimination is usually used safety code) and against unauthorized access

Manuscript received February 12, 2013; accepted November 20, 2013.
This work has been supported by the Educational Grant Agency of the Slovak Republic (KEGA) Number: 024ŽU-4/2012: Modernization of technology and education methods orientated to area of cryptography for safety critical applications.

to the system (for elimination of this is usually used cryptographic code). In the development phase of the system there shall be given quantitative evidence that safety mechanisms used in the safety profile meets the requirements for safety integrity level (SIL) for both these protections. SIL is defined for four levels from the lowest SIL 1 up to the highest SIL 4 in [10].

Within the qualitative analysis of wireless safety-related system the authors were focused on hazard analysis of the safety-related message transmission, on the determination of the error probability of cryptographic code decoder and on determination of dangerous failure rate of wireless safety-related communication system on the level of point-to-point connection.

II. Procedure for Solution Based on Quantitative Analysis

Let us consider a point-to-point communication system (Fig. 1) which consists of two wireless safety-related equipment W-SRE1 and W-SRE2 and wireless transmission system. Trusted wireless transmission system arranges safety-related transmission (physically implemented through couple of encoder/decoder of safety code - ESC/DSC) and accesses (physically implemented through couple of encoder/decoder of cryptography code - ECC/DCC) which are an extension of encoder/decoder of transmission code - ETC/ DTC of untrusted transmission system. One part of untrusted wireless transmission system is wireless communication channel, which is affected by EMI - electromagnetic interference (caused by noises, reflections respectively fading effect) and attacks caused by unauthorized person, what must be also considered in the case of open transmission system.

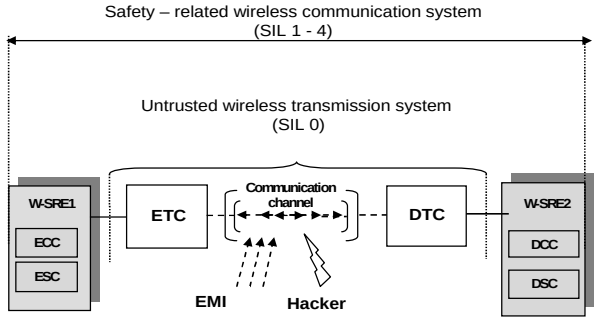

Fig. 1. Safety - related wireless communication system.

The dangerous failure rate of communication system $\lambda_{D(CS)}$ for continuous operation is the sum of dangerous failure rate of end device $\lambda_{D(ED)}$ and dangerous failure rate of transmission system $\lambda_{D(TS)}$

$$^{a}D(CS) = {}^{a}D(ED) + {}^{a}D(TS)\cdot \tag{1}$$

On the basis of dangerous failure formation for open transmission system on the basic fault model according to [9] a dangerous state of transmission system can be caused by:

– Hardware failures of untrusted transmission system including the technical equipment for message transmissions for example by wrong position of antennas or sensitivity of receiver;
– Random failures caused by EMI which are not detected by transmission or safety code;
– Failures of transmission code decoder;
– Failures of cryptographic code decoder.

If we mark dangerous failure rates of particular parts which can cause a dangerous state $\lambda_{D(1)}$, $\lambda_{D(2)}$, $\lambda_{D(3)}$, $\lambda_{D(4)}$ and assume that the impact of failures form particular parts is independent then the dangerous failure rate of whole transmission system is given by sum of those partial failure rates

$$^{a}D(TS) = {}^{a}D(1) + {}^{a}D(2) + {}^{a}D(3) + {}^{a}D(4)\cdot \tag{2}$$

In case the untrusted transmission system does not contain transmission code the influence of $\lambda_{D(3)}$ shall not be considered.

