Mechanics Transport Communications
Academic journal

issn 1312-3823
issue 1, 2009
article № 0342
http://www.mtc-aj.com

FUNCTIONAL SAFETY ASSESSMENT OF LED BASED SIGNAL LAMP

Jan Famfulík, Radek Krzyžanek
jan.famfulik@vsb.cz, radek.krzyzanek@vsb.cz

Institute of Transport, Faculty of Mechanical Engineering,
VŠB – Technical University of Ostrava
17. listopadu 15, 708 33 Ostrava-Poruba,
CZECH REPUBLIC

Key words: *LED based signal lamp, functional safety, safety integrity level, random hardware failure*

Summary: *Rail vehicle signal lamps used for signalling of train head or end in present are often designed as high brightness LED based lamps. Train operation safety is also influenced by proper function of its signal lamps therefore it is desirable to determine demands for safety of these systems. LED based signal lamps is possible to understand as a safety-related electronic system described in the standard IEC 61508 dealing with functional safety of these systems. Strict demands for system safety given by this standard are in compliance with hardware architecture of LED based signal lamp and its high-reliability components, contrary to common bulb signal lamps which are not suitable for functional safety assessment due to their design and low reliability level. This article deals with functional safety assessment of LED based control lamp hardware.*

Introduction

According to the Decree of Ministry of Transport of Czech Republic No. 173/1995 Coll. laying down the transport order of railways is not allowed to use a rail vehicle in operation which has signal system in failure state. The vehicle may only reach the place where is possible to repair the failure under the condition the situation cannot endanger the train operation safety. Signal lamps are part of railway vehicle signal system and are intended to indicate a head and an end of a train. Due this reason is useful to determine specific demands for signal lamp safety.

Signal lamps produced in present time are based on great number of high brightness LEDs, self diagnostic system and high-reliability electronic components. These systems meet the mentioned requirements in higher level than common bulb control lamps. LED based control lamps is possible to understand as safety-related

systems described in the standard IEC 61508 Functional safety of electrical/electronic/programmable electronic safety-related systems.

This standard sets out a generic approach for all safety lifecycle activities for mentioned systems that are used to perform safety functions. The standard uses the concept of safety integrity levels that relate to safety requirements for the hardware and software of safety-related systems. Standard [1] defines four safety integrity levels (from lowest SIL 1 to highest SIL 4) to accommodate a wide range of risk reduction or safety integrity that the safety-related systems will have to achieve.

Functional safety assessment in order to determine specific safety integrity level (SIL) for random hardware failures of LED based signal lamp in this paper is described for product of company MSV Elektronika s. r. o. (Czech Republic), the signal lamp BKS02 (see the Figure No 1 and 2).

Figure No. 1: LED based signal lamp BKS02

Figure No. 2: Rail vehicle with LED based signal lamps

Conceptual arrangement and functions of control lamp

Control lamp BKS02 is constructed of 45 high brightness LEDs, power source, input circuits, output circuits and control and diagnostic unit. Block diagram of this control lamp is shown in Figure No. 3.

In term of reliability the signal lamp can be separated into four basic units as is shown in reliability block diagram in Figure No. 4. It is obvious the system represents one channel hardware arrangement without redundancy.

Input and signal unit ensures signal lamp operating and its output circuits are intended for information about failure-free or failure state of system. Control unit is used for communication with LED control circuits and evaluation of diagnostic information. Lighting and diagnostic unit is composed of high brightness LEDs and circuits ensuring their control and function check. Power source unit contains DC/DC converter and is used for power supply of all other control lamp circuits.

Signal lamp BKS02 viewed as safety-related system according to the standard [1] is understood as equipment under control (EUC) operating in high demand or continuous mode of operation. System shall be regarded as type B because it does not

satisfy the condition there is sufficient dependable failure data from field experience for some system components.

