SOUČASNÉ PROBLÉMY V KOLEJOVÝCH VOZIDLECH

XXV. konference s mezinárodní účastí
15.–17. září 2021, Česká Třebová

FUNCTIONAL SAFETY PROBLEMATICS OF VEHICLES IN RELATION TO THE SAFETY RELATED REQUIREMENTS OF THE SAFETY INTEGRITY LEVEL

PROBLEMATIKA FUNKČNÍ BEZPEČNOSTI VOZIDEL V NÁVAZNOSTI NA BEZPEČNOSTNÍ POŽADAVKY ÚROVNĚ INTEGRITY BEZPEČNOSTI

Michal RICHTÁŘ[1], Jan FAMFULÍK[2], Jaromír ŠIROKÝ[3], Jakub ŠMIRAUS[4], Jana MÍKOVÁ[5]

Abstract
The article deals with current aspects of a significant part of the field of reliability, namely the issue of functional safety of railway vehicles in relation to the safety related requirements and system hardware architecture. This area is of course governed by a number of standards, but in this area and the application level, especially the standards EN 61508 and EN 50129. The fundamental steps related to the approval of vehicles and their components in terms of functional safety in this article have been described. Furthermore, the work with hardware architectures in connection to the safety related requirements of the safety integrity level SIL has been shown.

Keywords
functional safety, railway vehicles, reliability, hardware architectures

Abstrakt
Příspěvek se zabývá aktuálními aspekty významné části oblasti spolehlivosti, a to problematikou funkční bezpečnosti kolejových vozidel v návaznosti na požadavky na bezpečnost a hardwarovou architekturu systému. Tato oblast je pochopitelně řízena řadou norem, v této oblasti a aplikační rovině však především o mateřské normě EN 61508 a EN 50129. V příspěvku jsou představeny zásadní kroky související se schvalováním vozidel a jejich komponent z pohledu funkční bezpečnosti. Dále je ukázána práce s architekturami hardwaru v návaznosti na bezpečnostní požadavky úrovně integrity bezpečnosti SIL.

Klíčová slova
funkční bezpečnost, vozidla, spolehlivost, architektury hardware

[1] **Ing. Michal Richtář, Ph.D.**, VŠB – TU Ostrava, Fakulta strojní. Institut dopravy, 17. listopadu 15, 708 00 Ostrava – Poruba. Tel.: +420 596 991 229, e-mail: michal.richtar@vsb.cz
[2] **doc. Ing. Jan Famfulík, Ph.D.**, VŠB – TU Ostrava, Fakulta strojní. Institut dopravy, 17. listopadu 15, 708 00 Ostrava – Poruba. Tel.: +420 596 994 553, e-mail: jan.famfulik@vsb.cz
[3] **Ing. Jaromír Široký, Ph.D.**, VŠB – TU Ostrava, Fakulta strojní. Institut dopravy, 17. listopadu 15, 708 00 Ostrava – Poruba. Tel.: +420 596 994 375, e-mail: jaromir.siroky@vsb.cz
[4] **Ing. Jakub Šmiraus, Ph.D.**, VŠB – TU Ostrava, Fakulta strojní. Institut dopravy, 17. listopadu 15, 708 00 Ostrava – Poruba. Tel.: +420 596 994 553, e-mail: jakub.smiraus@vsb.cz
[5] **Ing. Jana Míková, Ph.D.**, VŠB – TU Ostrava, Fakulta strojní. Institut dopravy, 17. listopadu 15, 708 00 Ostrava – Poruba. Tel.: +420 596 994 553, e-mail: jana.mikova@vsb.cz

1 INTRODUCTION

Functional safety is a term that has appeared in the field of technical systems only in recent years. Its importance for the processes of design and documentation phases of technical systems functional safety is considerable. The application of some principles of functional safety is beginning to penetrate more and more into technical practice in the field of transport.

Generally, some functional safety requirements are specified by the parent standard EN 61508 – Functional safety of electrical/electronic/programmable electronic safety related systems. In some technical areas, also a branch standard has been introduced and extend the requirements of this parent standard EN 61508.

