DESIGN OF ROAD VEHICLES COMPONENTS RESPECTING THE FUNCTIONAL SAFETY PRINCIPLES

Michal Richtář[1], Jakub Šmiraus[2]

Summary: This paper deals with the functional safety of road vehicles, especially the utilization of appropriate methods, procedures and models, in response to the new situation, coupled with the introduction of new standards. The paper was focused on the design of appropriate procedures and the utilization of qualitative and quantitative reliability analysis of motor vehicles selected systems, which significantly affect the road safety. To verify the actual levels of selected reliability parameters of equipment the reliability tests program has been created.

Key words: Functional safety, road vehicles, safety integrity level, mechatronic system.

INTRODUCTION

Road vehicles are complex devices that combine various branches of engineering. The result is a device composed of several subsystems that are interconnected and work together synchronously. When we look on their reliability and safety, it is necessary to access these subsystems as the elements of a coherent system. Evaluation of subsystems then usually makes separately. Application of certain principles of functional safety becoming increasingly penetrate into engineering practice and in vehicles. Selected procedures and tools for functional safety assessment, based on the principles of functional safety of electrical / electronic safety-related systems, as described in the standards EN 61508 and ISO 26262, have been chosen.

1. ANALYSIS OF TRAIN DRIVER VIEW

For the system functional safety assessment are using different methodologies, which are usually based on basic standard EN 61508 and DIN ISO 26262. One of the most pressing problems for the construction of road vehicles could be transition to determine safety and structural elements according to this standard, particularly in connection with the evaluation of the mechanical parts. This transition would probably mean taking over methodologies for determining the functional safety of electronic components with the necessary modifications.

[1] Ing. Michal Richtář, Ph.D., VŠB – Technical University of Ostrava, Faculty of Mechanical Engineering, Institute of Transport, 17. listopadu 15/2172, 708033 Ostrava - Poruba, Tel.: +420 597 321 229, Fax: +420, E-mail: michal.richtar@vsb.cz
[2] Ing. Jakub Šmiraus, VŠB – Technical University of Ostrava, Faculty of Mechanical Engineering, Institute of Transport, 17. listopadu 15/2172, 708033 Ostrava - Poruba, Tel.: +420 597 324 553, Fax: +420, E-mail: jakub.smiraus@vsb.cz

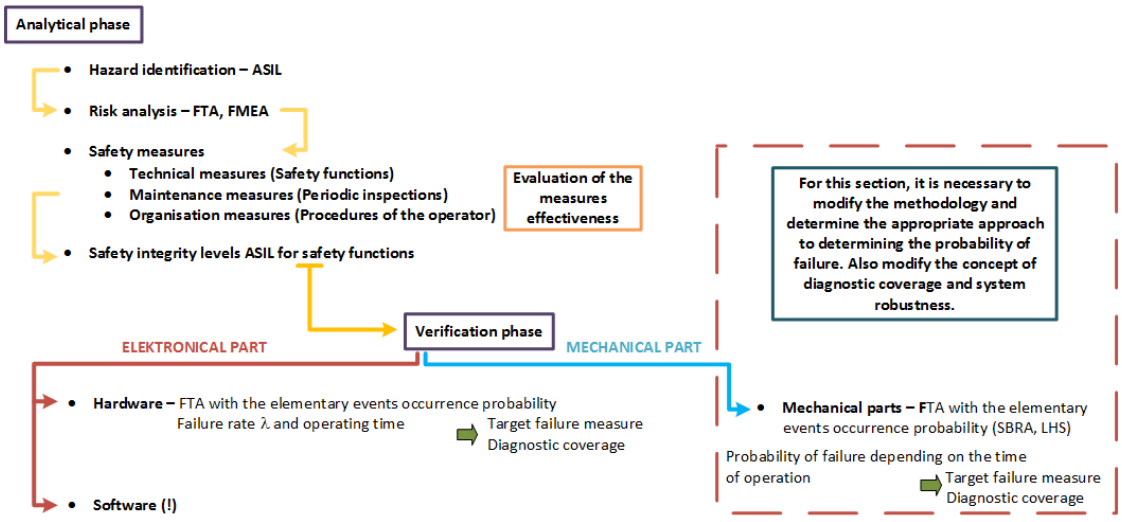
Another complicating component of this transition is evaluation of the diagnostic coverage for mechanical components.

