Adequacy Increase of Assessment of Minimal Cut Sets Considering Latent Failures

Leonid Ozirkovskyy, Bohdan Volochiy, Andriy Mashchak, Ihor Kulyk

***Abstract*—** This work proposes a new methodology for assessment of the average probability of minimal cut sets. This methodology deals with minimal cut sets assessed considering latent and evident failures or only latent failures. For latent and evident failures, the existing techniques provide the assessment only for the worst cases/scenarios. For only latent failures, the existing techniques provide significantly overstated values for the average probability of minimal cut sets. Such under/overstated assessment is not acceptable for the exploitation of the safety-critical radio-electronic system.

***Keywords*—**safety, minimal cut set, maintenance, latent failures, safety-critical system.

I. INTRODUCTION

In this paper, we discuss safety-critical radio-electronic system (SCRES). Exploitation of such systems is based on frequent but shot-term (up to several hours) cycles of usage [10, 11]. The main way to keep the required safety level during SCRES exploitation is the maintenance process [1]. Maintenance can be split into the two types of work:

- Corrective Maintenance (CM) – to restore the system and remove/correct the consequences after system sudden fail(s).
- Preventive Periodic Maintenance (PPM) – to remove gradual and parametrical system fails. Such type of maintenance decreases the number of sudden fails and, accordingly, decreases the frequency of the accident probability.

The rules and execution sequence of doing the CM and PPM form the strategy of the maintenance [1, 2]. The right selection of a maintenance strategy makes it possible to achieve the required safety level and required reliability level for SCRES.

The feature of the SCRES exploitation is that during SCRES task execution, parts of system elements and sub-modules are constantly controlled by the monitoring means. The monitored system elements and sub-modules are critical from the safety perspective. When a sudden fail occurs in the sub-systems and/or elements, the consequences are removed/neutralized by the fault tolerance means. The full system functionality is recovered by the service team during CM. It is stated that after CM in the systems, all identified fails are managed. Also, it is considered that after CM, the probability of an accident caused by a sudden failure is equal to zero [8]. The part of the SCRES elements and sub-modules is (can be) controlled by the monitoring means. These monitoring means can detect sudden failures. That is why failures that can be detected by the monitoring means are called “evident” failures. The other part of SCRES system including the reserve modules and elements is controlled and diagnosed very rarely. Failures in these elements and sub-modules can be detected only by the service team members during PPM and/or after a few cycles of the SCRES usage [3]. Let’s call such failures “latent” failures of the SCRES.

Therefore, from the safety perspective, there are two types of failures, during SCRES exploitation:

L. Ozirkovskyy, Lviv Polytechnic National University, Lviv, Ukraine.
B. Volochiy, Lviv Polytechnic National University, Lviv, Ukraine, (e-mail: bvolochiy@ukr.net).
A. Mashchak, Lviv Polytechnic National University, Lviv, Ukraine.
I. Kulyk, Lviv Polytechnic National University, Lviv, Ukraine.

- Evident failures that lead to SCRES accidents and catastrophic consequences;
- Latent failures that decrease the safety level of the SCRES. However, latent failures do not lead to SCRES accidents [3].

A problem occurs while doing an assessment of the accident probability (**Qreal**) on a period, shorter than the period between PPM [4]. Currently, a Fault Tree Analysis (FTA) is the main technique to do such an assessment [5]. It provides the possibility not only to do an assessment of the accident probability but also of minimal cut sets (MCS). Minimal cut sets – a combination of minimum failures of the system elements that leads the whole system to an accident [5, 6, 7]. A fault tree is built for every SCRES accident. Based on a built fault tree, a logical function is written. That logical function shows the dependency between the accident probability and failures of SCRES elements and sub-systems. If the accident probability is taken from this logical function, then the taken accident probability will have the value for the worst case $\mathbf{Q_{MAX}}$ (Fig.1) at the end of the time interval between PPM – T_{PPM}. For any interval of time $\mathbf{t < T_{PPM}}$, it is impossible to get a current accident probability using a fault tree analysis. And $\mathbf{Q_{MAX}}$ will be sufficiently overstated. This situation causes:

- Overestimation of the requirements for the SCRES elements reliability level
- Overestimation of the quantity for the reserve resources
- Decrease of the time interval between PPM.

