Article citation info:
OZ MA, KAYMAKCI OT, KOYUN A. A safety related perspective for the power supply systems in railway industry. Eksploatacja i Niezawodnosc – Maintenance and Reliability 2017; 19 (1): 114–120, http://dx.doi.org/10.17531/ein.2017.1.16.

Muhammet Ali OZ
Ozgur Turay KAYMAKCI
Ayhan KOYUN

A SAFETY RELATED PERSPECTIVE FOR THE POWER SUPPLY SYSTEMS IN RAILWAY INDUSTRY

BEZPIECZEŃSTWO SYSTEMÓW ZASILANIA W PRZEMYŚLE KOLEJOWYM

Within its structure railway transportation systems contain very critical subsystems that can seriously harm the system itself, people or the environment if not properly controlled. Therefore, these critical subsystems are analysed according to the related standards and necessary safety functions are implemented, verified and operated. On the other hand, railway power supply system, which is a critical subsystems, is generally properly analysed from a reliability perspective whereas the corresponding safety related functions are roughly examined. This paper proposes that the railway power supply systems should be considered as safety critical systems and justifies this proposal using risk analysis as presented in the standard IEC 61508. The safety related functions of the system are examined and each function is modelled in detail using Markov modelling method. These models are implemented over a power supply system of Istanbul Transportation Co. and SIL values of the safety functions are calculated using these modular and easily adaptable Markov models. Furthermore the obtained results are compared with simplistic Fault Tree analysis (FTA) and the significance of accurate calculation is demonstrated.

***Keywords**: Markov models, reliability, formal modeling.*

W skład struktury kolejowych systemów transportowych wchodzą krytyczne podsystemy, które, nieodpowiednio monitorowane, mogą narażać sam system, a także ludzi oraz środowisko na poważne szkody. Dlatego też, podsystemy krytyczne analizuje się zgodnie z odpowiednimi normami oraz wdraża w nich, weryfikuje i realizuje niezbędne funkcje bezpieczeństwa. W przypadku systemów zasilania kolei, które należą do grupy podsystemów krytycznych, system na ogół analizuje się dokładnie z punktu widzenia niezawodności, natomiast funkcje bezpieczeństwa bada się jedynie pobieżnie. W prezentowanej pracy postuluje się że systemy zasilania kolei powinny być traktowane jako krytyczne dla bezpieczeństwa, co autorzy uzasadniają z wykorzystaniem analizy ryzyka przedstawionej w normie IEC 61508. W proponowanym rozwiązaniu, bada się funkcje bezpieczeństwa systemu, przy czym każda funkcja zostaje szczegółowo zamodelowana za pomocą metody modelowania Markowa. Modele tego typu wdrożono w systemie zasilania firmy Istanbul Transportation Co. Wartości poziomu nienaruszalności bezpieczeństwa (SIL) badanych funkcji bezpieczeństwa obliczano za pomocą wspomnianych modularnych modeli Markowa charakteryzujących się łatwością adaptacji. Ponadto, uzyskane wyniki porównano z symplistyczną analizą drzewa błędów (FTA), a także wykazano znaczenie prowadzenia dokładnych obliczeń.

***Słowa kluczowe**: modele Markowa, niezawodność, modelowanie formalne.*

1. Introduction

Railways and highways are the two main means of public transport over the land. When compared to highways, railways are much more advantageous due to the fact that railways can carry a large amount of cargo and larger number of passengers faster and more comfortable over long distances. These advantages result in more railways being built especially in urban areas and more passengers choosing railway transportation. This increasing demand has forced the local operators to decrease the headway times up to 90 seconds and the availability of the overall system has become more important than ever. So that an incident or major failure can cause catastrophic problems for operating companies and this is unacceptable in any situation. Therefore analyzing the risks and the verification of the SRFs that satisfy the corresponding safety level is mandatory according to CENELEC 50126 [2].