Overall procedure of functional safety process consist of two main phases – the analytical phase and the verification phase.

Activities performed during the analytical phase should be implemented already in the design phase of a product, because of the need to minimize modifications to its structure and reduce the number of corrective action during production. Within the analytical phase the following steps are performed:

- Identification of hazards associated with the operation of equipment, and determination of the safety integrity level ASIL for considering risk.
- Risk analysis using appropriate methods (FTA, FMEA)
- Suggestion of the necessary security measures, typically technical (safety function), maintenance, organizational and legislative or external
- Evaluate the effectiveness of the proposed measures, repeating the risk analysis
- Set achievement level of safety integrity ASIL designed for safety functions

Activities performed during the verification phase leading to prove the reliability parameters of the system, such as to fulfill the requirements for the reduction of risks and to achieve the desired system security. This phase must include the necessary calculations to prove the desired target failure measures, including testing. Continuity of activities can be seen in graphical form in the corresponding segment in fig. 1.



Source: Author

Fig. 1 - Overall procedure of functional safety process

The necessary calculations include few basic parts – diagnostic coverage (DC), robustness Single Point Metric (SPM), robustness Latent Fault Metric (LFM), and target failure measure (PFH). In the process of verification is necessary to determine the diagnostic

coverage. Diagnostic coverage is split into diagnostic coverage with regard to residual faults (DC_{RF}) and diagnostic coverage with regard to latent multiple point faults (DC_{MPFL}).

Diagnostic coverage with regard to residual faults (DC_{RF}) indicates the efficiency of the diagnostic system and can be expressed as equation 1.

$$DC_{RF} = \left(1 - \frac{\lambda_{RF}}{\lambda}\right) \cdot 100 \tag{1}$$

where: DC_{RF} – diagnostic coverage with regard to residual faults [%]
λ_{RF} – failure rate associated to hardware element residual faults [h^{-1}]
λ – overall failure rate [h^{-1}]

Following parameter is robustness SPM (Single Point Metric). This metrics reflects the robustness of the item to single point faults either by coverage from safety mechanisms or by design. A high single point faults metric implies that the proportion of single point faults in the hardware is low. The definition is given by the following equation (2).

$$SPM = 1 - \frac{\sum\left(\lambda_{SPF} + \lambda_{RF}\right)}{\sum\lambda} \cdot 100 = \frac{\sum\left(\lambda_{MPF} + \lambda_{S}\right)}{\sum\lambda} \cdot 100 \tag{2}$$

where: λ_{SPF} – failure rate associated to hardware element single point faults [h^{-1}]
λ_{MPF} – failure rate associated to hardware element multiple point faults [h^{-1}]
λ_{S} – failure rate associated to hardware element safe faults [h^{-1}]
λ_{RF} – failure rate associated to hardware element residual faults [h^{-1}]

Following parameter is robustness LFM (Latent Fault Metric). This metrics reflects the robustness of the item to latent faults either by coverage of faults in safety mechanisms, by the driver recognizing or by design. A high latent fault metric implies that the proportion of latent faults in the hardware is low. The definition is given by the following equation (3) and the target values for ASIL levels are shown in tab. 1.

$$LFM = 1 - \frac{\sum\lambda_{MPFL}}{\sum\left(\lambda - \lambda_{SPF} - \lambda_{RF}\right)} \cdot 100 = \frac{\sum\left(\lambda_{MPFDP} + \lambda_{S}\right)}{\sum\left(\lambda - \lambda_{SPF} - \lambda_{RF}\right)} \cdot 100 \tag{3}$$

where: λ_{SPF} – failure rate associated to hardware element single point faults [h^{-1}]
λ_{MPFL} – failure rate associated to hardware element latent multiple point faults [h^{-1}]
λ_{MPFDP} – failure rate associated perceived or detected multiple point faults [h^{-1}]
λ_{S} – failure rate associated to hardware element safe faults [h^{-1}]
λ_{RF} – failure rate associated to hardware element residual faults [h^{-1}]