Protocols of wireless technologies in most cases consider the safety code in the form of CRC (*Cyclic Redundancy Check*) code. The procedure for quantitative expression of dangerous failure rates $\lambda_{D(1)}$, $\lambda_{D(2)}$, $\lambda_{D(3)}$ is given in annex of norm [9], but only for the case of closed transmission system. In case the transmission system is using wireless communication channel (it becomes an open transmission system) it is necessary to quantify also the value of dangerous failure rate $\lambda_{D(4)}$. In this paper authors deal only with a mathematical procedure to quantify this particular failure rate. Calculations of dangerous failures rates $\lambda_{D(1)}$, $\lambda_{D(2)}$, $\lambda_{D(3)}$ are taken from [9] respectively from results in [13], [14] stemming from authors experiences gained during years of practice in this field of expertise. Hardware errors of untrusted transmission system can lead to undetected errors during message transmission in case of simulations failure of detection properties of the safety code. Then for $\lambda_{D(1)}$ applies

$$^{a}D(1) = {}^{a}D(HW)\cdot p_{US}.k_1, \tag{3}$$

where $\lambda_{D(HW)}$ is the hardware failure rate of transmission system, p_{US} is the undetected error probability of safety code, k_1 is the hardware failure coefficient.

The mathematical apparatus of p_{US} calculation for (n, k) channel block codes can be found for example in [15]–[17].

The values of $\lambda_{D(HW)}$ and k_1 depends on the failure analysis of particular device or system. In most cases results are the experiences of the devices' operators and are estimated for the worst case. In analysis there is for the probability of undetected error used worst case approach (value 2^{-r}) where r is the number of redundant bits of the safety respectively transmission code. Undetected errors caused by corrupted data integrity due to influence of EMI during the transmission occur in case of failure of both channel codes: transmission (in untrusted transmission system) or safety (in safety layer). Dangerous failure rate $\lambda_{D(2)}$ is then

$$^{a}D(2) = p_{UT}\cdot p_{US}\cdot f_{EMI}, \tag{4}$$

where p_{UT} is the undetected error probability of transmission code, p_{US} is the undetected error probability of safety code,

f_{EMI} is the frequency of error messages per hour caused by EMI.

In case the transmission system does not contain channel encoder/decoder of transmission code then $p_{UT} = 1$.

The frequency of corrupted messages can be easily determined for example in case of cyclic transmission of messages. In other cases this value is estimated or is considered the worst case that means all generated messages from the source are corrupted.

Undetected transmission errors caused by hardware error of transmission code decoder (controlling device) can cause that all messages entering into safety-related layer are consider as correct. Falsification of received message can be detected only by safety code. Then the dangerous failure rate $\lambda_{D(3)}$ can be expressed

$$\lambda_{D(3)} = \lambda_{D(decTC)} \cdot p_{US} \cdot k_2, \quad (5)$$

where $\lambda_{D(\text{decTC})}$ is the dangerous failure rate of transmission code decoder, p_{US} is the undetected error probability of safety code, k_2 is the hardware failure coefficient.

The values of $\lambda_{D(\text{decTC})}$ and k_2 depend on analysis of particular situation for given application. In case we are not able to measure the bit error rate p_b of communication channel is necessary to take into account the worst case during the p_{US} determination, which for binary transmission is $p_b = 2^{-1}$ where p_{US} is limiting to value 2^{-r}, where r is the number of redundant bits of safety code.

During the usage of open transmission system it is necessary to consider that dangerous state (hazard) can occur also due to unauthorized access to the system (for example by hacker). In that case it is necessary to include the cryptographic code into the transmission string which modifies the message to unintelligible form for unauthorized user. It should also be quantified the cryptographic code failure on the side of receiver. It is recommended to use only computationally secure cryptographic block codes for safety-related applications.

III. MODEL DEVELOPMENT AND DESCRIPTION

The model was realized by continuous Markov processes. During model development the authors considered the impact of various factors on the safety of wireless transmission system. The aim of failure effects analysis of the wireless system safety was to create a model which allows identifying the transitions process from safe state to dangerous state and allows calculating the probability of occurrence of dangerous state as a result of failures during system operation. Corruption of transferred data which is not detected by transfer system and those data are handled as correct is considered as adverse effect.

In the model there are considered following types of random failures: random failures of hardware part of transmission system and failures caused by electromagnetic influence. Model development was based on Markov models implemented for closed transmission system (fieldbus) and was published in [18]. These models are extended for the needs of open transmission system. The transition from a functional safe state 1 to dangerous (failure) state 7 is shown in Fig. 2. A Markov diagram corresponding with safety-related message transfer through wireless transmission system is shown in Fig. 1.