There are own industry standards also in the field of rolling stock, known as EN 50128 Railway applications – Communication, signaling and processing systems – Software for railway control and protection systems and EN 50129 Railway applications – Communication, signaling and processing systems – Safety related electronic systems for signaling, which are intended to apply the requirements of the parent standard for railway vehicle technical systems.

However, standard EN 50129 does not specify useable computing procedures necessary to demonstrate the credibility of probability of hardware random failures, which may lead to problems in vehicle area. These standards are dedicated to solve functional safety problems of communication, signaling and processing systems, not exactly safety related problems of vehicles.

Utilization of different computational procedures is possible as will be shown. Firstly, the parent standard EN 61508 can be utilized, but also exist other suitable calculating procedures. The computations can be based on the application of FTA model. This method is often elaborated, e.g., literature [7,8]. In the field of functional safety, the FTA model is elaborated according to EN 61508 in Rausand and Høyland [9].

Obviously, this is not the only possible approach, there are other computational methods, such as RBD analysis, Markov analysis, which is also properly utilized. Probabilistic assessment of mechanical components because the important part of vehicle safety also by mechanical components must be covered [10,11], but this important problematic is not described in this paper. Also, the utilization of random vector as a very suitable computational method for functional safety assessment is possible [12]. The utilization of FTA analysis leads to relatively simple computational formulas and simplifies the procedures required to perform a qualitative analysis of the assessed system.

2 FUNCTIONAL SAFETY PROCESS

Overall process of functional safety is based on the sequence of related activities. These related activities form the parent standard EN 61508 can be obtained, in connection to safety lifecycle, but also in case of utilization of branch standards, modified lifecycles can be used.

Above mentioned related activities, which fulfilling the functional safety process by the following activities will be realized. Some of activities are based on quantitative and some on qualitative methods.

First activity is known as the Hazard log process. Hazard log for record of all hazards, related to assessed item or part of railway vehicle, will be used. The Hazard log team assessing all possible failures of item and their influence to safety. So important note is that all suppliers and customers must be a part of Hazard log team to eliminate lack of information about the hardware failures on both sides (supplier and customer). Hazard log also for SIL (Safety Integrity Level) determination is utilized. It is also a mandatory part of the functional safety documentation. The SIL reaches following levels of safety impact: SIL 0 = insignificant impact, SIL 1,2 = marginal impact, SIL 3 = critical impact, SIL 4 = catastrophic impact.

Using Hazard log process the SIL has been determined. Depending on the SIL level and thus the risk level, by appropriate measures risk must be reduced. Risk reduction measures should also

be proposed as part of the risk assessment [13]. The measures are designed separately or on the basis of other used methods (FTA analysis and FMEA analysis). The measures are divided into groups according to their nature, technical measures, measures realized by an external system, maintenance measures and organizational and legislative measures. The most important measures are the technical measures, known as the safety function. These safety functions are implemented into the hardware and software application level and reducing achieved risk.

Following activities utilize for example the FTA (Fault Tree Analysis) method to create the reliability model of the machine. Without the reliability model of the machine is not so easy to understand the relations between item failures and how to assess their impact to hazard event. Created FTA is obviously important for the final activity of the functional safety process, known as the proof of safety. The proof of safety process utilizes calculations based on mathematical theory of statistics and considering all safety related components. The appearance of the fault tree is, of course, influenced by the hardware architecture of the system.

3 HARDWARE ARCHITECTURES

Respecting the basic electrical architectures, known as a serial system and parallel system, also the reliability models utilize these systems. Obviously for relation between items in the reliability model also system *koon* can be applied. In our article only serial and parallel systems will be considered because of simplification.