Tab. 1 - SPM a LFM target values for ASIL levels

Safety integrity level	ASIL B	ASIL C	ASIL D
Robustness SPM	> 90 %	> 97 %	> 99 %
Robustness LFM	> 60 %	> 80 %	> 90 %

Source: ISO 26262

In the process of verification is necessary to determine the target failure measure (PFH). Target failure measure (PFH) is a basic quantitative indicator of functional safety assessment of hardware safety-related systems in the context of the emergence of random failures. The calculation procedure is dependent on the mode of operation and the hardware architecture of the systems. The PFH target values for ASIL levels are shown in tab. 2.

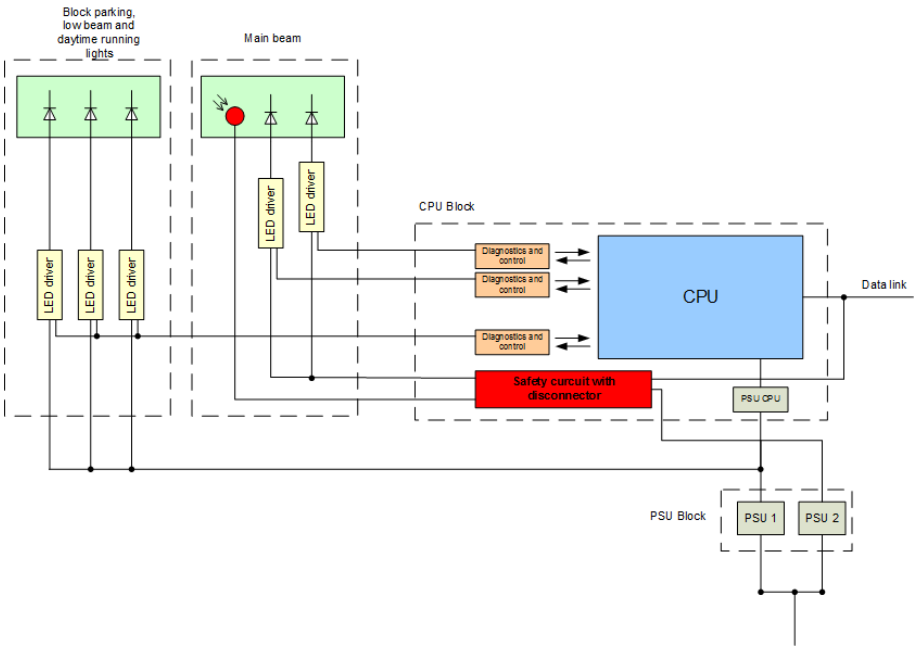
Tab. 2 - PFH target values for ASIL levels

Level ASIL	PFH target values [h-1]
D	$< 10^{-8}$
C	$< 10^{-7}$
B	$< 10^{-7}$
A	$< 10^{-6}$

Source: ISO 26262

2. APPLICATION OF THE FUNCTIONAL SAFETY PRINCIPLES TO LED HEADLAMP

The basic concept is given by a headlamp technical solution. The headlamp shall be divided into particular elements (subsystems). The headlamp is composed of a large number of LEDs, power supplies, control and diagnostic unit and the safety circuit with disconnector.