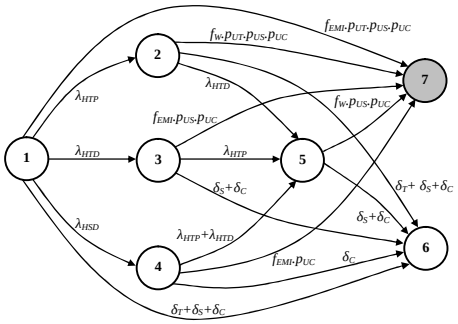

Fig. 2. Markov diagram.

Characteristics of individual states and of diagram transitions from Fig. 2 are given in Table I and Table II. Meaning of symbols used in diagram and in Fig. 2 is given in Table III.

TABLE I. STATE DIAGRAM.

State	State description	P(t=0)
1	Wireless transmission system is operational; transmitted messages are corrupted by EMI.	1
2	The state of wireless transmission system when transmitting part of transmission system or any part of communication channel is in failure.	0
3	The state of wireless transmission system when transmission code decoder is in failure.	0
4	The state of wireless transmission system when safety code decoder is in failure.	0
5	The state of wireless transmission system when transmitting part of transmission system or any part of the communication channel is in failure and also transmission code decoder and safety code decoder are in failure.	0
6	Permanent interruption of transmission due to control mechanism for number of received corrupted messages.	0
7	Dangerous state – corrupted message was not detected.	0

The authors simplified the diagram assuming that in case of transmission code decoder failure or in case of cryptographic code decoder failure it is no longer relevant to consider the impact of other parts of untrusted transmission system on the frequency of corrupted data (Fig. 3).

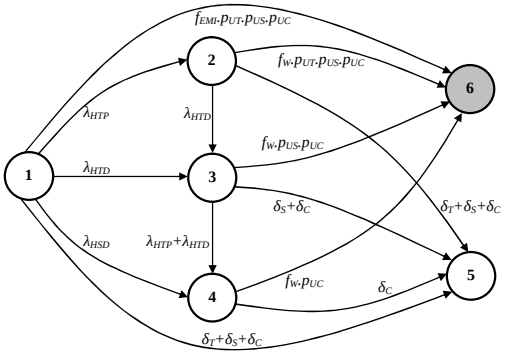

Fig. 3. Simplified Markov diagram for open transmission system.

Markov diagram in Fig. 3 can be mathematically described by a system of differential equations and by initial probability vectors. The system of differential equations is defined by

$$\frac{dP(t)}{dt} = A.P(t), \tag{6}$$

where $P(t) = \{p_1(t), p_2(t), ..., p_n(t)\}$ is the absolute probabilities vector and A is the transition integrity matrix. Vector of initial probabilities $P(t = 0) = \{1,0,...0\}$.

TABLE II. DIAGRAM TRANSITIONS.

Transition	Transition description	Marking
1 → 2	Transition will take place as a result of hardware failure of transmitting part of transmission system or of any part of communication channel.	λ_{HTP}
1 → 3	Transition will take place as a result of hardware failure of transmission code decoder.	λ_{HTD}
1 → 4	Transition will take place as a result of hardware failure of safety code decoder.	λ_{HSD}
1 → 6	Transition will take place as a result of operation of the control mechanism for the number of received corrupted messages by transmission code decoder or by safety code decoder or by cryptographic code decoder.	$\delta_T + \delta_S + \delta_C$
1 → 7	Transition will take place as a result of insufficient detection capability of transmission, safety and cryptographic code.	$f_{EMI}.p_{UT}.p_{US}p_{UC}$
2 → 5	Transition will take place as a result of hardware failure of transmission code decoder.	λ_{HTD}
2 → 6	Transition will take place as a result of operation of the control mechanism for the number of received corrupted messages by transmission code decoder or by safety code decoder or by cryptographic code decoder.	$\delta_T + \delta_S + \delta_C$
2 → 7	Transition will take place as a result of insufficient detection capability of transmission, safety and cryptographic code.	$f_W.p_{UT}.p_{US}.p_{UC}$
3 → 5	Transition will take place as a result of hardware failure of transmitting part of transmission system or of any part of communication channel.	λ_{HTP}
3 → 6	Transition will take place as a result of operation of the control mechanism for the number of received corrupted messages by safety code decoder or by cryptographic code decoder.	$\delta_S + \delta_C$
3 → 7	Transition will take place as a result of insufficient detection capability of transmission, safety and cryptographic code.	$f_{EMI}.p_{US}.p_{UC}$
4 → 5	Transition will take place as a result of hardware failure of transmitting part of transmission system or of any part of communication channel or as a result of hardware failure of transmission code decoder.	$\lambda_{HTP} + \lambda_{HTD}$
4 → 6	Transition will take place as a result of operation of the control mechanism for the number of received corrupted messages by cryptographic code decoder.	δ_C
4 → 7	Transition will take place as a result of insufficient detection capability of cryptographic code.	$f_{EMI}.p_{UC}$
5 → 6	Transition will take place as a result of intervention of the control mechanism for the number of received corrupted messages by safety code decoder or by cryptographic code decoder.	$\delta_S + \delta_C$
5 → 7	Transition will take place as a result of insufficient detection capability of safety and cryptographic code.	$f_W.p_{US}.p_{UC}$

