

Keywords: railway system; safety; reliability

Grzegorz KACZOR^{1*}, Maciej SZKODA², Magdalena MACHNO³

HAZARD AND RISK ANALYSIS OF RAILWAY VEHICLE CONTROL SYSTEMS ACCORDING TO SAFETY INTEGRITY LEVELS

Summary. This article presents an approach to the verification of the safety integrity level (SIL) of rail vehicle subassemblies in accordance with the applicable railway standards PN-EN ISO 50126-1, PN-EN ISO 50126:2, and PN-EN ISO 50129. Particular attention has been given to the calculation procedure related to the determination of the tolerable hazard rate and tolerable functional failure rate indicators in a situation where various reliability indicators have been declared for components of rail vehicles, such as $MTTF_D$ or B_{10D} . In this case, the verification of the safety integrity level using the above-mentioned railway standards may be difficult, and it becomes necessary to use additional standards for safety systems based on electronic components. An example is the PN-EN ISO 13849-1:2006-01 standard, which contains a calculation method based on the transformation of the exponential model, which is useful for hazard and risk analyses of electronic systems containing components with different reliability indices. Another supplementary standard is the PN-EN 61025:2007 standard, which concerns fault tree analysis. Based on the above-mentioned standards, an algorithm was developed to verify the safety integrity level of the frequency converter control system. The obtained results allowed us to confirm the fulfillment of the functional safety requirements of the considered system.

1. INTRODUCTION

In rail vehicles, the issues of the reliability and safety of operating systems are undoubtedly important research areas. Of particular significance is functional safety, which is closely linked to a rail vehicle's technical systems. These systems carry out so-called safety functions, the stoppage or improper performance of which affects the possibility of hazards to the railway system and its environment. The key issue in verifying the functional safety of rail vehicles is to determine how the safety functions are performed. The requirements that are placed on typical safety functions for rail vehicles are included in the PN-EN 15380-4:2013-06 standard. When specifying the safety-related functions of technical objects, many factors relating to their operation should be considered, such as their characteristics and conditions of use [18], which include:

- mode of operation (e.g., manual, automatic, zoned),
- frequency of operation,
- time of reaction (response) to input signals,
- reactions of the device to loss of power supply,

¹ Cracow University of Technology; Department of Rail Vehicles and Transport, al. Jana Pawła II 37, 31-864 Cracow, Poland; gkaczor@pk.edu.pl; orcid.org/0000-0002-4915-6116

² Cracow University of Technology; Department of Rail Vehicles and Transport, al. Jana Pawła II 37, 31-864 Cracow, Poland; maciej.szroda@pk.edu.pl; orcid.org/0000-0002-9511-2253

³ Cracow University of Technology; Department of Rail Vehicles and Transport, al. Jana Pawła II 37, 31-864 Cracow, Poland; magdalena.machno@pk.edu.pl; orcid.org/0000-0002-5486-3982

* Corresponding author. E-mail: gkaczor@pk.edu.pl

- conditions for the activation or deactivation of operation,
- the impact of the failure of the machine on other objects in its surroundings.

In addition, the reliability indicators of electrical and electronic components play an important role in the functional safety assessment of rail vehicles. These indicators are among the main parameters of rail vehicle control systems and are usually provided by their manufacturers. In the absence of these indicators, special databases can be used, such as IEC TR 62380 (RDF 2000), Bellcore/Telcordia, China 299B, PRISM, SAE Rel. Pred. Meth., or MIL-HDBK-217. These make it possible to estimate, *inter alia*, failure severity rates depending on the operating conditions, materials used, complexity, load, and many other criteria. Some of these databases are already obsolete and are not always suitable for use with modern rail vehicle subassemblies [4, 8].

Safety integrity concerns various aspects, each of which is necessary to ensure that the requirements are met. The quantitative safety objective is only one of the aspects of safety integrity. This means that, in addition to quantitative aspects, safety integrity includes factors such as quality management, safety management, and technical safety measures. In the EN 50126-2:2018-02 standard, “quality measures” are addressed as [1, 12]:

- quality management conditions,
- safety management conditions,
- technical safety measures.

All factors shown in Fig. 1 must be met in order to achieve the specified safety integrity:

- the particular quantified safety target,
- the quality management conditions, safety management conditions, and technical safety measures associated with a particular safety integrity level.

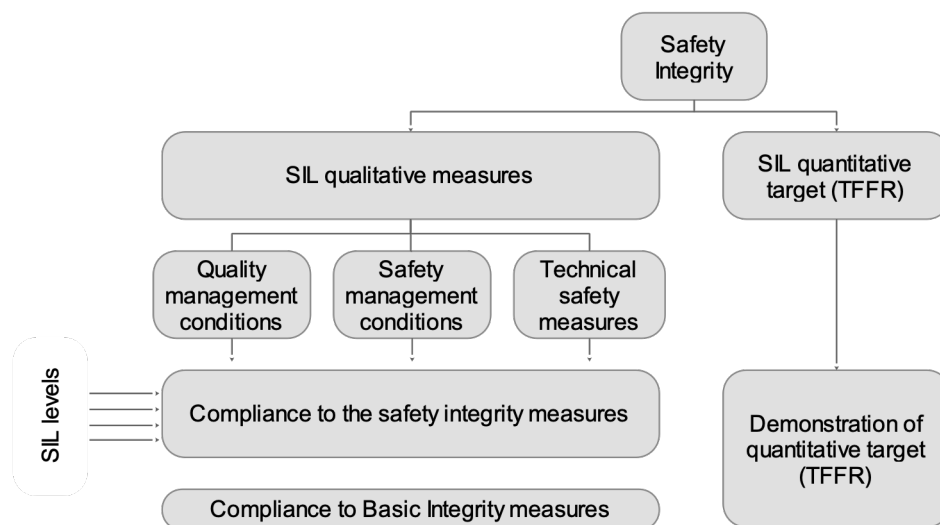


Fig. 1. Categorization of safety integrity measures [14]