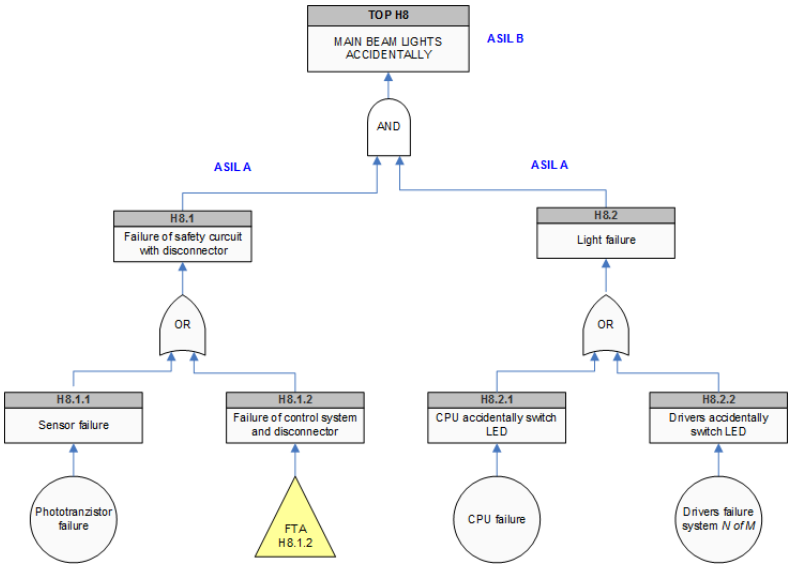
Source: Author

Fig. 2 - Block diagram of LED headlamps

2.1 Verification phase for LED

After input risk analysis a FTA models have been created. For example, FTA model in figure 3 represents the failure state, when main beam accidentally lights, ie hazard H8.

In terms of reliability are interlinked forming blocks of LED lights combined system. Branches H8.1 and H8.2 are arranged parallel, represent the backup system, the internal arrangement of the two branches is serial.



Source: Author

Fig. 3 - FTA for hazard H8

However, a group of LED drivers (part H8.2.2) is a system with a majority backup, specifically 5 good from the 6. Hazard H8 represents failure state, when main beam lights accidentally, FTA is shown in fig. 3. The aim of the calculation is to determine a target failure measure, ie. failure rate of the system. Drivers form a system with majority backup, puncture hazard occurs when two drivers of six are damaged. The safety circuit is parallel connected alongside the control circuit. Calculation of drivers block is in tab. 3 and calculation of the FTA model is in the tab. 4.

Tab. 3 - Calculation of drivers block – main beam

Input values		Calculation	
Drivers	6	Reliability $R_s(t)$	$9{,}99 \cdot 10^{-1}$
Driver operating time (h)	1000	Failure probability F(t)	$1{,}92 \cdot 10^{-5}$
Driver failure rate (h^{-1})	$3{,}33 \cdot 10^{-6}$	**Failure rate λ (h^{-1})**	**$1{,}93 \cdot 10^{-8}$**
Architecture *m* z *n*	4 ze 6		

Source: author

Tab. 4 - Calculation for hazard H8

Input values		Calculation	
Block	**F(t)**	**Gate**	**F(t)**
Phototransistor	$4{,}67 \cdot 10^{-4}$	H8.1.2	$3{,}05 \cdot 10^{-4}$
Driver	$1{,}43 \cdot 10^{-5}$	H8.1	$3{,}79 \cdot 10^{-4}$
CPU	$3{,}84 \cdot 10^{-4}$	H8.2	$4{,}03 \cdot 10^{-4}$
Disconnector	$3{,}60 \cdot 10^{-4}$	TOP	$1{,}53 \cdot 10^{-7}$
Control logic	$1{,}84 \cdot 10^{-4}$	**λ (h^{-1})**	**$1{,}53 \cdot 10^{-7}$**

Source: author

Circuit solution for hazard H8 meets target failure rate at ASIL B, as could be seen by comparison with the tab. 2.

2.2 LED accelerated test plan

The aim of this part is creation of LED accelerated test plan and verification of target failure measure and reliability in life cycle profile. Accelerated test is based on test plans and factor of acceleration using Arrhenius model has been calculated.