As a result, the price, weight, size, maintenance increase.

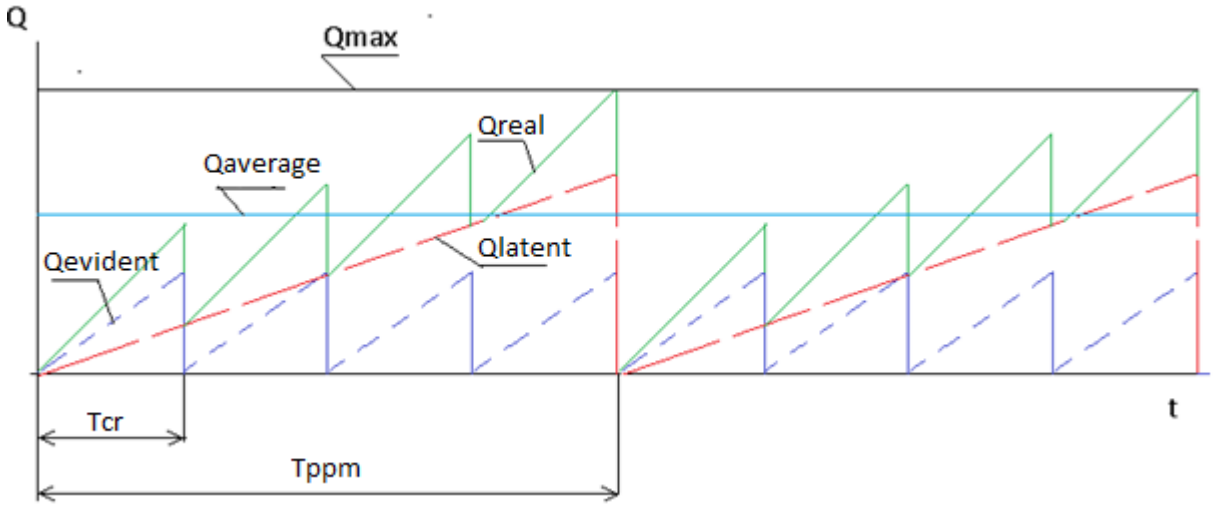


Fig. 1. Determination of the SCRES accident probability in case of having latent and evident failures

That is why in practice, during a safety quantitative assessment of SCRES that includes latent and evident failures, the **average accident probability index** is used **Q** for one SCRES cycle of usage or (for one hour of exploitation) [3, 4, 8]. The average accident probability is assessed considering the following:

Continuous monitoring captures the occurrence of evident failures, and before the time interval between PPM, these failures would be fixed/corrected by CM. A period of CM is typically equal to the mean time of one cycle of SCRES usage. If evident failures occurred during one cycle of SCRES usage, the service team starts execution of the CM. On the other hand, latent failures are detected and corrected once in a few tens or hundreds of cycles of SCRES usage – at the time period right before PPM ($\mathbf{T_{PPM}}$). At the end of this time, the service team does the PPM. During PPM, the latent failures are fixed.

During the first cycles of SCRES usage (when **t << T_{PPM})**, the probability of latent failures – **Qlatent** is typically drastically smaller than the probability of evident failures – **Qevident**. For the calculations, we can state that the probability of latent failures is equal to zero. And the sum probability of latent and evident failure probabilities is equal to the probability of a evident failure. At the end of the time between PPM (when **t = T_{PPM}**), the probability of latent failures increases and is significantly higher than the probability of evident failures (Fig.1). During the last cycle of SCRES usage on the time interval between PPM (**T_{PPM}**), the probability of a latent failure is maximal. Accordingly, the accident probability for the SCRES is maximal **Q_{max}**.