The basic standard that refers to the functional safety of systems with electrical, electronic or programmable electronic components is the IEC 61508 functional safety of electrical/electronic/programmable electronic safety-related systems. This standard has been prepared to facilitate quantitative safety assessments for programmable automation systems (Fig. 2) [16]. The IEC 61508 standard introduces the concept of safety integrity levels as a quantitative measure of the functional safety of technical systems, enabling the determination of the limiting level of risk associated with the occurrence of specific undesired events. The safety integrity of a technical system is understood as the ability to achieve the required safety level for each safety function of that system. Safety integrity concerns both systematic failures and random failures. However, it is worth noting that the estimation of the safety integrity level for systematic failures is not possible using quantitative methods. The main focus of safety integrity verification is on random failures. An important supplement to the industry standards listed in Fig. 2 is PN-EN ISO 13849-1:2016-02.

Over the years, many industry standards have been developed that deal with safety requirements in various areas of the industry. The appropriate standard for the railway industry, in this case, is the series of standards PN-EN 50126, PN-EN 50128 and PN-EN ISO 50129 [1, 12-14]. These refer to the general approach to the Reliability, Availability, Maintainability, Safety process and safety assurance for railway systems. Many real-life scenarios throughout the life cycle of these systems show that the calculation examples in these standards referring to the procedural assessment of reliability and safety are insufficient. For this reason, reference is made to other related standards that do not only concern electronic components or elements largely concerned with railway standards. Moreover, the “machine” standard PN-EN ISO 13849-1:2016-02 broadens the approach to assessing the reliability and safety of components (e.g., hydraulic, pneumatic, or mechanical components). The latest version of EN IEC 50129:2019-01 also introduces the concept of “basic integrity” (SIL0), which indicates the absence of functional safety requirements – that is, the tolerable hazard rate (THR) and tolerable functional failure rate (TFFR) values are not specified.

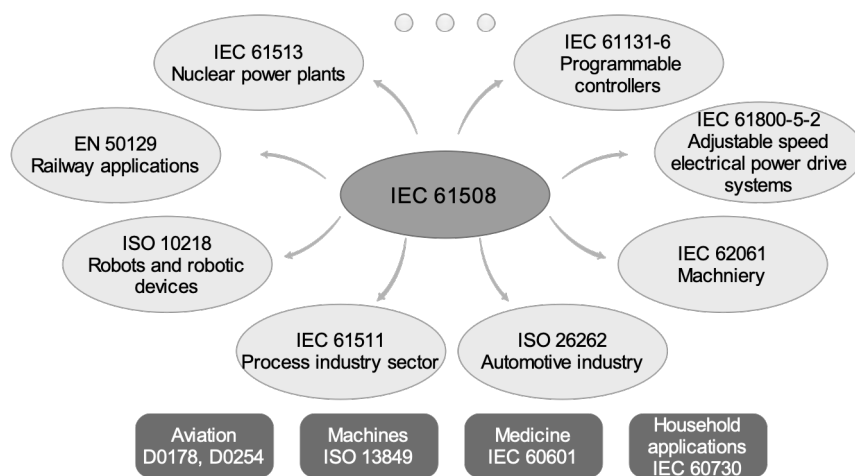


Fig. 2. Standards related to functional safety [16]

Selected aspects of verification of the SIL are presented based on the example of an analysis of the safety functions of the frequency converter control system used in an electric multiple unit. This is a modern passenger vehicle consisting of four sections based on two biaxial driving bogies and three biaxial Jacobs-type rolling bogies. Depending on the conditions, route profile, and size of passenger streams, the train can run in multiple tractions up to three vehicles. The vehicle is equipped with automatic couplers of the Scharfenberg system to enable quick coupling and decoupling. The driver’s cab is located at both ends of this type of vehicle. Frequency converters constitute the main component of the modern energy-electronic drive with pulse start on these vehicles. The devices are built into the roof of the vehicle’s outer sections. The converters have two primary purposes. The first is to convert the direct current picked up by the current collector from the catenary network into a three-phase alternating current used to power the four asynchronous traction motors in the bogies. The second purpose is to ensure the implementation of the basic vehicle functions, including start-up control and electrodynamic braking, with the possibility of energy recuperation into the traction network. A general working diagram of a frequency converter is shown in Fig. 3.

In available scientific papers that refer to railway systems, frequently applied approaches are based on the fault tree analysis (FTA) method. An example can be found in [2]. The authors verified the safety integrity level using a railway station in Turkey as an example. They used k out of n redundancy structures, which were considered part of the analysis. The FTA was combined with a Markov graph method. Both methods were also adopted in [10] to verify the safety of railway power supply systems. Attention was drawn to the importance of monitoring the safety of railway power supply systems as a group of critical subsystems.