Most of the railway systems, such as rolling stocks [13], fire safety systems [11] and railway trackside equipment [14], are already considered as safety related system. Whereas railway safety, railway power supply system's availability is usually analysed from a reliability perspective using methods such as Bayesian networks [22], state-space partitioning [7] and an innovative method supported by state enumeration technique [5]. In a study by Rosinski A. and Dabrowski T. issues related to the reliability of power supply systems have been discussed and analysed [19]. On the other hand, if a safety related function does not operate properly on time, the system and the establishment can be seriously harmed. Therefore only calculating the reliability of the power system is not enough to guarantee system availability but also system's safety level must be greater than an expected value. In this context, all safety functions of the railway power supply system should be assessed according to IEC 65108 perspective and a detailed analysis containing failure modes should be made. This paper proposes that the railway power supply systems have to be analysed as a safety related system. For this purpose a risk analysis is made and the corresponding safety related functions are examined and each function is modelled in detail using Markov modelling method. The justification of the proposal and the developed easily adaptable Markov models can be considered as the original contributions of this study. Also this study points out the risks of inaccurate calculation of the SIL level by comparing applied detailed Markov model results to applied Fault Tree results.

For safety assessments a system modelling method is needed in order to determine safety integrity level (SIL) of the system. In general, Fault Tree method is used and this method is also recommended by the standard IEC 61025 [9]. Fault Tree analysis is a simple and a primitive method. This method is also insufficient to reflect the dynamics of the system when the system have too many failure modes. In spite of all the drawbacks of Fault Tree analysis, it is frequently used. Collong and Kouta evaluated probability of explosion and identified critical failure sequences of a fuel cell system using Fault Trees [3].To overcome the drawbacks of FTA modified versions of Fault Tree method such as conditional Fault Tree [20] or combination of methods such as fuzzy logic [16] and generic algorithm [12] with FTA can be used. Detailed modelling capabilities of Markov modelling makes it a better alternative and is used by many researchers when modelling safety related systems for instance systems with self-diagnostic components [23] and redundant standby safety systems [8] and is also used for different purposes such as SIL verification [21] and performance assessments [15]. In this paper Markov modelling technique, which is recommended by the standard IEC 61165, will be used for its detailed modelling capabilities and precise results. It is also be noted that the created models are modular and easily adaptable for all railway power supply systems.

The organization of paper is as follows, in section 2 parameters and techniques used in the paper will be explained. In section 3 the power supply system, which is analysed, will be introduced and the desired SIL level of the power supply system is obtained by examining the risk factors. Railway power supply system's safety related functions are examined and each function is modelled in detail using Markov modelling method in section 4. Finally results and discussions are given in section 5.

2. Safety relaed system

A safety-related system is a system which ensures or maintains safety therefore correct operation of this system is crucial for ensuring or maintaining safety. The purpose of a safety related system is to transit the system to a safe state when a dangerous state is detected. All safety related systems are composed of a combination of sensors, logic solvers and final elements. There are three stages of a properly realized of safety life cycle SRS called design, implementation and operation phases. Existing standards act a guide and explain the important steps of the safety life cycle. Major necessities of all phases are defined in the IEC 61508 standard [9]. EN 50128 describes the essential aspects of developing software for E/E/PE systems used in railway safety related applications (CENELEC 2011) [10].

Table 1. Risk factor parameter explanations

Parameters		Description
Consequence (C)	C_a	Minor injury
	C_b	Serious injury
	C_c	Death of a person
	C_d	Death of more than one person
Frequency and exposure time risk (F)	F_a	Rare exposure risk
	F_b	Frequent exposure risk
Possibility of avoidance of hazard (P)	P_a	Possible under certain conditions
	P_b	Risk prevention very low
Frequency of occurrence of hazard without protection system (W)	W_1	Very slight probability of hazardous incident
	W_2	Slight probability of hazardous incident
	W_3	High probability of hazardous incident

2.1. The safety lifecycle

The safety life cycle is a series of phases starting from initiation to specifications of safety requirements. It covers the design and development of safety features in a safety-critical system, and the termination of that system. In the analysis phase a risk and hazard analysis is made for the designed system. Frequencies, causes and aftereffects of possible threats are considered when the operation mode of the SRS is determined. IEC 61508 determines the operation mode of the SRS with the demand rate. Also at this phase a SIL (Safety integrity level) is assigned to the system which is a measurement of performance required for a safety instrumented function.