Depending on architectures the target values of reliability and functional safety in the proof of safety will be calculated. The target values are:

PFD_G – Probability of failure on demand (for systems with low demand – for railway restricted)

PFH_G – Probability of failure per hour (for systems with high demand)

With regards to calculation of target values, related failures of item must be considered (see Fig. 1). The diagnostic system of safety function must detect defined percentage of all failures, and due this reason all failures to following groups can be divided:

λ_{SD} – Safety detected failure rate [h^{-1}]

λ_{SU} – Safety undetected failure rate [h^{-1}]

λ_{DD} – Dangerous detected failure rate [h^{-1}]

λ_{DU} – Dangerous undetected failure rate [h^{-1}]

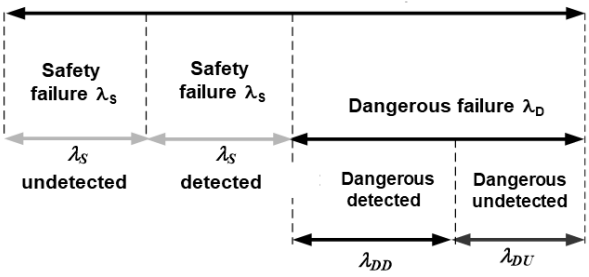

Fig. 1 Failure rate groups

In the area of railway vehicles, the branch standard EN 50128 and EN 50129 for functional safety assessment has been declared. Despite that application problems of utilization of standard EN 50129 in the introduction of this article has been mentioned. Standard EN 50129 does not specify useable computing procedures necessary to demonstrate the credibility of probability of hardware random failures. Furthermore, according to the authors of this article it is impossible to solve more complex hardware architectures with this methodology. Similar situation in different vehicle functional safety areas can be found [14].

In this situation, it is possible to refer to the parent standard EN 61508 or try to apply different procedure, as will be shown below.

3.1 Serial system 1oo1

Serial system, also known as system 1oo1 (without redundancy), is typical hardware architecture. One failure in the chain of safety function causes failure of the all system.

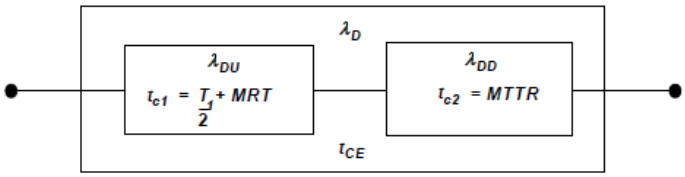

Fig. 2 Serial system architecture 1oo1 according the EN 61508

Architecture of this system in relations to failure rates and mean time of channel downtime according EN 61508 is described on Fig. 2. Probability of failure on demand PFD_G (for systems with low demand) according equation (1) can be calculated.

$$PFD_G = (\lambda_{DU} + \lambda_{DD}) \cdot t_{CE} \tag{1}$$

Where PFD_G – Probability of failure on demand (for systems with low demand [h^{-1}], λ_{DD} – Dangerous detected failure rate [h^{-1}], λ_{DU} – Dangerous Undetected failure rate [h^{-1}], and t_{CE} – Mean time of channel downtime [h].

The mean time of channel downtime t_{CE} according equation (2) can be calculated.

$$t_{CE} = \frac{\lambda_{DU}}{\lambda_D} \cdot \left(\frac{T_1}{2} + MRT\right) + \frac{\lambda_{DD}}{\lambda_D} \cdot MTTR \tag{2}$$

Where T_1 – interval of monitoring of safety function [h], MRT – mean repair time [h], MTTR – mean time to recovery [h].

Probability of failure per hour (for systems with high demand) according equation (3) can be calculated.

$$PFH_G = \cdot \lambda_{DU} \tag{3}$$

Where PFH_G – Probability of failure per hour (for systems with high demand) [h^{-1}], λ_{DU} – Undetected safety failures [h^{-1}].

The described equations are confusing and complicated. Defined times MRT and MTTR are incorrectly defined.

3.2 Parallel system 1oo2

Parallel system, also known as system 1oo2 (with redundancy), is also typical hard ware architecture. Two failure in the chain of safety function means failure of all system.