According the vehicle life cycle profile is LED life span calculated for 8 years (about 70000 hours) and lighting time 8000 hours. The test is partitioned between two parts, because the test must model the situation when the light is on (under voltage) and when it is off (without voltage).

Tab. 5 Operational and test temperatures

Mode of operation	**Test temperature (°C)**	**Operational temperature (°C)**	**Difference (°C)**
under vaoltage	90	50	40
without voltage	90	20	70

Source: author

For accumulated test time equation 4 has been used. Required target failure measure comes from the standards and determines T_D. On the confidence level C = 0.7 the test has been evaluated (minimum value by standards) and no failure occurs during test has been assumed. Using equation (4) the accumulated test time is $1{,}2 \cdot 10^6$ hours.

$$T_D \geq \frac{2 \cdot t_{AKU}}{\chi^2_{2\nu;C}} \tag{4}$$

where: T_D - lower limit of confidence interval. [h],
t_{AKU} - accumulated test time [h],
χ^2 - value of chi-square distribution [-].

Factor of acceleration is for Arrhenius model described by equation 5.

$$A_F = \frac{L_U}{L_A} = \frac{C \cdot e^{\frac{B}{T_U}}}{C \cdot e^{\frac{B}{T_A}}} = e^{B \cdot \left(\frac{1}{T_U} - \frac{1}{T_A} \right)} \tag{5}$$

where:
A_F - factor of acceleration [-],
L_U - reliability indicator at operating load [h],
L_A - reliability indicator at increased load [h],
T_U - load in operating conditions [K],
T_A - increased test load [K],
K - Bolzman constant [$eV.K^{-1}$],
C - model parametr,
B - model parametr.

Activation energy for all tested component is on the same level, and comes from manufactures data. Results of calculations are shown on tab. 6.

Tab. 6 Factor of acceleration for modes of operation

Input parameters		**Mode of operation**	**Test temperature T_A**	**Operational temperature T_U**	**Factor of acceleration A_F**
			(K)	**(K)**	**(-)**
E_A (eV)	0,876	under voltage	363	323	32
K ($eV \cdot K^{-1}$)	8,62E-05	without voltage	363	293	805

Source: author

2.3 Test profile design

The test is partitioned between two parts. In the first part LED block works under voltage with temperature 90 °C. The test is passed, if at least *m* of *n* diodes lighting. Test time is calculated using equation 6.

$$T_l \geq \frac{t_{AKU}}{n \cdot A_{FS}} \tag{6}$$

where:
T_l - test time [h],
t_{AKU} - accumulated test time [h],
n - number of tested components [-],
A_{FS} - factor of acceleration [-],

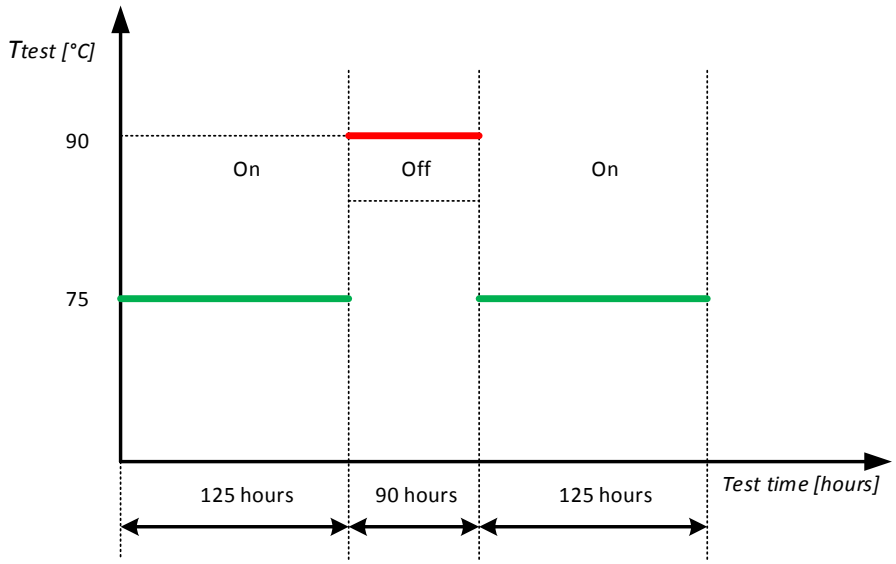
Test time for 10 LED blocks is 3450 hours and more.