According to [3, 4, 8], to calculate **Qaverage** , the methodology with the following formula is proposed:

$$Q\text{average}\{q_1, q_2, \dots . q_m\} = \frac{\sum_{i=1}^{N} Qevident\{q_1, q_2, \dots . q_f\} \cdot Qlatent_i\{q_g, \dots . q_m\}}{N}, \quad (1)$$

where, $Qlatent_i$ – the probability of the latent failure, during the *i*-th cycle of SCRES usage, on the time interval while monitoring the following evident failure,

Qevident - the probability of the evident failure

q_j – the failure probability of low-level elements,

f - the quantity of low-level elements, which continuously monitored,

m – the quantity of low-level elements, which periodically monitored,

N – the quantity of time intervals on which the evident failures occurred, and these failures occurred on one-time interval of the monitoring for latent failures (**T_{PPM}**).

The same problem exists in minimal cut sets assessments. But, currently in present methodologies [3, 4, 5, 6, 7] no recommendations exist on how to do an assessment for the minimal cut sets probability on the time interval **t << T_{PPM}**. The methodologies in [6, 7] guarantee a valid value of the minimal cut sets probability only at the moment of the end of the time interval between PPM time t = T_{PPM}.

Therefore, it is important to investigate and develop a methodology for the minimal cut sets probability for time interval **t << T_{PPM}**.

II. Problem Statement

As it was said earlier, for an assessment of the average accident probability a known methodology exists presented by expression (1). However, minimal cut sets are assessed by traditional methodologies [3, 5, 6, 7] and these methodologies have significant disadvantages. The main disadvantage is the overstated value of the minimal cut sets probability if the system contains latent failures. To increase the credibility/adequacy of the minimal cut sets probability, coefficients are used to decrease the obtained probability of minimal cut sets [8]. However, in such a way, the adequacy of the results cannot be guaranteed.

That is why it is important to develop a methodology for assessment of the average probability of minimal cuts sets for cases with evident and/or latent failures.

III. Development of Methodology for Assessment of Average Probability of Minimal Cut Set Caused By Latent Failure

Before we start to form a methodology, let's review the following statements of the fault tree analysis. A fault tree is a graphical representation of a cause – effect relationships of undesired events (failures), which cause to accident. The tree is built from the top event (accident or other catastrophic system event) to the bottom by identifying all possible associated elements/events in the system which caused the top event to occur [5, 6]. Based on the built tree, the logical

function of the accident Q(x) is written down. The arguments for this function is the basic (lowest level) event (x_i) – the failure of a system element:

$$Q(x) = \Lambda_{j=1}^{R}(\mathrm{V}_{i=P_j} q_i), \qquad (2)$$

where $x = \{x_1, x_2, \ldots . x_s\}$ – a set of values of the base level – the failure of a system element;
Pj – the quantity of base-level OR elements connected to the j-th logical element
R – the quantity of base-level AND elements.

The accident logical function can contain a redundant quantity of the arguments. That is why it is important to do the minimization of this logical function [7, 13]. After the minimization, we obtain an equivalent logical function of the accident occurrence. The elements of such a function are minimal cut sets (3). Minimal cut sets (MCS) – a minimal combination of base-level elements of the system, failure of which will immediately cause an accident to occur to the system:

$$Q(x) = (x_1 \ldots x_d) \mathrm{V} (x_f \ldots x_h) \mathrm{V} \ldots \mathrm{V} (x_n \ldots x_s), \qquad (3)$$

The minimized equivalent logical function is also considered as a fault tree (3) because it is assessed from the accident logical function using Boolean algebra (2). This equivalent fault tree contains only two levels of the logic (Fig.2b): low base-level events are ANDed between themselves and then ORed at the top event. The events connected to the j-th AND element form one MCS.