Based on formulas in [18] it is possible for the simplified Markov diagram of open transmission system in Fig. 3 to determine the transition integrity matrix which implies following system of differential equations:

$$p'_{1(T\le t)} = (-{}^{a}_{HTP} - {}^{a}_{HTD} - {}^{a}_{HSD} - ¢_T - ¢_S - ¢_C - f_{EMI}\,p_{UT}\,p_{US}\,p_{UC})\,p_{1(T\le t)}, \tag{7}$$

$$p'_{2(T\le t)} = {}^{a}_{HTP}\,p_{1(T\le t)} + (-{}^{a}_{HTD} - ¢_T - ¢_S - ¢_C - f_W\,p_{UT}\,p_{US}\,p_{UC})\,p_{2(T\le t)}, \tag{8}$$

$$p'_{3(T\le t)} = {}^{a}_{HTD}\,p_{1(T\le t)} + {}^{a}_{HTD}\,p_{2(T\le t)} + (-{}^{a}_{HTP} - {}^{a}_{HTD} - ¢_S - ¢_C - f_W\,p_{US}\,p_{UC})\,p_{3(T\le t)}, \tag{9}$$

$$p'_{4(T\le t)} = {}^{a}_{HSD}\,p_{1(T\le t)} + ({}^{a}_{HTP} + {}^{a}_{HTD})\,p_{3(T\le t)} + (-¢_C - f_W\,p_{UC})\,p_{4(T\le t)}, \tag{10}$$

$$p'_{5(T\le t)} = (¢_T + ¢_S + ¢_C)\,p_{1(T\le t)} + (¢_T + ¢_S + ¢_C)\,p_{2(T\le t)} + (¢_S + ¢_C)\,p_{3(T\le t)} + ¢_C\,p_{4(T\le t)}, \tag{11}$$

$$p'_{6(T\le t)} = f_{EMI}\,p_{UT}\,p_{US}\,p_{UC}\,p_{1(T\le t)} + f_W\,p_{UT}\,p_{US}\,p_{UC}\,p_{2(T\le t)} + f_W\,p_{US}\,p_{UC}\,p_{3(T\le t)} + f_W\,p_{UC}\,p_{4(T\le t)}, \tag{12}$$

where λ_{HTP} – hardware failure rate of transmitting part of the transmission system and of the communication channel; λ_{HTD} – hardware failure rate of transmission code decoder; λ_{HSD} – Hardware failure rate of safety code decoder; λ_{EMI} – failure rate of EMI disturbance on transmitted messages; p_{UT} – undetected error probability of transmission code; p_{US} – undetected error probability of safety code; p_{UC} – undetected error probability of cryptographic code; f – frequency of generated messages by transmitter; f_{EMI} – frequency of corrupted messages due to EMI; f_{HTP}– frequency of corrupted messages due to hardware failures of transmitting part of transmission system and of the communication channel; f_W – frequency of corrupted messages without reason distinction; T_T – reception tolerance time of corrupted messages of untrusted part of transmission system (detected by transmission code decoder); T_S – reception tolerance time of corrupted messages of trustworthy part of transmission system (detected by safety code decoder); T_C – reception tolerance time of corrupted messages of trustworthy part of transmission system (detected by cryptographic code decoder); $¢_T$ – transition intensity to permanent safe state because of the control mechanism for the number of received corrupted messages by transmission code decoder; $¢_S$ – transition intensity to permanent safe state because of the control mechanism for the number of received corrupted messages by safety code decoder; $¢_C$ – transition intensity to permanent safe state because of the control mechanism for the number of received corrupted messages by cryptographic code decoder.