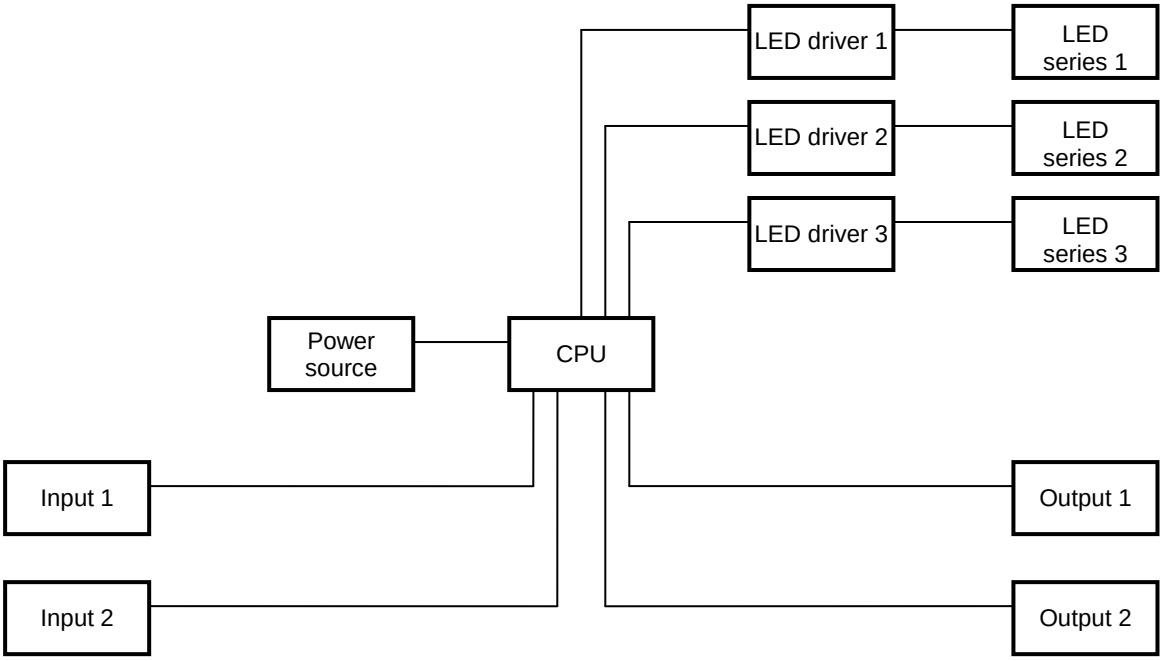


Figure No. 1: Block diagram of signal lamp BKS02

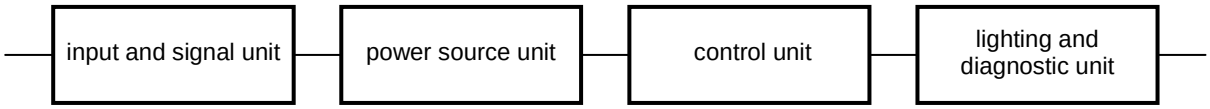


Figure No. 2: Reliability block diagram of signal lamp BKS02

Hazard and risk analysis

During railway vehicle operation the control lamp can cause a hazard due to degradation of luminous intensity and/or total functionality loss of signal lamp. These situations can cause identification deterioration of vehicle (train) head or end.

Hazardous event for signal lamp is the state when the mentioned hazard occurs and is not detected by signal lamp diagnostic system. The definition of signal lamp safety function results from hazard analysis. This function is determined as hazard identification and signalling of this situation. If signal lamp diagnostic system detects and signalizes the hazard then engine driver or train crew are obliged to implement measures according to Decree of Ministry of Transport No. 173/1995 Coll. thereby reduce the impending risk.

Hazardous event caused by degradation of luminous intensity due to LED ageing arises gradually in relation to accumulated operation time of LEDs. Thereby high brightness LEDs is necessary to rate as components with exactly defined limited life.

Hazardous event caused by random failures of hardware components which effects partial or total functionality loss of signal lamp together with this state is not

detected and signalized by diagnostic circuit. Necessary risk reduction of this event is assessed with use of quantitative methods i. e. calculation the probability of hardware random failure.

Functional safety measures

For assignment of certain safety integrity level (SIL) of signal lamp hardware with a view to functional safety assessment is necessary to determine these measures: diagnostic coverage and target failure measure.