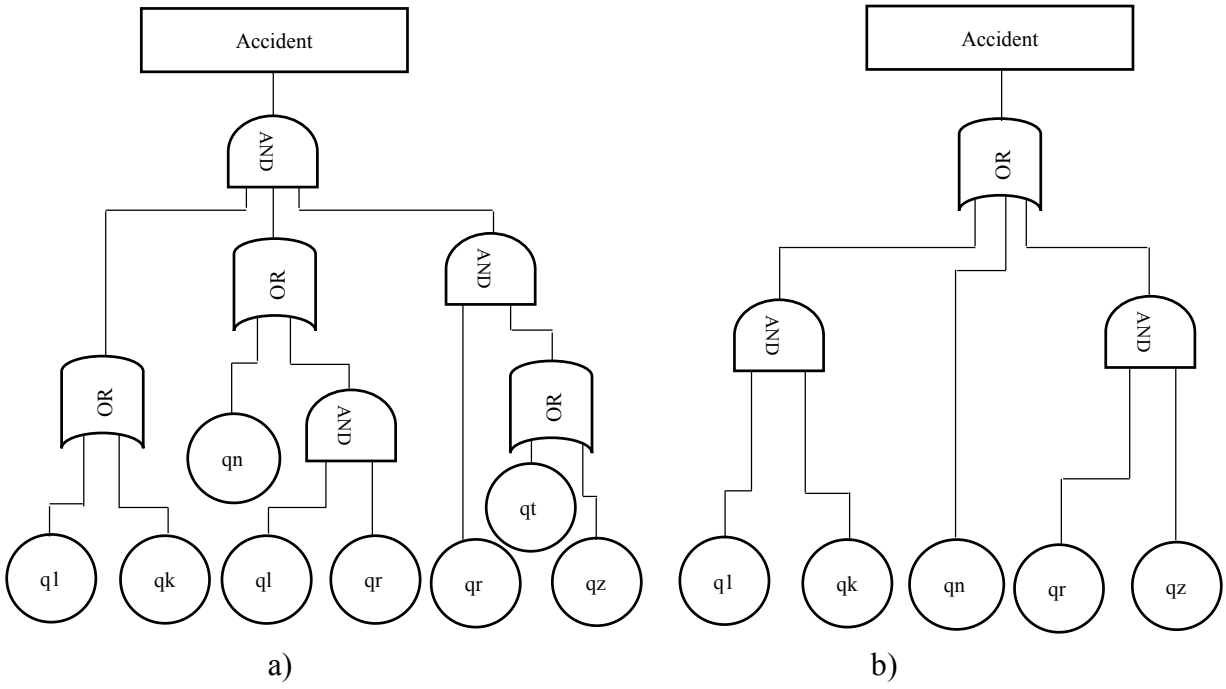


Fig. 2. Fault tree (a) and equivalent fault tree (b)

As the trees in Figure 2a and 2b are equivalent, expressions (2) and (3) are also equivalent and can be equaled:

$$Q(x) = \Lambda_{j=1}^{L}(\mathrm{V}_{i=P_j} q_i) = (x_1 \ldots x_d) \mathrm{V} (x_f \ldots x_h) \mathrm{V} \ldots \mathrm{V} (x_n \ldots x_s), \qquad (4)$$

To get the formula for calculating the accident rate probability Q(x) using the probabilities of system elements failures x= {q_1, q_2, … , q_f}, we need to do the following:

According to [9], if in (4) switch from base-level events x_i - *system elements failures as arguments of the logical function* to *probabilities of system elements failures*- q_i. Logical operands AND and OR should be changed to multiply and sum operands accordingly:

$$Q(x) = \sum_{j=1}^{K} MCS_j\{q_1, q_2, \ldots . q_f\} \qquad (5)$$

K – the number of minimal cut sets,
f – the number of base-level events included into the j-th minimal cut set.

Formula (5) and the equivalent fault tree (Fig. 2b) show that probabilities of the accident rate occurrence Q(x) are calculated as a sum of minimal cut sets probabilities under the condition that probabilities of base-level elements failures are independent events. Therefore, according to (1), the following statement is valid – **the average probability of the accident occurrence is equal to the sum of the average probabilities of the minimal cut sets:**

$$Qmean(x) = \frac{\sum_{i=1}^{N} Q_i(x)}{N} = \sum_{j=1}^{K} MCS\text{average }_j\{y\}, \qquad (6)$$