IV. MODEL VERIFICATION AND OBTAINED RESULTS

The accuracy of the calculation depends on suitably of

chosen calculation method and on the numerical accuracy of computing technique. There exist several software tools which support the solution of Markov diagrams. Authors used the software tool Windchill Quality Solutions (former Relex 2011) from company PTC and the results were verified in software tool Wolfram Mathematica 8 from Wolfram Research.

In practice, the use of model in Fig. 3 is problematic because of the high degree of uncertainty in determination of the model parameters. Therefore, in practical calculations is often used further simplification for example in terms of worst case approach during determination of model parameters. The authors assumed during the quantitative evaluation of transitions in model in Fig. 3 the following:

- Hardware failure rate of transmitting part of the transmission system and of the communication channel is according to [18]: $^{a}{}_{HTP} = 5,3.10^{-5} h^{-1}$;
- Hardware failure rates of transmission code decoder and of safety code decoder are according to [18] $^{a}{}_{HTD} = 2,5.10^{-6} h^{-1}$ and $^{a}{}_{HSD} = 2,5.10^{-6} h^{-1}$;
- It is assumed the cyclic mode of safety-related messages transmission from the source – time of cycle is 50 *ms*;
- Frequency of safety-related messages generated by transmitter is $f = 72.10^{3} h^{-1}$;
- Frequency of corrupted messages due to EMI is $f_{EMI} = 72.10^{3} h^{-1}$ (messages are transmitted periodically every 50 *ms*, worst-case assumption that all messages are corrupted due to EMI);
- Frequency of corrupted messages without reason distinction is $f_W = 72.10^{3} h^{-1}$ (messages are transmitted periodically every 50 *ms*, assuming all messages are corrupted);
- Reception tolerance time of corrupted messages of trustworthy part of transmission system is set to value T_C = 150 *ms* (the transmission system is set up so that if three successive messages are corrupted the connection is terminated), behaviour of the system is after restart verified also for other values of T_C (100 ms and 200 ms);
- Transition intensity to permanent safe state because of the control mechanism for the number of received corrupted messages by cryptographic code decoder is $¢_C = \frac{1}{T_C} = 36000h^{-1}, 24000h^{-1}, 18000h^{-1}$;
- It is assumed a transmission code type CRC-16 − according to standard [9] the occurrence of undetected error probability of transmission code is: $P_{UT} = 2^{-16}$ (worst case assumption);
- It is assumed a safety code type CRC-32 − type according to standard [9] the occurrence of undetected error probability of transmission code is: $P_{US} = 2^{-32}$ (worst case assumption);
- It is assumed a block cryptographic code with block size k = 64, 128, 256 bits;
- The lengths of transmitted messages are: $n = 10^{1}$, 10^{3}, 10^{4}, 10^{5}, 10^{8} bits.

For the calculation of undetected error probability of cryptographic code P_{UC} is according to [19] used the formula (8), by which the P_{UC} can be approximately calculated as $P_{UC} \approx P_{CW}$. For those interested in the relation (8) we suggest for example [20]

$$P_{CW} = \left(1-2^{-n}\right)^{-1}\left(1-2^{-k}\right)\left[1-\left(1-P_{UT}.P_{US}\right)^{n/k}\right]. \qquad (13)$$

Numerical and graphical results of probability of entry into dangerous (hazardous) state (6) in time t: $P_6(t)$ for Markov diagram in the Fig. 3 [21] has been determined after application of above mentioned parameters and after application of the system of differential equations (7)–(12).

The undetected error probability of cryptographic code P_{UC} for the message with length $n = 10^5$ bits is shown in graphs in Fig. 4 and in Fig. 5. The authors monitored the impact of block length of block cipher k on the resulting undetected error probability of cryptographic code P_{UC} as well as on progress of error probability of gaining the dangerous state $P_6(t)$. The size of block cipher was chosen in accordance with lengths used in practice k = 64 bits (for example for block cipher DES), k = 128 bits (for example for block cipher AES) and k = 256 bits (for example for block cipher AES/Rijndael).