One of the methods, which is approved by IEC 61508, for determining the required safety integrity level of the system is the risk graph. Risk graph method requires the knowledge of the risk factors of the system. The risk factors associated with the system are represented as C, F, P and W parameters. The description of these parameters is as give in table 1.

There are six possible outcomes of the risk graph. Numbers 1 through 4 indicate the safety integrity level where integrity level increases from level 1 to 4 meaning 4 represents the highest and level 1 represents the lowest integrity level. The symbol "a" represents there is no safety requirement and the symbol "b" means a single E/E/PE safety system is not sufficient. The risk graph method, which is obtained from IEC 61508 Part 5 Annex B (IEC 2002), is given in figure 1.

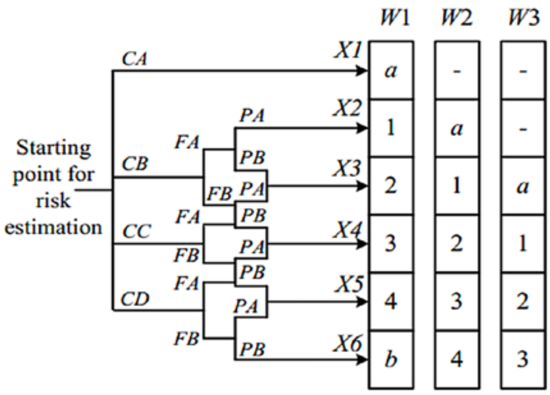

Fig. 1. The risk graph

2.2. Functional reliability parameters

Some reliability parameters for the safety related systems are introduced by the IEC 61508 standard. These parameters are used to classify hardware aspects of systems. Below are some of the major related parameters:

Failure rate: Failure rate is the frequency with which a system or component fails, expressed in failures per unit of time and is represented by λ. Failure rates can be categorized into safe failures (S) and dangerous failures (D). As shown in Equation (1) and Equation (2), dangerous failures can also be separated into two types called detectable dangerous failures (DD) and undetectable dangerous failures (DU) [1].

$$\lambda = \lambda_d + \lambda_s \tag{1}$$

$$\lambda_d = \lambda_{du} + \lambda_{dd} \tag{2}$$

Safe failure factor: the relation between λ_d and is λ_s described with safe failure factor S as given in equation (3):

$$S = 100(\lambda_d / \lambda) \tag{3}$$

Safe failure fraction (): Safe failure fraction is the ratio of the total safe failure rate of a subsystem plus the dangerous detected failure rate of the subsystem to the total failure rate of the subsystem. The calculation of SFF is shown in Equation (4) and is proposed in IEC 61508-6 Annex C:

$$SFF = \frac{\sum \lambda_s + \sum \lambda_{dd}}{\sum \lambda_s + \sum \lambda_d} \tag{4}$$

Proof test Interval (Ti): It is the interval of time between two proof tests. According to the IEC/EN 62061 proof test is a test to detect fault and degradation in SRCs in order to restore the system to brand new condition. All dangerous faults must be detected while proof testing.

Mean time to failure (MTTF): According to the standard IEC/EN 60050, it is the statistical average elapsed time until the first occurrence of failure of a system or a unit [17]. This time is depended on the architecture and the failure rate of the system.

Mean time to repair (MTTR): It represents the average time required to repair a failed component or device. IEC/EN 61508 defines MTTR as 8 hours.