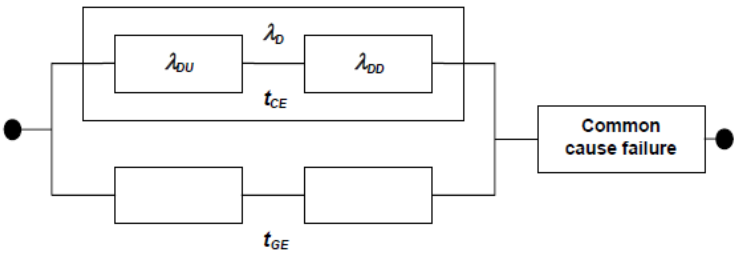

Fig. 3 Parallel system architecture 1oo2 according the EN 61508

Architecture of this system in relations to failure rates and mean time of channel downtime is described on Fig. 3. Probability of failure on demand PFD_G (for systems with low demand) according equation (4) can be calculated.

$$PFD_G = 2 \cdot \left((1-\beta_D) \cdot \lambda_{DD} + (1-\beta) \cdot \lambda_{DU}\right)^2 \cdot t_{CE} \cdot t_{GE} + \beta_D \cdot \lambda_{DD} \cdot MTTR + \beta \cdot \lambda_{DU} \cdot \left(\frac{T_1}{2} + MRT\right) \quad (4)$$

Where PFD_G – Probability of failure on demand (for systems with low demand [h^{-1}], β_D and β – common caused failures coefficients [-].

The mean time of channel downtime t_{CE} according equation (2) can be calculated.

$$t_{CE} = \frac{\lambda_{DU}}{\lambda_D} \cdot \left(\frac{T_1}{2} + MRT\right) + \frac{\lambda_{DD}}{\lambda_D} \cdot MTTR \quad (5)$$

Where T_1 – interval of monitoring of safety function [h], MRT – mean repair time [h], MTTR – mean time to recovery [h].

The mean time of group downtime t_{GE} according equation (6) can be calculated.

$$t_{GE} = \frac{\lambda_{DU}}{\lambda_D} \cdot \left(\frac{T_1}{3} + MRT\right) + \frac{\lambda_{DD}}{\lambda_D} \cdot MTTR \quad (6)$$

Where T_1 – interval of monitoring of safety function [h], MRT – mean repair time [h], MTTR – mean time to recovery [h].

Probability of failure per hour PFH_G (for systems with high demand) according equation (7) can be calculated.

$$PFH_G = 2 \cdot \left((1-\beta_D) \cdot \lambda_{DD} + (1-\beta) \cdot \lambda_{DU}\right) \cdot (1-\beta) \cdot \lambda_{DU} \cdot t_{GE} + \beta \cdot \lambda_{DU} \quad (7)$$

Where PFH_G – Probability of failure per hour (for systems with high demand) [h^{-1}], β_D and β – common caused failures coefficients [-].

The described equations are confusing and complicated, the method of their derivation is very unclear from the reliability point of view. Defined times MRT and MTTR are incorrectly defined.

Beta coefficients are determined on the basis of subjective evaluation using tables in the standard.

4 FTA UTILIZATION APPROACH

The utilization of fault trees (FTA) looks like a slightly cleaner system of calculation. System is based on calculation of average probability of failure F_{AVG} and this probability relative to operating time gives target value probability of failure per hour PFH_G.

In general, the average probability F_{AVG} according to equation (8) can be calculated and target value probability of failure per hour PFD_G according to equation (9) can be calculated.

$$F_{AVG} = \frac{1}{t}\int_0^t (\lambda \cdot t)dt = \frac{1}{2} \cdot (\lambda \cdot t) \quad (8)$$

$$PFD = \frac{F_{AVG}}{t} = \frac{1}{2} \cdot (\lambda \cdot t) \quad (9)$$

Where λ –failure rate [h^{-1}], t – time [h].