The authors of [6] also used the FTA method to verify the functional safety of a selected railway system as an aid to the unified modeling language. This made it possible to describe the system's architecture and identify its weak links. The versatility of the fault tree analysis in railway applications was also demonstrated by the application of this technique in the case of uncertainty in the model parameters. A fuzzy environment is a case that can be encountered during SIL verification in the railway sector. A calculation example for a train-breaking system for this issue is shown in [5].

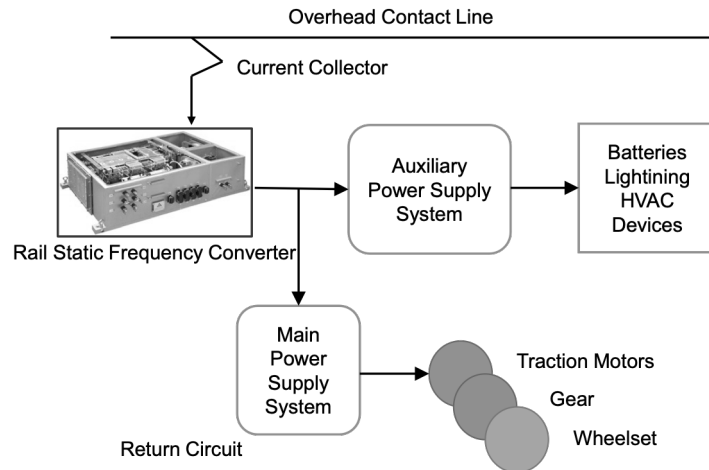


Fig. 3. Diagram of the location of the frequency converter

In turn, the approach of Szkoda and Kaczor based on the FTA method and Monte Carlo simulation may be useful in the assessment of the reliability and availability of rail vehicles and their subassemblies [20]. Papers on functional safety in railway systems consider common and divergent practices in the application of SIL allocation, as demonstrated in [9]. The authors relied on the MODUrban and MODTRAIN projects, which have been implemented. For the above reasons, it is necessary to develop a model of a system in terms of reliability theory in order to verify the functional safety of that system. The aim of such an approach is to identify the failures of components and to analyze the impacts of these failures on the implemented safety functions.

Another interesting approach to functional safety verification is the use of the Petri network. One author [6] proposed a method of functional safety verification of train-centric communication-based train control using the above-mentioned technique. The proper operation of the train communication network guarantees the safe and reliable movement of trains, especially as this network is increasingly being extended through distributed microcomputers and other electronic devices, as mentioned by the authors.

The verification of the SIL of the railway control system also involves a risk assessment, which can be carried out using, *inter alia*, a risk graph. This makes the classification of safety requirements clearer and more effective. It is also particularly important for high-speed trains because of the possible consequences of any risks. The basic principles for the verification of the SIL in high-speed rail transport have been discussed in [21].

The analyzed scientific papers address relevant functional safety issues for railway systems, often based on real-life objects. The included scientific approaches go beyond the scope of dedicated standards in many aspects. The scenarios considered take into account complex systems, as well as reliability data with a high degree of uncertainty. However, it is difficult to find any papers that consider random variables of different types (time, cycle) in the SIL verification process. For this reason, the topic addressed in the present paper seems to be valuable and brings new content to the approach of the functional safety verification of railway systems.

On the other hand, it is worth referring to the historical background of the technological evolution of power electronics traction systems in high-speed rail contexts [1]. In [24] it is introduced examples of research and development related to these fields and trends in the main circuit and traction system

development for railway vehicles. Electric traction systems progressed mainly in the field of main circuits, evolving from rheostatic control to chopper control. Then to field added excitation control and combinations of adjustable voltage adjustable frequency inverters and induction motors. Electrical semiconductor devices used in the adjustable voltage frequency inverters can also change according to thyristors to GTO, to GTR, to IGBT, and, more recently, to SiC. In addition, interesting technical solutions in the construction of the traction inverters of modern rail vehicle drive systems are presented in [2]. The work draws attention to the increasing reliability requirements of rail vehicle control systems.

The present paper concerns the verification of the level of safety integrity of the frequency converter control system in a case where the reliability data of the elements of this system are expressed in different work units. Due to the lack of the indicated normative approach in relation to railway systems, a method is developed using related standards, referring to the issues of reliability and functional safety. As a result of the developed approach, a model of the reliability of the frequency converter control system is designed. Next, on the basis of this model, the TFFR is determined for the individual functions of the converter control system.

2. MATERIALS AND METHODS

2.1. Indicators for verifying the functional safety of rail systems

The verification of the functional safety of technical systems is possible on the basis of the knowledge of the structure and reliability indices of elements of these systems, which is related to the frequency or probability of the occurrence of hazardous failures. According to the PN-EN ISO 13849-1 standard, the probability of occurrence of a hazardous failure of a technical system also depends on [15]:

- mechanisms for fault detection,
- diagnostic coverage,
- common cause failure indicator,
- design and production factors,
- operating conditions (load, environmental factors),
- corrective and preventive maintenance.

The basic indicators used to verify the functional safety of technical facilities include:

- $MTTF_D$ – mean time to hazardous failure,
- λ_D – hazardous failure severity index,
- B_{XD} – reliability index that can be interpreted in two ways:
 - amount of work done (time, number of cycles) after which x% of the system population suffers a hazardous failure,
 - amount of work done (time, number of cycles) after which the system's capacity decreases by x% (e.g., due to wear and tear).

The application of the B_{XD} index is based on the cumulative distribution function, an overview of which is shown in Fig. 4.