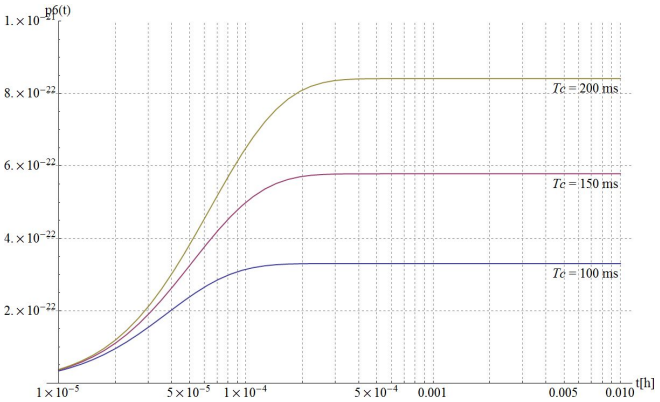

Fig. 4. Probability of undetected corrupted message for block size 64 bits.

The progress chart of the dependence of dangerous state probability and of the time for block size k = 64 bits, for values T_C = 100 *ms*, 150 *ms* and 200 *ms*, is shown in Fig. 4.

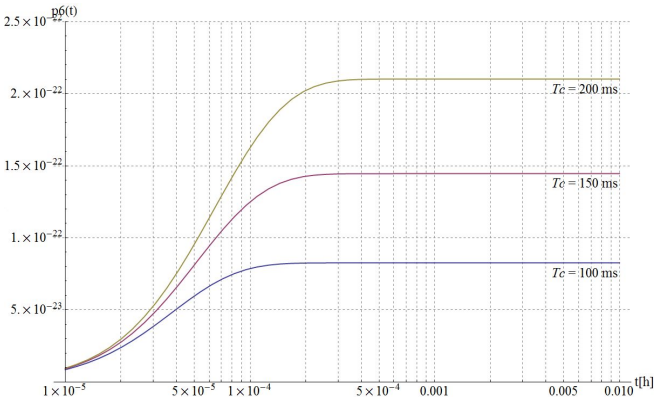

Fig. 5. Probability of undetected corrupted message for block size 256 bits.

The progress chart of the dependence of dangerous state probability and of the time for block size k = 256 bits, for values T_C = 100 *ms*, 150 *ms* a 200 *ms*, is shown in Fig. 5.

V. CONCLUSIONS

Cryptographic techniques are common security aids for decades in the area of so-called COTS technologies e.g. in the financial sector (banking, e-commerce), in office and in corporate information and communication systems and networks, but for the safety-related applications is their usage recommended only last few years. When choosing cryptographic techniques, activities and methods related to the key management for applications with higher levels of safety integrity is necessary to choose the procedures accord to the standards for transmission of safety-related messages via open transmission systems. This in many cases narrows the options of cryptography for safety-critical systems.

The authors were focused during the verification of results on the calculation of the most important coefficient – the dangerous failure rate of the system, which corresponds to the values in the table of SIL (according to [10]). In practice it is for the development of wireless safety-related devices for the need of industrial applications required SIL 3 (for example [22]). Therefore, the results gained from the model in Fig. 3 were compared with this value.

For all mentioned cases it was verified that the resulting value of failure rate caused by undetected message using combined communication system consist of safety and cryptography codes is in the range from 10^{-8} to 10^{-7} [h^{-1}] for messages with lengths $n = 10^1$, 10^3, 10^4, 10^5 bits. In case of longer messages $n = 10^8$ bits this range was not achieved. This is not a problem for safety-related applications as in most cases there are expected transmissions of short messages.

On the graphs it can be seen the progress of dangerous state probability (state 6) which was tested for different blocks of encrypted messages k and for different lengths of messages generated from the source n and consequent failure probability of cryptographic code decoder P_{UC}. Results are calculated assuming the worst case bit error rate of communication channel considering the BSC model (*Binary Symmetric Channel*) $P_b = 2^{-1}$ and for the worst case estimation of probability of undetected corrupted messages by transmission and safety code 2^{-r}. Reaction to a dangerous failure is in the system handled by the value of time T_C. In most cases (resulting from the implementation of the safety analysis from practice) the value T_C = 150 *ms* (the transmission system is set up to step into safe state after three false messages received). As it is evident from graphical results the curve shape of stepping into safe state $P_6(t)$ depend on the T_C parameter.

REFERENCES

[1] R. F. Stapelberga, *Handbook of reliability, availability, maintainability and safety in engineering design*, Springer-Verlag London Limited, 2009.