where x = {q1, q2, … , qf} – the base-level elements – failure probabilities included in the j-th minimal cut set;
f – the number of base-level events included in the j-th minimal cut set;
MCSaverage (y) – the average probability of the minimal cut set.
Let's assume that the average probability of the minimal cut set can be obtained using the following formula:

$$MCS\text{average }(y) = \frac{\sum_{i=1}^{N}\left((Le1\cdot \mathrm{T}_{CM})\cdot\ldots\cdot(Lek\cdot \mathrm{T}_{CM})\cdot(Ll1\cdot \mathrm{T}_{PPM_i})\cdot\ldots\cdot(Llr\cdot \mathrm{T}_{PPM_i})\right)}{N}, \qquad (7)$$

where Le – the intensity of the occurrence of evident failures
Ll – the intensity of the occurrence of latent failures;
T_{CM} – the average time between CM
T_{PPM} – the time interval between PPMs
i – the i-th cycle of SCRES usage
$N = T_{PPM}/T_{CM}$ – corresponds to the number of cycles of SCRES usage, a cycle is done during one-time interval while the latent failures are monitored
$Le\cdot T_{CM}$ – the probability of a evident failure [12]
$Ll\cdot T_{PPM}$ – the probability of a latent failure [12].

Thus, the final expression for the calculation of the average probability of the minimal cut set is as follows:

$$Qmean(x) = \sum_{j=1}^{Q} \frac{\sum_{i=1}^{N}\left((Le1\cdot \mathrm{T}_{CM})\cdot\ldots\cdot(Lek\cdot \mathrm{T}_{CM})\cdot(Ll1\cdot \mathrm{T}_{PPM_i})\cdot\ldots\cdot(Llr\cdot \mathrm{T}_{PPM_i})\right)_j}{N}, \qquad (8)$$

The methodology for calculating the average probabilities of the minimal cut sets is shown as a scheme in Figure 3.

IV. Validation of Methodology

Validation of the methodology was done on the assessment of the average probability of the accident occurrence while exploiting an unmanned aerial vehicle (UAV) [14]. The analyzed UAV has a redundant UAV control link.

The redundant UAV control link consists two channels. One is the primary channel and the secondary is a hot reserve. Both channels have a main receiver of operating configuration and a backup receiver (spare). The functionality of the main receiver is checked before each flight.

If the receiver of the operating configuration of primary channel fails during the flight, the secondary channel starts working instead. After switching to the secondary channel, the reserve receiver in the primary channel switches to the position of the main receiver. After such switching, this primary channel becomes a secondary channel but with a faulty reserve receiver. If the backup receiver was not switched to the main configuration, it is checked once per 1000 flights during a PPM.

After the flight is over (approximately 1-hour flight), CM is done to replace the failed receiver of the operating configuration of the main channel, if this receiver failed. If the receiver of the operating configuration did not fail, CM is not done. The backup receivers are not checked during CM.

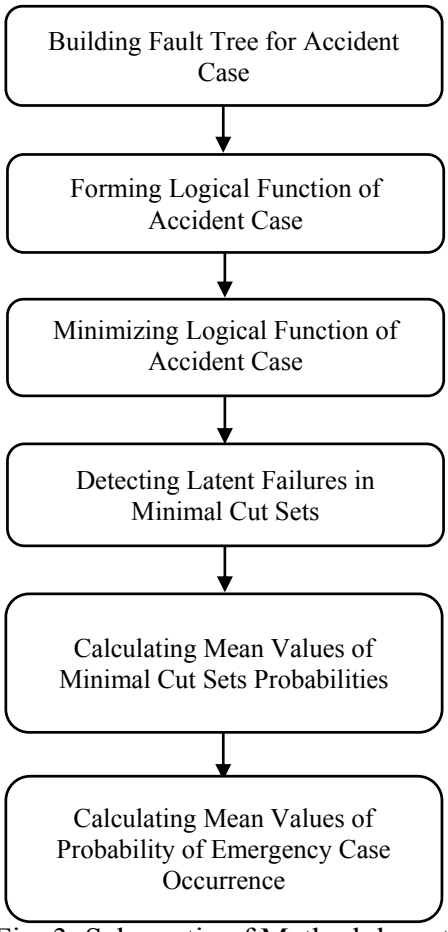


Fig. 3. Schematic of Methodology to Define Mean Values of Probabilities of Occurrence of Minimal Cuts

The fault tree of the redundant radio channel for UAV control is built in RAM Commander (Figure 4).