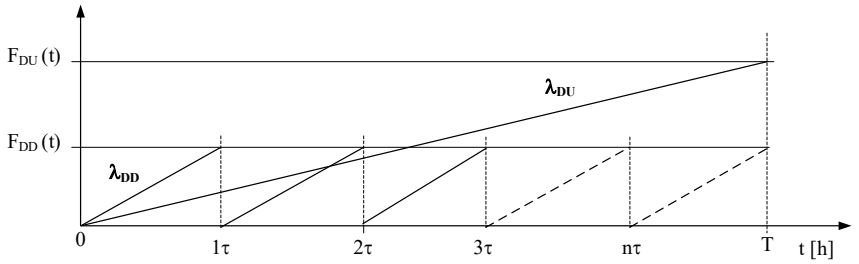

Fig. 4 Course of λ_{DD} and λ_{DU} for one item

The average probability of failure F_{AVG}, regarding to failure rates λ_{DD} and λ_{DU} for one item using formula (10) has been calculated and target value probability of failure per hour PFD_G according to equation (11) can be calculated.

$$F_{AVG} = \frac{1}{2} \cdot t \cdot \lambda_{DD} + \frac{1}{2} \cdot T \cdot \lambda_{DU} \tag{10}$$

$$PFD = \frac{1}{2} \cdot (\lambda_{DD} + \lambda_{DU}) \tag{11}$$

Where t – selftest time period) [h], T –safety function test time period [T].

These derivations to the serial and parallel systems of hardware architecture have been applied.

4.1 Serial system 1oo1

The resulting system failure rate for a serial system is the sum of the failure rates of channels (see equation (12)). Then the calculation of PFD for a series system composed of n channels is given by equation (13).

$$\lambda^{1oo1} = \lambda^A + \lambda^B \tag{12}$$

$$PFD^{1oo1} = \frac{1}{2} \cdot (\sum_1^n \lambda_{i,DD} + \sum_1^n \lambda_{i,DU}) \tag{13}$$

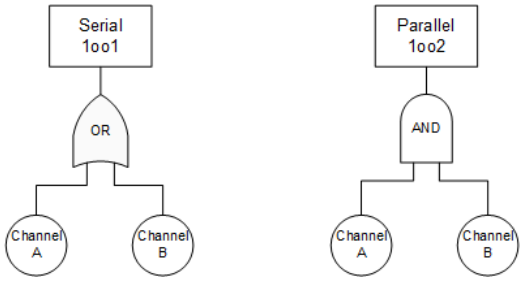

Fig. 5 Serial 1oo1 and parallel 1oo2 systems architecture according the FTA

4.2 Parallel system 1oo2

This architecture consists of two channels connected parallelly, so that only one channel is needed to perform the safety function. Probability of system F(t) is given by equations (14). The average probability of failure F_{AVG} for channels A and B is given by equation (15).

$$F(t) = F_A(t) \cdot F_B(t) \qquad F(t) = (\lambda_A \cdot t) \cdot (\lambda_B \cdot t) \tag{14}$$

$$F_{AVG}^{1oo2} = \frac{1}{t} \int_0^t (\lambda_A \cdot t) \cdot (\lambda_B \cdot t) dt = \frac{1}{3} \cdot \lambda_A \cdot \lambda_B \cdot t^2 \tag{15}$$

The average probability of failure F_{AVG}, regarding to failure rates λ_{DD} and λ_{DU} for one channel using formula (16) has been calculated and target value probability of failure per hour PFD_G according to equation (17) can be calculated, on the condition that both channels are identical.

$$F_{AVG}^{1oo2} = \frac{1}{3} \cdot [(t^2 \cdot \lambda_{DD}^2) + (T^2 \cdot \lambda_{DU}^2)] \tag{16}$$

$$PFD^{1oo2} = \frac{1}{3} \cdot [(t \cdot \lambda_{DD}^2) + (T \cdot \lambda_{DU}^2)] \tag{17}$$

Similarly, as these two hardware architectures also for other hardware architectures suitable equations have been derived.

Advantages and utilization off all hardware architectures in the Tab. 1 have been described.

Tab. 1 Utilization of hardware architectures

Hardware architecture	Application level
1oo1	Basic architecture, only one channel, without redundancy. Applicable for SIL1 and SIL2 (reliability and SFF requirements are low).
1oo2	Safety function with redundancy, reliable activation of safety function, e.g. emergency stop. Applicable for SIL3 and SIL4 (reliability and SFF requirements are high).
2oo3	Majority redundancy (majority voting systems), reliable activation of safety function, e.g. emergency stop. Used due to SW, can eliminate hidden software errors (each channel is programmed by a different group of programmers). High costs, applicable for SIL3 and SIL4.
2oo2	Specil architecture. Used when we have to be very sure that safet function is really to be activated (e.g. engine extinguishing starts if a fire is signaled by both the temperature sensor and the smoke sensor).