The second part is concerned to verification of reliability in life cycle profile. Requirement of life span is defined is defined such that after the life span 5 of 10 products must be in faultless state. Test simulate state, when the headlamp is on (8000 hours) and when is off (72000 hours). Test time is calculated using equations 7 and 8.

$$T_{2S} = \frac{t_{on}}{A_{FS}} \tag{7}$$

$$T_{2N} = \frac{t_{off}}{A_{FN}} \tag{8}$$

where:
- T_{2S} - test time, under voltage [h],
- t_{on} - time of lighting [h],
- A_{FS} - factor of acceleration, under voltage [-],
- T_{2N} - test time, without voltage [h],
- t_{off} - time – light is off [h],
- A_{FN} - factor of acceleration, without voltage [-],



Source: author

Fig. 4 Test profile of LED

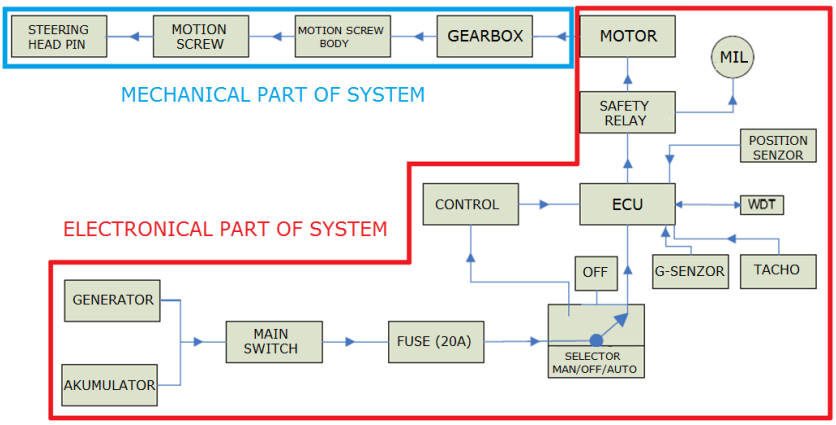
Test time for second part of test is at least 340 hours, 5 LED blocks of 10 must be in faultless state. Test profile is shown on fig. 4. Both test parts have a different test times. It is evident, that the requirements to verification of reliability in life cycle profile are easier than requirements to verification of ASIL level.

3. APPLICATION OF THE FUNCTIONAL SAFETY PRINCIPLES TO MOTOCYCLE MECHATRONIC SYSTEM

Functional safety of mechatronic motorcycle system, which regulate the chassis parameters is also is given by a system technical solution. The basic step is decomposition to the electronic and mechanical system. The electronic part in this case consists of a control system (selector), electronic control unit and accessories (position sensor, acceleration sensor, etc.) and power supply parts (accumulator, generator and wiring). The mechanical part consists of pins and bearings, linear motion screw, gearbox and the electric drive. The diagnostics of system ensures safety cut-off relay which controls the actuator position and sensors output signal. In the case of conflict for more than a defined interval, cut-off relay

disconnect the system and switch warning light on MIL. The diagnostic system is not considered simultaneously with the calculation of functional safety. It is not provided with any backup, only security functions in a safe state