The calculations were done using the following inputs:

Le = 0,0001 hr $^{-1}$ – The failure rate of evident failures of the main receiver in Channel 1 and 2.

Ll = 0,00001 hr $^{-1}$ – The failure rate of latent failures of the main receiver in Channel 1 and 2.

N = 1000 – The quantity of using UAV on the interval of monitoring latent failures T_{PPM}.

$i := 1..N$ – The number of the current flight. The flight duration is 1 hour.

The probabilities of an occurrence of evident and latent failures in the given case are calculated with formula $P_{failure}(t) = L*t$. According to [9], this formula works for the case if the failure rates does not exceed 10^{-4} hr^{-1}. If failure rates is higher than 10^{-3} hr^{-1}, following expression is used $P_{failure}(t) = 1-e^{-L*t}$

$Pe_i = Le*t = Le*1$ – The probability of an occurrence of an evident failure of the main receiver during the i-th flight of UAV.

$Pl_i = Ll*i$ – The probability of an occurrence of a latent failure during the i-th flight. The assessment of the average probability of the accident occurrence was done in MathCAD according to the methodology shown in Figure 3.

According to Stage 3 of the RAM Commander methodology, minimal cut sets for the i-th were found which are represented below:

$$MCS1_i := (Le \cdot 1) \cdot (Le \cdot 1) \qquad MCS2_i := (Le \cdot 1) \cdot \frac{(Ll \cdot i)}{2} \qquad MCS3_i := (Ll \cdot i) \cdot \frac{(Le \cdot 1)}{2} \qquad MCS4_i := \frac{(Ll \cdot i)}{2} \cdot \frac{(Ll \cdot i)}{2}$$

Minimal cut set MCS1 contains only evident failures, minimal cut sets MCS2 та MCS3 contain one evident and one latent failure, and minimal cut set MCS4 contains two latent failures. The values of the probabilities of an occurrence of those minimal cut sets calculated in RAM Commander are shown in Table 1.

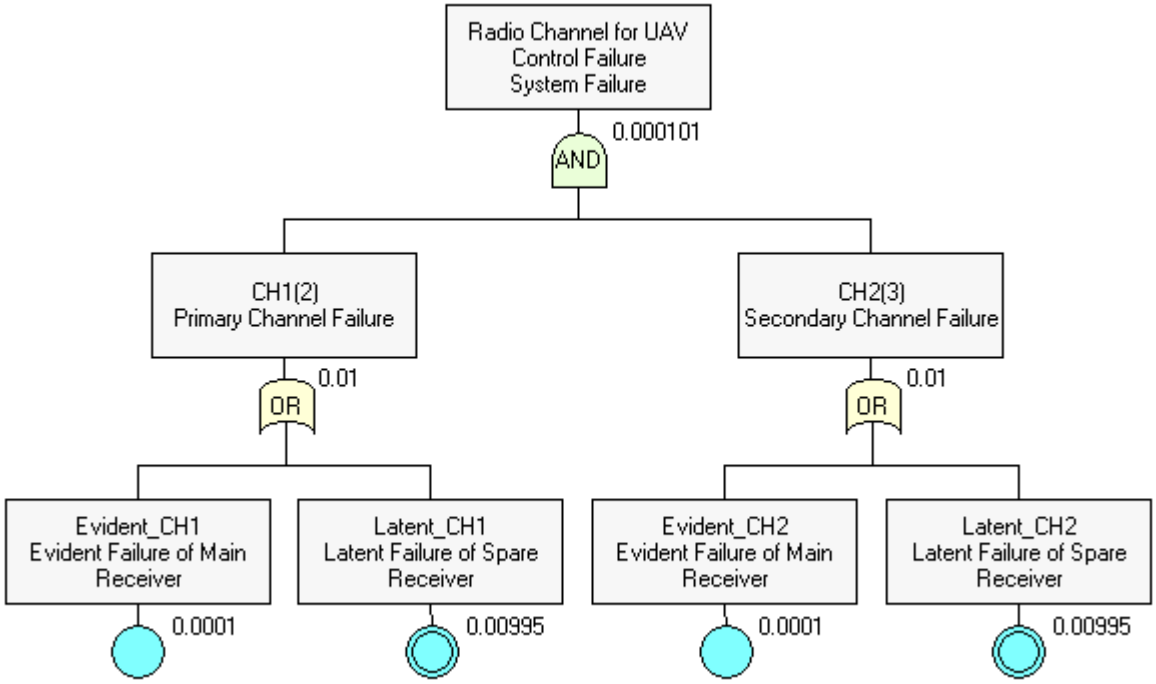
Table 1 Values of Probabilities of Occurrence of Minimal Cut Sets Calculated in RAM Commander