When classifying safety integrity levels, one of the most important indicators is the failure intensity rate $\lambda(t)$. In relation to functional safety, instead of the concept of failure intensity, the concept of hazard intensity is used. This ratio is denoted by THR or TFFR. In the PN-EN 50126:2019-01 standard, there is a distinction between these indicators:

- THR – related to the fault type that the hazard induces,
- TFFR – related to the specific function that the technical system performs.

If the safety integrity level requirement is set at the level of a specific safety function of a technical system and one hazard is assigned to each of these functions, then only the THR is used. Otherwise, when a function has multiple hazards assigned, the THR must be allocated to each of these functions, and these functions must be assigned an individual TFFR. The classification of security integrity levels includes four essential SILs shown in Table 1.

In accordance with Table E.4 contained in the PN-EN 50129:2019-01 standard, the fault tree analysis method is recommended for the calculation and verification of the TFFR. Such a recommendation was used in [14] to develop the calculation algorithm. The basic symbols used in the fault tree analysis method, along with their descriptions, are included in Table 2.

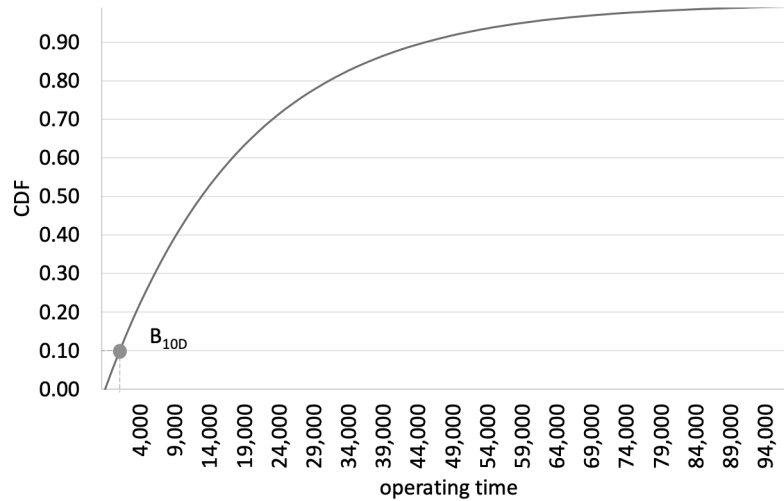


Fig. 4. Reliability function of the control system of a frequency converter with two-sided confidence level intervals

Table 1
Classification of security integrity levels according to PN-EN 50126:2019-01 [1]

TFFR [1/hr]	SIL
$10^{-9} \leq \text{TFFR} < 10^{-8}$	4
$10^{-8} \leq \text{TFFR} < 10^{-7}$	3
$10^{-7} \leq \text{TFFR} < 10^{-6}$	2
$10^{-6} \leq \text{TFFR} < 10^{-5}$	1

3. HAZARD AND RISK ANALYSIS OF THE FREQUENCY CONVERTER CONTROL SYSTEM

This chapter deals with an example of the verification of the level of the safety integrity of the frequency converter control system in a situation in which the control system elements are characterized by reliability indicators expressed in different units. An algorithm is developed for this purpose (see Fig. 5). The algorithm uses recommendations of the PN-EN 50129 standard applicable to railway systems and additional related standards.

The presented algorithm can be used for any technical system comprising electrical, electronic, and programmable electronic components. The applied reliability standards allow for the decomposition of complex subsystems and their individual assignment to safety-related functions. Such an approach reveals the possibility of modeling complex operational scenarios, taking into account diagrams containing k out of n redundancy or time-dependent reliability configurations. As all of the standards contained in the algorithm are interrelated, the application of one of them does not cause any inconsistencies with the other. This is an important consideration for the independent safety assessment body, which is responsible for assessing the compliance of the methods used with the relevant standards.

3.1. Frequency converter safety functions to be analyzed

Frequency converters are designed to supply 3,000 VDC traction voltage. The basic technical data of the selected frequency converter are shown in Table 3.

Table 2

Frequently used symbols for a fault tree technique according to PN-EN 61025:2019-01 [17]


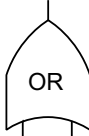

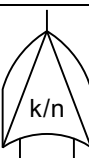
Symbol	Name	Description	Reliability correlation
	BASIC EVENT	The lowest-level component with given reliability information	Component failure mode or a failure mode cause
	OR GATE	The system fails if all of the associated components fail	Series reliability configuration
	AND GATE	The system fails only if all of the associated components fail	Parallel redundancy
	VOTING GATE	The system fails if k out of n components fail	k out of n redundancy

Table 4 characterizes the safety functions that are subject to SIL verification and are used in this paper. Each safety function may have different requirements for the safety integrity level.

Verification of the safety integrity levels of the frequency converter control system requires the availability of the input data of its components. The reliability source data specified by the manufacturers were used in order to calculate the TFFR and the SILs for the frequency converter functions under consideration. These data are shown in Table 5. It is desirable for the reliability-related parameters of each component to be expressed in units of the same type (e.g., units of time or number of working cycles). A problem arises when the types of these units differ from one element to another, as is the case with the traction inverter control system. The currently used railway standards for safety assessment do not provide guidance for dealing with such situations.

In the case of integrated circuits, the FIT (Failures in Time) indicator (i.e., the number of hazardous failures per $1 \cdot 10^9$ working hours) was given. In the analysis, the value of $FIT = 126.74$ was assumed, which presents the most pessimistic variant highly accelerated stress test (HAST). This ensures that the TFFR values will be deducted with some reserve. For relays, the reliability indicator B_{10D} , expressed in operating cycles, is given. The values of B_{10D} are provided depending on the rated current flowing through the relay contacts. For the frequency converter under consideration, the rated current value does not exceed $I_e = 16$ A; hence, the value of B_{10D} for this current value is used in the calculations.