Diagnostic coverage (DC) is defined as the fractional decrease in the dangerous undetected hardware failures resulting from the operation of the automatic diagnostic tests. In the standard [3] this definition is also expressed by equation (1):

$$DC = \frac{\sum \lambda_{DD}}{\sum \lambda_{D}} \qquad [-] \tag{1}$$

where: DC is diagnostic coverage,
λ_{DD} is the failure rate of dangerous detected failures [h^{-1}],
λ_{D} is the failure rate of dangerous failures [h^{-1}].

Target failure measure (PFH) is defined as the intended probability of dangerous mode failures to be achieved with respect to the safety-integrity requirements. For a high-demand or continuous mode of operation PFH is specified as the probability of a dangerous failure per hour. With supposition of exponential distribution of time to failure can be the probability of dangerous undetected failure (PFD) obtained:

$$PFD_{SYS} = 1 - e^{-\lambda_{DU} \cdot t_{CE}} \qquad [-] \tag{2}$$

where: PFD_{SYS} is probability of dangerous undetected failure [-],
λ_{DU} is failure rate of dangerous undetected failure [h^{-1}],
t_{CE} is equivalent down time, that the required safety function can be in the failure state [h].

Calculation of functional safety measures for signal lamp BKS02

The calculation of functional safety measures for signal lamp BKS02 results from realized analysis of risk and hazard. There will be reasoned next failure types:

- safe failure – due to one channel hardware architecture of signal lamp (without redundancy) after failure occurrence is not possible to achieve the state that the signal lamp is lighting properly; this failure will not be analyzed;
- dangerous detected failure – the state if the failure of some signal lamp units occurs and it is detected;
- dangerous undetected failure – the state if the failure of some signal lamp units occurs and it is not detected.

Fault tree analysis (FTA) [5] is made for described types of signal lamp failures, see the Figure No. 5 and 6.

From the analysis results that dangerous failure of signal lamp (detected or undetected) occurs at the moment if any signal lamp unit fails.

It is necessary to determine failure rates of each signal lamp unit for mentioned failure categories for calculation of diagnostic coverage and target failure measure. Next equation is valid for failure rates of dangerous failures:

$$\lambda_D = \lambda_{DD} + \lambda_{DU} \qquad [h^{-1}] \qquad (3)$$

where: λ_D is the failure rate of dangerous failures [h^{-1}],
λ_{DD} is the failure rate of dangerous detected failures [h^{-1}],
λ_{DU} is the failure rate of dangerous undetected failures [h^{-1}].