FTA - Minimal Cut Sets

Result for top event: Q(1000)=0.000101006 FTA Name: Example_1_ALD__2_channel_System_with_Evident_and_Latent_Basic_Ever

Minimal Cut Sets: Number of MCS: 4 / 4 Order of MCS: Min 2 Max 2

N	Q(t)	%	Order	Event 1	Event 2
1	9.90058e-005	98.0	2	Latent_CH1	Latent_CH2
2	9.94967e-007	1.0	2	Evident_CH1	Latent_CH2
3	9.94967e-007	1.0	2	Evident_CH2	Latent_CH1
4	9.999e-009	0.0	2	Evident_CH1	Evident_CH2



According to (7), the average values of the probability of an occurrence of minimal cut sets are calculated:

$$MCS1 := \frac{\sum_{i=1}^{N} MCS1_i}{N} = 10 \times 10^{-9} \qquad MCS2 := \frac{\sum_{i=1}^{N} MCS2_i}{N} = 2.503 \times 10^{-7}$$

$$MCS3 := \frac{\sum_{i=1}^{N} MCS3_i}{N} = 2.503 \times 10^{-7} \qquad MCS4 := \frac{\sum_{i=1}^{N} MCS4_i}{N} = 8.346 \times 10^{-6}$$

The calculation results show that the average value of the probability of an occurrence of a minimal cut set, which contains two evident failures, calculated in RAM Commander (Row 4, Table 1) and the average value of the probability of an occurrence of minimal cut set MCS1 calculated with formula (7) are identical/coincide. The values of the probabilities of an

occurrence of minimal cut sets that contain one evident and one latent failure are calculated in RAM Commander (Rows 2, 3, Table 1), and the average values of the probabilities of an occurrence of minimal cut sets that contain one evident and one latent failure MCS2, MCS3 calculated with formula (7) differ by 3 or 9 times, whereas RAM Commander gives overstated values of those probabilities. The values of the probabilities of an occurrence of minimal cut sets that contain two latent failures are calculated in RAM Commander (Row 1, Table 1) the average value of the probability of an occurrence of minimal cut sets MCS4 calculated with formula (7) differ by two orders (by 107,9 times), whereas RAM Commander gives a significantly overstated value of the probability of an occurrence of a minimal cut set.

The average probability of an accident occurrence is calculated according to (8):

$$Paverage\_MCS := MCS1 + MCS2 + MCS3 + MCS4 = 8.856 \times 10^{-6}$$

The average probability of accident occurrence is calculated according to (1):

$$Paverage := \frac{\sum_{i=1}^{N} Ptop\_event_i}{N} = 8.856 \times 10^{-6}$$

The calculated probabilities $P_{average}$ are equal from the comparison of the probabilities $P_{average}$, obtained using expression (1) and $P_{average}$ calculated using expression (1). Consequently, expressions (7) and (8) and the statement: **the average probability of the accident occurrence is equal to the sum of average probabilities of the minimal cut sets** is proven.