The FTA method recommended in the PN-EN 50126 standard was used in order to determine the TFFR for the frequency converter control system. The fault tree model applied to the frequency converter control system is shown in Fig. 6. The structure takes into account only the elements that are responsible for the realization of safety functions (listed in Table 4).

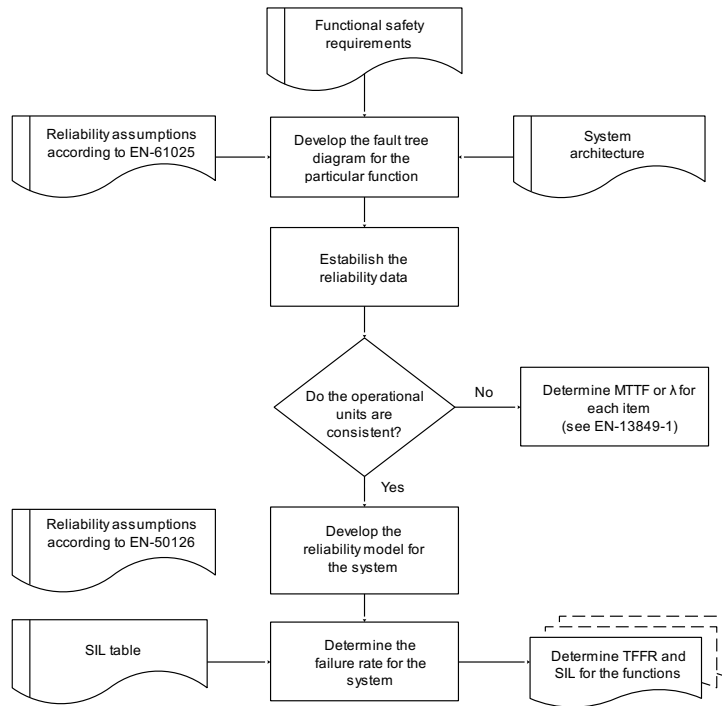


Fig. 5. Algorithm adopted in the utilized test method

Table 3
Basic frequency converter technical data [22]

Features	Value
Rated input voltage	3,000 VDC ±25%
Auxiliary voltage	24 VDC ±20%
Rated output current	1,350 Arms
Hourly-rated output current	200 Arms
180-sec maximum output current	310 Arms
Rated power	525 kW
Frequency	0–160 Hz
Cooling	forced inner
Weight	1,275 kg
Working temperature range	between -30°C and +40°C

Table 4
Safety-related functions of the frequency converter control system to be analyzed

Function designation according to PN-EN 15380-4	Function description	Hazard to the vehicle control system	Effect of the hazard	Required SIL
GB 1c-1	Maintaining the pre-set vehicle speed	No overspeed detected	Exceeding the speed limit for a vehicle on a particular stretch	SIL1
GB 1a-1	Securing a stopped vehicle against unexpected start-up	Spontaneous vehicle start-up due to the unintentional	Sudden vehicle movement during passenger exchange. The driver, who is present in	SIL1

	(when the operator is in the driver's cab)	powering of traction motors	the cab, can minimize the risk	
GB 1a-2	Securing a stopped vehicle against unexpected start-up (when the operator moves between drivers' cabs)	Spontaneous vehicle start-up due to the unintentional powering of traction motors	Sudden vehicle movement during passenger exchange. The driver is not present in any cab and cannot minimize the risk	SIL1
GB 1b-2	Securing the vehicle against changing direction while in motion	Change of current direction in traction motor windings. Start-up opposite to intended	Acceptance of a direction change request due to an error (e.g., in software)	SIL1

Table 5

Reliability data of frequency converter elements

Element	FIT for hazardous failures, λ_D $1 \cdot 10^{-9}$ [hour]	Indicator	Remarks
		B_{10D} $1 \cdot 10^6$ [cycles]	
R1 relay	-	1.68	under I_e (where I_e is the nominal current)
	-	2.58	with current $I_e = 2$ A
	-	4.09	with current $I_e = 4$ A
	-	8.60	with current $I_e = 8$ A
	-	15.05	with current $I_e = 16$ A
USC01÷ USC06 integrated circuits	16.34	-	HBTR FIT CL = 60%, activation temperature 0.7 eV. Test temperature 125° C. Operating temperature 40° C
	38.86	-	HBTR FIT CL = 60%, activation temperature 0.7 eV. Test temperature 130° C. Operating temperature 40° C
	52.13	-	HTOL FIT CL = 95 %
	126.74	-	HAST FIT CL = 95 %

In a failure tree structure consisting of k out of n redundancy gates and events that follow the one-parameter exponential failure model, the reliability function for the frequency converter control system can be determined from partial equations using the following relationship [18]:

$$R_{k/n}(t) = \sum_{i=k}^n \frac{n!}{(n-k)!i!} (e^{-\lambda_j t})^i \cdot (1 - e^{-\lambda_j t})^{n-i}, \quad (1)$$

where:

n – number of components [days],

k – number of required components operating successfully [h],

λ_j – failure intensity of element j ,

t – operating time.