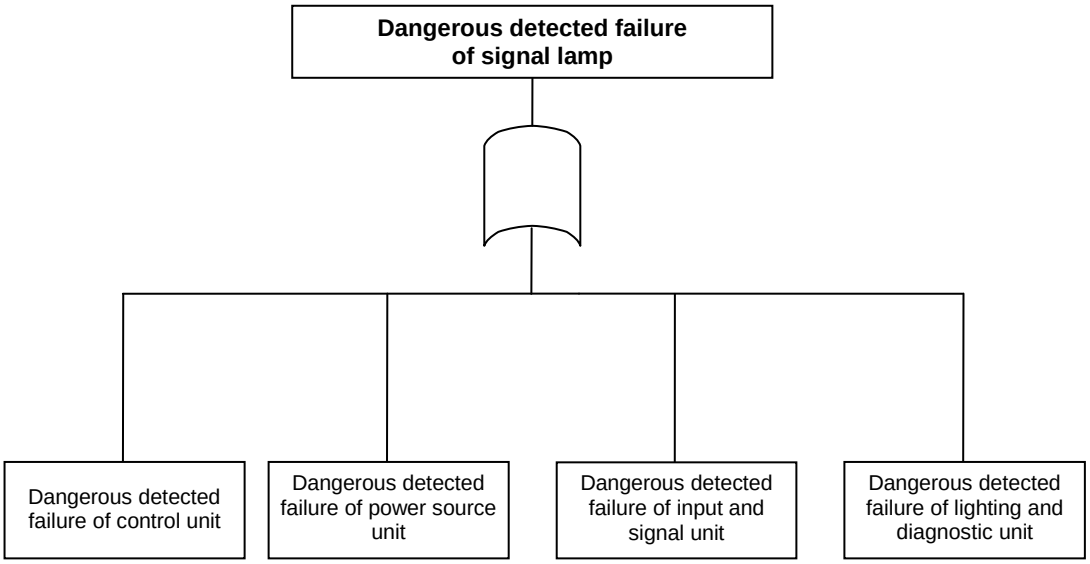
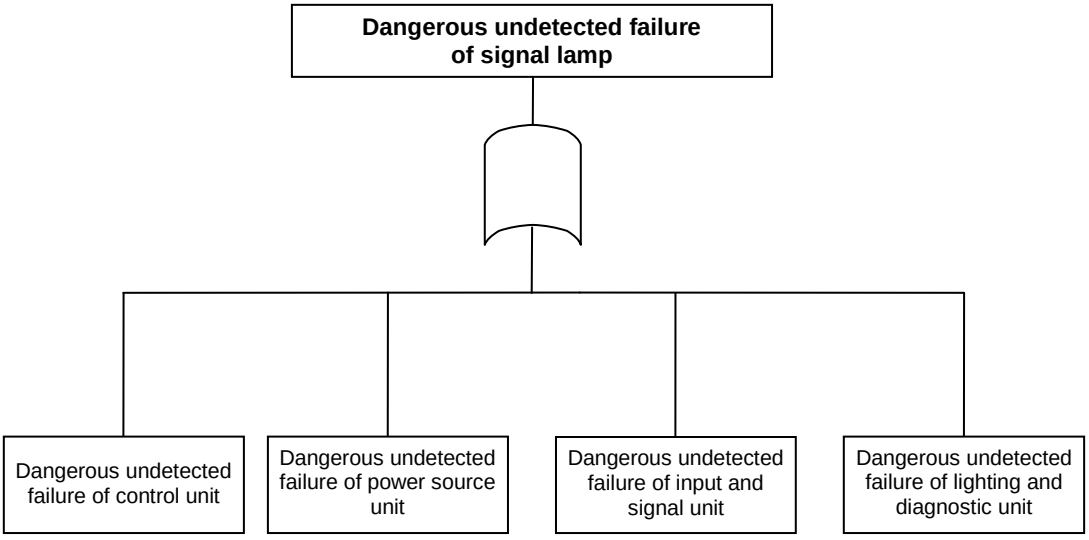
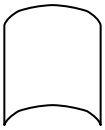


Figure No. 5: FTA – Dangerous detected failure of signal lamp



Notes:



OR Gate
logic 1 – failure state
logic 0 – failure free state

Figure No. 6: FTA – Dangerous undetected failure of signal lamp

Failure rate of each signal lamp unit dangerous failure presents sum of its component failure rates (with supposition of exponential distribution of time to failures and series component arrangement in reliability block diagram of each signal

lamp unit). Component failure rate data are determined on the basis of component manufacturer information or, if they are not available, with use of standard MIL-HDBK-217F Reliability Prediction of Electronic Equipment [7].

Component failure rates of dangerous detected failures and dangerous undetected failures are specified on the basis of possible failure analysis and diagnostic coverage of each signal lamp component. There are analyzed failure types as circuit opening, short circuit or drift and function change [4]. For each mentioned failure effect is determined the ratio of detection possibility assuming that the relevancy of all three viewed states is the same. The fraction of this analysis is shown in the Table No. 1. The calculated values of mentioned failure rates for each signal lamp unit are represented in the Table No. 2.

Table No. 1: Fraction of component diagnostic coverage analysis

Component			Open circuit		Short circuit		Drift, function		λ_{COMP} [h^{-1}]	λ_D [h^{-1}]	λ_{DD} [h^{-1}]	λ_{DU} [h^{-1}]
designation	value	number	detect.	undetect.	detect.	undetect.	detect.	undetect.				
...												
C8	330pF	1	0,9	0,1	0,9	0,1	1	0	3,90E-08	3,90E-08	3,64E-08	2,60E-09
R17 - R20	39W	4	0,9	0,1	0,9	0,1	1	0	3,00E-10	1,20E-09	1,12E-09	8,00E-11
L2	33mH	1	1	0	0,9	0,1	1	0	4,60E-08	4,60E-08	4,45E-08	1,53E-09
C9-11,22,23	100uF	5	0,99	0,01	1	0	1	0	3,90E-08	1,95E-07	1,94E-07	6,50E-10
C12 - C17	100N	6	0,99	0,01	0,9	0,1	1	0	3,90E-08	2,34E-07	2,25E-07	8,58E-09
R21	2,2kW	1	0,99	0,01	1	0	0,99	0,01	3,00E-10	3,00E-10	2,98E-10	2,00E-12
...												