[2] M. Franekova, F. Kallay, P. Peniak, P. Vestenicky, *Communication safety of industrial networks*, EDIS, University of Zilina, Slovakia, 2007. (in Slovak).

[3] K. Rastocny, J. Zdansky, *Control system with safety PLC*, EDIS, University of Zilina, Slovakia, 2013. (in Slovak).

[4] J. Zahradnik, K. Rastocny, *Application of interlocking systems*, EDIS, University of Zilina, Slovakia, 2006. (in Slovak).

[5] M. Franekova, K. Rastocny, A. Janota, P. Chrtiansky, "Safety analysis of cryptography mechanisms used in GSM for railway", in *Int. Journal of Engineering: Annals of Faculty Engineering Hunedoara*, Romania, vol. 3, 2011.

[6] T. Malm, J. Herard, J. Boegh, M. Kivipuro, "Validation of safety-related wireless machine control systems", NT Technical report TR 605, Oslo, Norway, 2007.

[7] I. Zolotova, R. Hosak, M. Pavlik, "Supervisory control sustainability of technological processes after the network failure", *Elektronika ir Elektrotechnika (Electronics and Electrical Engineering)*, vol. 18, no. 9, pp. 3–6, 2012.

[8] I. Zolotova, L. Lacinak, T. Lojka, "Architecture for a universal mobile communication module", in *Proc. IEEE 11th Int. Conf. Int. Symposium on Applied Machine Intelligence and Informatics* (*SAMI 2013)*, Kosice, Slovakia, 2013. [Online]. Available: http://dx.doi.org/10.1109/SAMI.2013.6480945

[9] *EN 50159: Railway applications. Communication and signalling systems for data processing. safety-related communications in transmission system*, CENELEC, 2010.

[10] *IEC 61508: Functional safety of electrical, electronic, programmable electronic systems*, 2002.

[11] *IEC 61784-3-3: Industrial communication networks – profiles. Part 3-3: functional safety fieldbuses – additional specification for CPF 3*, 2010.

[12] *IEC 61784-4: Digital data communications for measurement and control. Part 4: Profiles for secure communications in industrial network*, 2011.

[13] M. Franekova, K. Rastocny, "Safety evaluation of fail-safe fieldbus in safety-related control system", *Journal of Electrical Engineering*, vol. 61, no. 6, p. 1–7, 2010. [Online]. Available: http://dx.doi.org/10.2478/v10187-010-0054-z

[14] K. Rastocny, K. Rastocny Jr., "UML – a part of an interlocking system development process", in *12th Int. Conf. Transport Systems Telematics (TST 2012)*, Katowice–Ustron, Poland, 2012.

[15] M. Franekova, "Mathematical apparatus for safety evaluation of cryptography and safety codes used in safety-related communication system", in *11th Int. Conf. on Modern Transport Telematics (TST 2011)*, Katowice–Ustron, Poland. Selected papers: Springer-Verlag. Berlin Heidelgerg series CCIS 104 – Communications in Computer and Information Science, pp. 126–135.

[16] L. Karna, S. Klapka, M. Harlenderova, "Quantitative assessment of safety code", in *Int. symposium FORMS/FORMAT*, Budapest, 2008, pp. 249–255.

[17] M. Franekova, M. Vyrostko, P. Luley, "Determination of error probability of cryptography and safety codes for safety-related railway applications", *Advances in Electrical and Electronic and Engeneering*, vol. 11, no. 2, p. 94–99, 2013.

[18] K. Rastocny, M. Franekova, "Modelling of safety properties of communication systems", *Scientific Journal Communications*, University of Zilina, Slovakia, pp. 24–30, 2008.

[19] M. Vyrostko, P. Luley, T. Ondrasina, M. Franekova, "Probabilistic error analysis of encrypted transmission for safety-related railway applications", in *9th Int. Scientific Conf. ELEKTRO 2012*, Rajecke Teplice, Slovakia, pp. 386–390.

[20] J. Torrieri, *Principles of Secure Communication Systems*. Artech House, Norwood, MA, USA, 1992.

[21] T. Ondrasina, "Safety mechanisms of wireless networks for industrial applications", Ph.D. dissertation, University of Zilina, Slovakia, 2011. (in Slovak).

[22] *Simatic HMI fail-safe operation of the mobile panel 277F IWLAN V2*, Siemens Germany 2010.