In the field of functional safety also exist a special group of failures – CCF (Common Caused Failures). These CCF failures can deactivate whole safety function only in occurrence of one failure. The CCF during the assessment process of functional safety also must be considered. Utilization of FTA (fault Tree Analysis) approach brings also another advantage. CCF can be simply included in the fault tree as an individual item with its own failure rate.

5 CONCLUSIONS

The paper is focused on the simplification and transparency of the described computational procedures in connection to standards EN 61508 and EN 50129. Especially in the early stages of hardware development, the simplicity of calculation is desirable, when frequent changes in hardware design and consequently changes in calculation will be expected. The utilization of fault trees (FTA) looks like a slightly cleaner system of calculation. Example of utilization of fault tree approach for serial and parallel hardware architectures in this paper has been shown.

◆◆

References

[1] EN 61508-1. *Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 1: General requirements.* Geneva, Switzerland: © IEC:2010.

[2] EN 61508-2. *Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 2: Requirements for electrical/electronic/programmable electronic safety-related systems*. Geneva, Switzerland: © IEC:2010.
[3] EN 61508-4. *Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 4: Definitions and abbreviations*. Geneva, Switzerland: © IEC:2010.
[4] EN 61508-5. *Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 5: Examples of methods for the determination of safety integrity levels*. Geneva, Switzerland: © IEC:2010.
[5] EN 50128. *Railway applications – Communication, signaling and processing systems – Software for railway control and protection systems*. Brussels: CENELEC, 2020.
[6] EN 50129. *Railway applications – Communication, signaling and processing systems – Safety related electronic systems for signaling*. Brussels: CENELEC, 2018.
[7] STAMATELATOS, M., VESELY, W., DUGAN, J., FRAGOLA, J., MINARICK, J., RAILSBACK, J. *Fault Tree Handbook with Aerospace Applications*. Washington DC: NASA Office of Safety and Mission Assurance, 2002.
[8] CHAE, C. K., KO, J. W. FTA-FMEA-based validity verification techniques for safety standards. *Korean Journal of Chemical Engineering*. 2017, **34**(3), 619–627. DOI: 10.1007/s11814-016-0321-1
[9] RAUSAND, M., HØYLAND, A. *System Reliability Theory: Models, Statistical Methods, and Applications*. 2nd ed. Hoboken, New Jersey: Wiley, 2004. ISBN 047147133X.
[10] MESICEK, J., RICHTAR, M., PETRU, J., PAGAC, M., KUTIOVA K. Complex view to racing car upright design and manufacturing. *Manufacturing technology*. 2018, **18**(3), 449–456. ISSN 1213-2489. DOI: 10.21062/ujep/120.2018/a/1213-2489/MT/18/3/449
[11] RICHTÁŘ, M., SMIRAUS, J. Functional safety utilization in road vehicles design. In: *Proceedings: deterioration, dependability, diagnostics*. Brno: Univerzita obrany, 2014, 171–178.
[12] FAMFULÍK, J., MIKOVA, J., RICHTAR, M., HALAMA, R. Random vector approach to the calculation of the number of railway vehicles to hold in reserve. *Proceedings of the Institution of Mechanical Engineers, Part F: Journal of Rail and Rapid Transit.* 2016, **230**(1), 253–257. DOI: 10.1177%2F0954409714536382
[13] GRENCIK, J., GALLIKOVA, J., VOLNA, P. Risk management in the operation and maintenance of railway freight wagons. In: *24th International Conference on Current Problems in Rail Vehicles: proceedings*. Žilina, Slovakia: VTS pri ŽU v Žiline, 2019. ISBN 978-80-89276-58-5.
[14] FAMFULIK, J., RICHTAR, M., REHAK, R. et al. Application of hardware reliability calculation procedures according to ISO 26262 standard. *Quality & Reliability Engineering Int*. 2020, **36**(6), 1–15. DOI: 10.1002/qre.2625