The mean time to failure for individual k gates of the n fault tree can be determined as follows [18]:

$$MTTF_{k/n} = \int_0^{\infty} R_{k/n}(t) dt = \frac{1}{\lambda_j} \left(\frac{1}{n} + \dots + \frac{1}{k} \right). \quad (2)$$

The elements considered in the model of the frequency converter control system belong to the group of non-renewable electronic elements. According to the PN-EN 50126 standard, for this type of element,

an exponential distribution of the time of correct work to failure applies, the reliability function of which is expressed by the following formula [18]:

$$R_i(t) = e^{-\lambda_j \cdot t} \tag{3}$$

Using the approach proposed in PN-EN ISO 13849-1:2006-01 makes it possible to verify the level of safety integrity for components with different types of units. This approach is based on the transformation of an exponential distribution; thus, it applies mainly to electronic, programmable electronic, and automation elements. Based on the indicator B_{10D} expressed in work cycles, it is possible to change to the indicator $MTTF_D$ expressed in time units. Using a simplified model for electronic components with constant failure frequency, we obtain the following expression [15]:

$$MTTF_D = \frac{B_{10D}}{0.1 \cdot n_{op}} \tag{4}$$

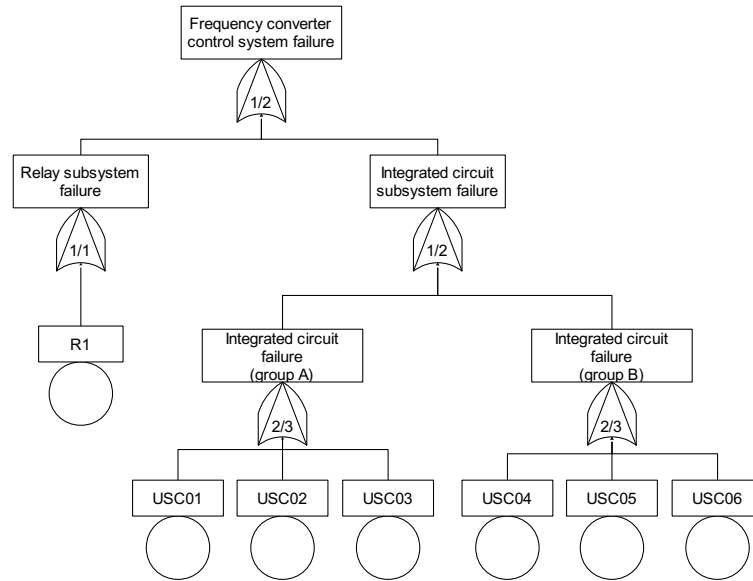


Fig. 6. Fault tree model for the adopted frequency converter control system

where:

n_{op} – average number of operating days per year,

$$n_{op} = \frac{d_{op} \cdot h_{op} \cdot 3,600}{t_{cycle}} \tag{5}$$

where:

d_{op} – average number of operating days per year [days],

h_{op} – average number of operating hours per day [h],

t_{cycle} – average time before the start of two consecutive operating cycles [s/cycle].

The average time to hazardous failure in 10% of the population is equal to:

$$T_{10D} = \frac{B_{10D}}{n_{op}} \tag{6}$$

Ultimately, the intensity of hazardous failures λ_D is given by the following formula:

$$\lambda_D = \frac{0.1}{T_{10D}} \tag{7}$$

Based on Equation (6) for the fault tree shown in Fig. 6, a general form of the reliability function of the frequency converter control system can be written as:

$$R_s(t) = e^{-\lambda_{D,R1}t} \cdot \left(1 - \left(1 - e^{-\lambda_{D,USC}t} \right)^6 \right) = e^{-\lambda_{D,SPSt}} \cdot \left(\begin{matrix} 6e^{-\lambda_{D,USC}t} - 15e^{-2 \cdot \lambda_{D,USC}t} \\ + 20e^{-3 \cdot \lambda_{D,USC}t} - 15e^{-4 \cdot \lambda_{D,USC}t} \\ + 6e^{-5 \cdot \lambda_{D,USC}t} - e^{-6 \cdot \lambda_{D,USC}t} \end{matrix} \right) \tag{8}$$

where:

λ_{D_R1} – intensity of hazardous failures of the SPS214-110VDC relay,

λ_{D_USC} – intensity of hazardous failures of the XP63152V integrated circuit.

4. RESULTS AND DISCUSSION

The verification of the safety integrity level of the frequency converter control system was based on the reliability data of the R1 relay and the components of the USC01÷USC06 integrated circuit.

The following assumptions for the relay R1 were made:

$$\begin{aligned} d_{op} &= 300 \text{ days,} \\ h_{op} &= 20 \text{ h,} \\ t_{cycle} &= 3 \frac{s}{\text{cycle}}, \end{aligned}$$

Based on these assumptions, we obtained, respectively:

$$\begin{aligned} n_{op} &= 7.2 \cdot 10^6 \left[\frac{\text{cycles}}{\text{year}} \right] \\ T_{10D} &= 0.972 \text{ [years]} \\ \lambda_{D_R1} &= 5.461 \cdot 10^{-6} \left[\frac{1}{\text{h}} \right] \end{aligned}$$

Based on transformations of Relationship (2) and the properties of exponential distribution ($\lambda = 1/MTTF$), we obtain the hazardous failure intensity indicator of the frequency converter control system:

$$TFFR = \lambda_D = \lambda_{D_R1} + \frac{2 \cdot \lambda_{D_USC}}{\left(1 + \frac{1}{2} + \frac{1}{3}\right)} = 5.599 \cdot 10^{-6} \left[\frac{1}{\text{h}} \right] \quad (9)$$

Based on the determined TFFR values, the corresponding SILs for the required functions are summarized in Table 6.