V. Conclusion

The proposed methodology increased the adequacy of the assessment for the average probability of minimal cut sets, if compared to calculations with the existing methodologies, under conditions that the methodology considers latent failures. The comparison of obtained values was done using the present methodologies implemented in the following software: RAM Commander, ReliaSoft BlockSim etc. Such an increase of the credibility is explained by the statement that in the known methodologies the probability, of an accident occurrence and the probability of minimal cut sets are assessed for worst cases. But the worst case is the last cycle of SCRES usage, when the accident probability is equal to the maximum value. The proposed methodology considers the condition that on the first cycles of SCRES usage the latent failures probability is close to zero in time interval $t << TPPM$. And in the next cycles of SCRES usage, the latent failures probability increase. As a result, in the latest cycle of SCRES usage the latent failures probability has the maximum value.

The calculated average probabilities of minimal cut sets that contain only latent failures differ from the average probabilities of minimal cut sets assessed by the known methodologies [7]. The difference is in from several times to even several orders. The difference increases along with the time interval PPM – T_{PPM} increase, and when the difference of the time interval increases between T_{CM} and T_{PPM}.

The obtained results also confirm the hypothesis that with having evident and latent failures evident failures make the same contribution to the accident probability on every cycle of SCRES usage. And on the time interval T_{PPM}, evident failures have bigger impact than latent failures. Latent failures practically are equal to zero on the first cycles of the SCRES usage. But when $t > 0{,}5T_{PPM}$, the impact from latent failures increases. And at the end of the monitoring time interval, this impact becomes dominant.

REFERENCES

[1] Ben-Daya M., Duffuaa S.O., Raouf A., Knezevic J., Ait-Kadi D., Handbook of Maintenance Management and Engineering, Springer-Verlag London Limited 2009

[2] Bohdan Volochiy, Leonid Ozirkovskyy, Ihor Kulyk, Designing of the effective maintenance strategies. Mathematical models, algorithms and techniques, LAP LAMBERT Academic Publishing, 2015 (in Russian)

[3] SAE ARP 4761. Guidelines and methods for conducting the safety assessment process on civil airborne systems and equipment, Society of Automotive Engineers, Inc., 1996

[4] AC/AMJ No: 25.1309 Federal Aviation Regulations (FAR)/Joint Airworthiness Requirements (JAR), 2002

[5] Henley, Ernest J., Hiromitsu Kumamoto: Probabilistic Risk Assessment: Reliability Engineering, Design and Analysis. 2 edition, Wiley-IEEE Press, 2000

[6] Marvin Rausand, Reliability of Safety-Critical Systems: Theory and Applications, Hoboken, New Jersey Wiley, 2014

[7] "Minimal cut set analysis. Appendix D", Guidelines for Chemical Process Quantitative Risk Analysis, Second Edition by Center for Chemical Process Safety, American Institute of Chemical Engineers, 2010

[8] Ramesh, A., "Average Probability Calculation Methods for System Safety Analysis," SAE Int. J. Aerosp. 8(2): pp. 214-226, 2015

[9] W. E. Vesely, F. F. Goldberg, N. H. Robert, D. F. Haas, Fault tree handbook, US Nuclear Regulatory Commission, Tech. Rep. NUREG 0492, 1981.

[10] David Smith, Kenneth Simpson The Safety Critical Systems Handbook. 4th Edition, Butterworth-Heinemann, 2016

[11] R. Pietrantuono, S. Russo "Introduction to Safety Critical Systems", Innovative Technologies for Dependable OTS-Based Critical Systems, Challenges and Achievements of the CRITICAL STEP Project, Springer-Verlag Italia, 2013, pp. 17 - 27

[12] A. B. Relcon, Risk Spectrum Theory Manual, 1998.

[13] Akinode, John Lekan, Oloruntoba S.A. "Algorithms for Reducing Cut Sets in Fault Tree Analysis", International Journal of Advanced Research in Computer and Communication Engineering, Vol. 6, Issue 12, December 2017

[14] Rana Abdallah Reliability approaches in networked systems : Application on Unmanned Aerial Vehicles, Université Bourgogne Franche-Comté, 2019