Table No. 2: Failure rates of signal lamp BKS02 units

Signal lamp unit	**$\Sigma \lambda_D$ [h^{-1}]**	**$\Sigma \lambda_{DD}$ [h^{-1}]**	**$\Sigma \lambda_{DU}$ [h^{-1}]**
Control unit	1,42E-06	1,31E-06	1,14E-07
Power source unit	2,46E-06	2,43E-06	2,26E-08
Input and signal unit	2,78E-06	2,36E-06	4,22E-07
Lighting and diagnostic unit	4,50E-04	4,43E-04	7,50E-06
Signal lamp BKS02	**4,57E-04**	**4,49E-04**	**8,06E-06**

Diagnostic coverage for signal lamp BKS02 is given according to Equation (1):

$$DC = \frac{4{,}49 \cdot 10^{-4}}{4{,}49 \cdot 10^{-4} + 8{,}06 \cdot 10^{-6}} = 0{,}982 \qquad [-]$$

This diagnostic coverage value corresponds to limits of safety integrity level SIL 2 for one channel hardware architecture, type B system (0,9 ÷ 0,99) [2].

Target failure measure results from the definition and the Equation (2) and for signal lamp BKS02 has the value:

$$PFH_{SYS} = \frac{1 - e^{-8{,}06 \cdot 10^{-6} \cdot 50000}}{50000} = 6{,}635 \cdot 10^{-6} \qquad [h^{-1}]$$

This calculated value falls into limits for safety integrity level SIL 1 for high demand or continuous mode of operation (10^{-5} ÷ 10^{-6} h^{-1}) [1]. Due this reason the signal lamp BKS02 must be categorized on lower safety integrity level SIL 1.

Value used in the calculation of equivalent down time (50 000 hours) corresponds to total accumulated lifetime of signal lamp due to its specified maintenance system which does not demand realization of safety function proof test [4].

Equivalent down time of signal lamp presents only accumulated operation time and that does not include signal lamp time to repair because during this time the rail

vehicle is not in operation. Essentially, signal lamp restoration is realized during vehicle down time in maintenance, at the same time the signal lamp is not in operation, thereby the hazardous event cannot occur.

Conclusion

On the basis of random hardware failure assessment of LED based signal lamp BKS02 the calculated values of diagnostic coverage and target failure measure correspond to requirements for the lowest safety integrity level, category SIL 1 for systems with high demand or continuous mode of operation according to the standard IEC 61508 Functional safety of electrical/electronic/programmable electronic safety-related system.

This standard presents useful instrument for RAMS parameters assessment of railway vehicle electronic parts, besides the standard EN 50126 Railway applications – The specification and demonstration of reliability, availability, maintainability and safety (RAMS). This standard describes general principles of risk assessment and necessary measures for risk reduction but it does not contain any specific quantitative values, contrary to methods used for functional safety assessment.

References

[1] IEC 61508-1 Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 1: General requirements.

[2] IEC 61508-2 Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 2: Requirements for electrical/electronic/programmable electronic safety-related systems.

[3] IEC 61508-4 Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 4: Definitions and abbreviations.

[4] IEC 61508-6 Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 6: Guidelines on the application IEC 61508-2 and IEC 61508-3.

[5] BRIŠ, R. Aplikovaná matematika [online]. Ostrava: VŠB – Technická univerzita Ostrava, 2003. [cit. 2009-02-10]. <http://am.vsb.cz/bris>.

[6] Vyhláška č. 173/1995 Sb. Ministerstva dopravy ze dne 22. června 1995.

[7] MIL-HDBK-217F Reliability Prediction of Electronic Equipment.

The article was supported by project programme TANDEM of Ministry of Industry and Trade of Czech Republic, project registration number FT-TA4/036, titled *"Development of railway vehicle control system with guaranteed RAMS parameters"*.