Table 6
SILs for the required functions of the frequency converter control system

Function designation	Vehicle function	TFFR [1/hour]	SIL
GB 1c-1	GB	$5.599 \cdot 10^{-6}$	SIL 1
GC 1a-1	GC	$5.599 \cdot 10^{-6}$	SIL 1
GC 1a-2	GC	$5.599 \cdot 10^{-6}$	SIL 1
GC 1b-2	GB	$5.599 \cdot 10^{-6}$	SIL 1

The difference in fault intensity values between the R1 relay and the components of the USC01÷USC06 integrated circuit is considerable, as shown in Fig. 7.

Despite the relatively low failure intensity of components of the USC01÷USC06 integrated circuit, the failure intensity of the whole IC subsystem is drastically reduced from $126.74 \cdot 10^{-9}$ (1/h) to $1.383 \cdot 10^{-7}$ (1/h). This is due to the fault tree structure with type 2 out of 3 gates used for the IC subsystem. This means that although there are three components in a particular IC group, the simultaneous operation of at least two is required to perform the safety functions. As a result, the difference in failure intensity between the R1 relay and the IC subsystem is reduced, and the TFFR value for the frequency converter control system is strongly affected.

The advantage of the SIL verification algorithm presented in this article is that it extends the procedure based on the PN-EN 50129:2018-02 and PN-EN 50126:2018 standards and can also be used for other control systems in rail vehicles, as well as for railway traffic control systems. Based on the analyzed works of other researchers in the relevant research area, it can be concluded that the approach proposed in this work has not been used so far and that it will add value to the research area.

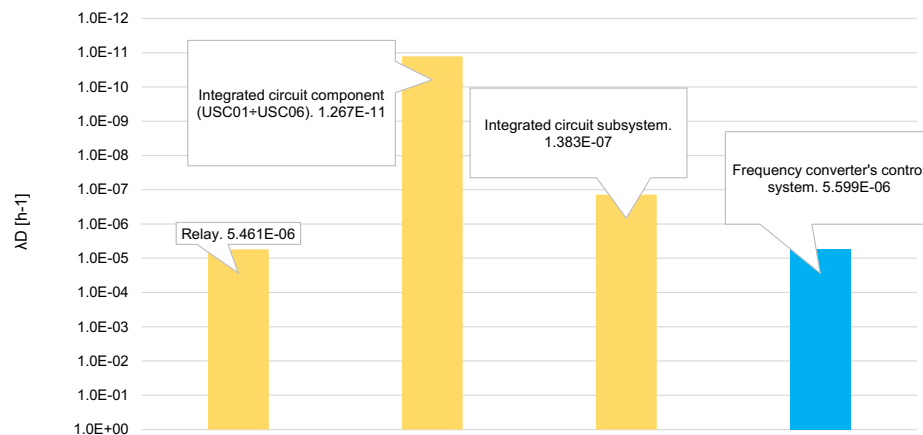


Fig. 7. Comparison of the indicator λ_D between elements (yellow) and the frequency converter control system (blue)

A limitation of the utilized method is its inability to take into account the impacts of common cause failures and renew parameters. Common cause failures are an issue often found in the literature as a separate research problem. In turn, the impact of the renewal parameters on the level of safety integrity occurs primarily in safety supervision systems (e.g., fire protection systems). These components include a self-diagnostic and reset function in the event of errors. For this reason, the authors recommend taking into account the impact of damage in common cause and renewal behavior in the developed algorithm as a direction for future research.

5. CONCLUSIONS

The present study makes it possible to verify the safety integrity level of the considered traction inverter control system. The following conclusions are drawn:

1. The analyzed traction inverter control system meets the requirements of SIL1.
2. For higher safety integrity level requirements to be met, additional redundancy shall be considered for the R1 relay, which is the weakest item of the entire system.
3. The presented solution allowed us to take into account components with different reliability indicators expressed in different units.
4. The PN-EN ISO 13849:2016-02 machine standard can be used as a supplementary document to verify the safety integrity level of railway systems without creating inconsistencies with the applicable railway standards.

References

1. Abad, G. *Power Electronics and Electric Drives for Traction Applications*. John Wiley & Sons. 2017. Ltd. DOI: 10.1002/9781118954454.
2. Anik, V.G. & Ustolgu, I. & Kaymakci, O.T. The functional safety calculation of a real interlocking system in Turkey. In: *2011 IEEE International Conference on Mechatronics*. Istanbul, Turkey. P.71-76.
3. Biliński, J. & Malczewska, M. & Rojek, A. & Kruczek, W. Falowniki trakcyjne kolejowych pojazdów szynowych – rozwiązania techniczne i kierunku rozwoju konstrukcji. [In Polish: Traction inverters of railway rail vehicles - technical solutions and direction of construction development]. *TTS Technika Transportu Szynowego*. 2020. R. 27. No. 5-6. P. 43-57.