3.1 Architecture of mechatronic system

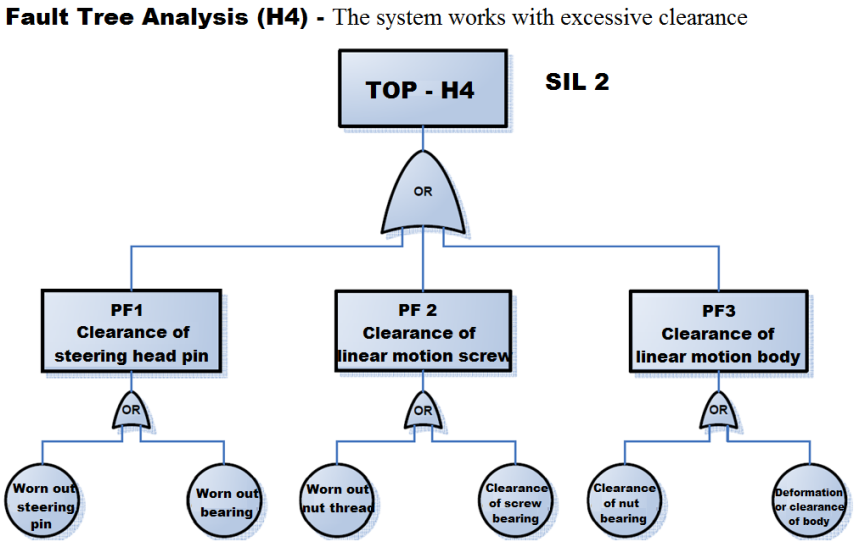


Source: author

Fig. 5 - Block diagram of solved motorcycle mechatronic system VGP

Fault tree analysis in fig. 6 represents a failure state, when the device works with the clearance, which can´t be detected by safety cut-off relay. This clearance will may cause vibrations, which in extreme cases can cause loss of motorcycle stability or crash. This case (Hazard 4) leads to safety integrity level requirement at level ASIL B. Is possible to replace this FTA expression by serial system (RBD) of mechanical elements. The procedure for determining the SIL electronic part is set in the previous solution of LED headlamp. For mechatronic system is exactly the same, so there will not be shown.

For mechanical elements the failure probability of individual system components cannot be simply obtained. However we can use the failure rate. For mechanical components such as bearings, joints or motion screws the manufacturers' data can be used. In case that it is necessary to determine the failure rate of unknown or untested components, basically by two ways the required data can be obtained.

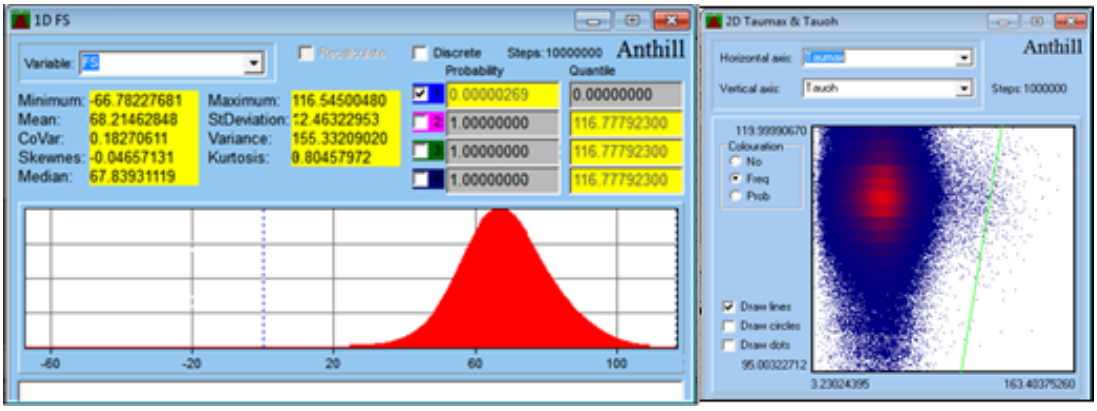


Source: author

Fig. 6 - FTA for Hazard 4 (H4) (only mechanical parts)

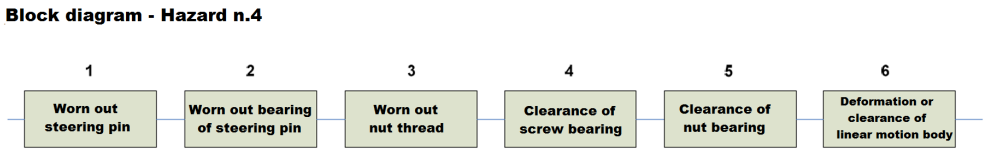
3.2 Failure intensity determination of mechanical elements