4. De Francesco, E. & De Francesco, R. & Petritoli, E. Obsolescence of the MIL-HDBK-217: A critical review. In: *2017 IEEE International Workshop on Metrology for AeroSpace (MetroAeroSpace)*. 2017. Padua, Italy. P. 282-286.
5. Jafari, H. & Sandidzadeh, M.A. & Ghavibazoo, A. Determining safety integrity level by considering uncertainty aspects in fuzzy environment (case study on train braking system). *International Journal of Railway Research*. 2020. Vol. 7(2). P. 51-59.
6. Lin, J. & Xu, Q. Functional safety verification of train control procedure in train-centric CBTC by Colored Petri Net. *Archives of Transport*. 2020. Vol. 54(2). P. 43-58.
7. Marzec, M. & Uhl, T. & Barszcz, T. Application of UML modeling for analysis of safety integrity level in railway traffic control systems. *Diagnostyka – Diagnostics and Structural Health Monitoring*. 2011. Vol. 4(60). P. 21-26.
8. MIL-HDBK-338B. *Military handbook: Electronic reliability design handbook*. 1998.
9. Ouedraogo, K.A. & Beugin, J. & El Kourssi, E.M. & Clarhaut, J. & Renaux, & Lisiecki, D. Safety integrity level allocation shared or divergent practices in the railway domain. In: *Congrès de l'International Railway Safety Council (IRSC 2016)*. 2017. Hong Kong. P. 1-10.
10. Oz, A.M. & Kaymakci, O.T. & Koyun, A. A Safety related perspective for the power supply systems in railway industry. *Eksploatacja i Niezawodność – Maintenance and Reliability*. 2017. Vol. 19(1). P. 114-120.
11. PN-EN 50126-1:2018-02. *Zastosowania kolejowe - Specyfikowanie i wykazywanie niezawodności, dostępności, podatności utrzymaniowej i bezpieczeństwa (RAMS) - Część 1: Proces ogólny RAMS*. Warsaw: Polish Committee of Standardization. [In Polish: *Railway applications - Specifying and demonstrating reliability, availability, maintainability and safety (RAMS) - Part 1: General RAMS process*].
12. PN-EN 50126-2:2018-02. *Zastosowania kolejowe - Specyfikowanie i wykazywanie niezawodności, dostępności, podatności utrzymaniowej i bezpieczeństwa (RAMS) - Część 2: Sposoby podejścia do bezpieczeństwa*. Warsaw: Polish Committee of Standardization. [In Polish: *Railway applications - Specifying and demonstrating reliability, availability, maintainability and safety (RAMS) - Part 2: Safety approaches*].
13. PN-EN 50128:2011. *Zastosowania kolejowe - Systemy łączności, przetwarzania danych i sterowania ruchem - Oprogramowanie kolejowych systemów sterowania i zabezpieczenia*. Warsaw: Polish Committee of Standardization. [In Polish: *Railway applications - Communication, data processing and traffic control systems - Software for railway control and security systems*].
14. PN-EN 50129:2019-01. *Zastosowania kolejowe - Systemy łączności, przetwarzania danych i sterowania ruchem - Elektroniczne systemy sterowania ruchem związane z bezpieczeństwem*. Warsaw: Polish Committee of Standardization. [In Polish: *Railway applications - Communication, data processing and traffic control systems - Safety related electronic traffic control systems*].
15. PN-EN ISO 13849-1:2016-02. *Bezpieczeństwo maszyn - Elementy systemów sterowania związane z bezpieczeństwem - Część 1: Ogólne zasady projektowania*. Warsaw: Polish Committee of Standardization. [In Polish: *Safety of machinery - Safety related parts of control systems - Part 1: General principles for design*].
16. PN-EN 61508:2010 (series). *Bezpieczeństwo funkcjonalne elektrycznych / elektronicznych / programowalnych elektronicznych systemów związanych z bezpieczeństwem*. Warsaw: Polish Committee of Standardization. [In Polish: *Functional safety of electrical/electronic/ programmable electronic safety-related systems (IEC 61508 series)*].
17. PN-EN 61025:2007. *Fault Tree Analysis. Analiza drzewa niezdatności (FTA)*. Warsaw: Polish Committee of Standardization.
18. PN-EN 15380-4:2013-06. *Kolejnictwo - System klasyfikacji pojazdów szynowych - Część 4: Grupy funkcyjne*. Warsaw: Polish Committee of Standardization. [In Polish: *Railway applications - Rail vehicle classification system - Part 4: Function groups*].
19. Smith, J.D. & Kenneth, G. & Simpson, K.G.L. *Safety Critical Systems Handbook. Straightforward Guide to Functional Safety. IEC 61508 (2010 Edition) and Related Standards*. Elsevier: Oxford. 2011.

20. Szkoda, M. & Kaczor, G. reliability and availability assessment of diesel locomotive using fault tree analysis. *Archives of Transport*. 2016. Vol. 40. P. 65-75.
21. Szmel, D. & Zablocki, W. & Ilczuk, P. & Kochan, A. Method for selecting the safety integrity level for the control-command and signaling functions. *Sustainability*. 2019. Vol. 11(24). No 7062.
22. *Technical and Operational Documentation of the 31WEb Electric Multiple Unit*. NS/31WEb/4244/20, NEWAG S.A., 20.11.2020.
23. Wenjin, Z. & Nan, L. & Xinwei, L. Estimating technology of safety integrity level of safety-related systems in high-speed train. In: *2012 2nd International Conference on Mechanical, Industrial, and Manufacturing Engineering*. 2012. Vol. 1. P. 172-277.
24. Yamamoto, T. Trends in recent research on main circuits and traction systems for railway vehicles. *Quarterly Report of Railway Technical Research Institute (RTRI)*. 2018. Vol. 59. No. 1. P. 1-5.

Received 16.08.2021; accepted in revised form 07.03.2023