At first can be obtained by reliability tests, at second by suitable mathematical model. The ideal choice is a mathematical method Monte Carlo or PPDV. In engineering practice is often used method SBRA (Simulation-Based Reliability Assessment). The advantage of this method is low computation time, but is demanding on computing power of the PC. The method calculates the probability of achieving the expected result. However, inputs for calculation are entered in the form of failure probability for life interval in the form of histograms. The input parameters for the calculation are the random quantities (geometrical and material characteristics, load ...) expressed by histograms like fig. 7.



Source: author

Fig.7 - Example of probability calculation of clearance generation due to linear motion body deformation using Anthill (condition Fs = $\tau_{Dov} - \tau_{vyp}$, Fs > 0 = satisfied)



Probability of matrix deformation is $2{,}69.10^{-6}$. Similarly probabilities of the other elements are calculated and is possible to calculate the final probability of H4.

$$Rc_{(t)} = R1_{(t)}.R2_{(t)}.R3_{(t)}.R4_{(t)}.R5_{(t)}.R6_{(t)} \quad (9)$$

$$Rc_{(t)} = (1-(8{,}09.10^{-1})).(1-(5{,}82.10^{-1})).(1-(1{,}19.10^{-1})).(1-(1{,}46.10^{-1})).(1-(2{,}69.10^{-1})).(1-(8{,}04.10^{-1}))$$

$$Rc_{(t)} = 0{,}999996279$$

$$F(t)=1-R(t) \quad (10)$$

Using the equation 10 the final probability $P_{H4} = 3{,}7212.10^{-6}\ h^{-1}$ of hazard H4 has been calculated. The target failure measure must for ASIL B be less than $10^{-7}\ h^{-1}$, but calculated value is $3{,}7212.10^{-6}\ h^{-1}$. The device does not met the requirements and is necessary to make design changes of the system. It is not necessary to proceed the diagnostic coverage evaluation, because of uncompliant target failure measure calculation.

4. CONCLUSIONS

The content of this paper is the functional safety of road vehicles, in particular the use of appropriate methods, procedures and models in relation to the new situation, associated with the implementation of new standards. The paper was focused on the design of appropriate procedures and utilization qualitative and quantitative reliability analysis of selected systems of road vehicles that significantly affect road safety.

For functional safety assessment procedures and tools have been selected, which are based on the principles of functional safety of systems, as described in the standards EN 61508 and ISO 26262.

Diagnostic coverage is not sufficiently solved for mechanical (mechatronic) system. Problems of diagnostic coverage will be subject of another scientific activities of the authors of this paper. Complete methodology for diagnostic coverage determination can be possible to apply the whole methodology of determining SIL on all mechatronic systems. This results can fill the gap of the ASIL determination process for complicated vehicle systems.

REFERENCES

(1) ISO 26262-1. *Road vehicles – Functional safety* – ICS 43.040.10 , 2011. International Organization for Standardization

(2) ČSN EN 61508-1. *Funkční bezpečnost elektrických/elektronických/ programovatelných elektronických systémů souvisejících s bezpečností* - Praha :Český normalizační institut, 2002

(3) MAREK, P.; GESTAR, M.; ANAGNOS, T. *Simulation-based Reliability Assessment for Structural Engineer*, CRC Press, Boca Raton, 1996, 365 s. ISBN 0-8493-8286-6.

(4) KECECIOGLU, D. *Reliability & Life Testing Handbook*, Volume 2. Englewood Cliffs : PTR Prentice Hall, 1994. 859 s. ISBN 0-13-772369-5.

(5) FRYDRÝŠEK, K. *Pravděpodobnostní výpočty v mechanice* 1, VŠB- TU Ostrava, 2010