Probability of failure on demand (PFD): A value that indicates the probability of a system failing to respond to a demand. Usually average probability of failure on demand is discussed in SRS [17]. PFD_{avg} value is defined in Equation (5):

$$PFD_{avg} = \frac{1}{T}\int_0^T P(t)dt \tag{5}$$

Hardware fault tolerance (HFT): HFT is the number of hardware faults that the system or the unit can tolerate until a dangerous failure [13]. The HFT is calculated as given in Equation (6):

$$HFT_{sys} = \min_{i=1}^{n} HFT_i \tag{6}$$

After the safety related system is designed its performance is calculated and a comparison is made in order to check if the required SIL level has been achieved or not. The SRS must be improved until the required SIL level is achieved. The performance of the SRS is measured using the PFD_{avg}, PFH, SFF and HFT measures. The standard takes into account PFD_{avg} for low demand system and PFH for high demand systems. Table 2 shows SIL levels and their corresponding probability intervals for PFD_{avg} and PFH. Table 3 shows the maximum allowable SIL when SFF and HFT is taken into account. Values of table 2 and table 3 are taken from the standard IEC 61508. IEC 61508 defines the safety level and safety conditions that must be ensured by all E/E/PE devices and all industrial standards are derived from this standard. Therefore these values are well suited for this study.

Table 2. PFD_{avg} and PFH values and their corresponding SIL levels

SIL	PFD_{avg}	PFH
4	$\geq 10^{-5}$ to $< 10^{-4}$	$\geq 10^{-9}$ to $< 10^{-8}$
3	$\geq 10^{-4}$ to $< 10^{-3}$	$\geq 10^{-8}$ to $< 10^{-7}$
2	$\geq 10^{-3}$ to $< 10^{-2}$	$\geq 10^{-7}$ to $< 10^{-6}$
1	$\geq 10^{-2}$ to $< 10^{-1}$	$\geq 10^{-6}$ to $< 10^{-5}$

Table 3. Maximum allowable SIL *for a safety related function*

SFF	HFT		
	0	1	2
≤ 60%	Not Allowed	SIL 1	SIL 2
60% – <90%	SIL 1	SIL 2	SIL 3
90% – <99%	SIL 2	SIL 3	SIL 4
≥ 99%	SIL 3	SIL 4	SIL 4

2.3. Markov Model Analysis

In safety related systems system availability is very important therefore these systems are usually repairable systems. Simple probabilistic methods cannot adequately model repairable systems when issues such as system configuration, entire or partial system repairs, repair time, diagnostic time, diagnostic coverage, etc. are taken into consideration. In order to introduce these parameters Markov model is a good alternative. Markov models have two components: states and the transitions. States are represented by circles while transition curves are represented by lines with direction arrows.

These transition rates and the states can be written as a matrix rows representing states and matrix entities representing transitions. System model can be expressed as equation (8) where P is the transition matrix and x is the probability vector of states at time t:

$$\dot{x}(t) = x(t) \cdot P \tag{8}$$

Probability of failure on demand is calculated as shown in equation (9) where the initial state condition vector is x_0 and c is a constant vector defining in which states the system is safe:

$$PFD(t) = 1 - x_0 \cdot x^{Pt} \cdot c^T \tag{9}$$

3. Description of railway power supply systems

Railway systems consist of many critical sub-systems that require clean power without drop-offs or variances which is why power supply systems are a crucial part of the railway systems. Power supply system generally converts the electrical energy from the national grid and feeds all components of the railway system. A malfunction in the power supply system can cause unacceptable situations resulting serious passenger grievances or accidents. In order to prevent these kinds of situations, the safety analysis of the system must be made and the required SIL level have to be accomplished. In this context, a railway power supply system of Istanbul Transportation Co. is analysed as an example system but introduced models in this paper can easily be extended and adopted to other railway power systems.

Railway power supply system consists of five main parts which are traction power transformers, the ring line which connects substations to each other, Medium Voltage Switchgear System, DC Switchgear System and the catenary line.

Power supply system is connected to the national grid via three main feeding points and the traction power needed on the catenary line is supplied through 11 substations. These substations are connected to each other because of high reliability and flexible management advantages. Electrical diagram of the power supply system is given in figure 2.

Inside the substation medium voltage busbar is connected to the traction power transformer via a medium voltage circuit breaker. Traction power transformers have one primary connected in delta and two secondary connected in delta and star. These power transform-

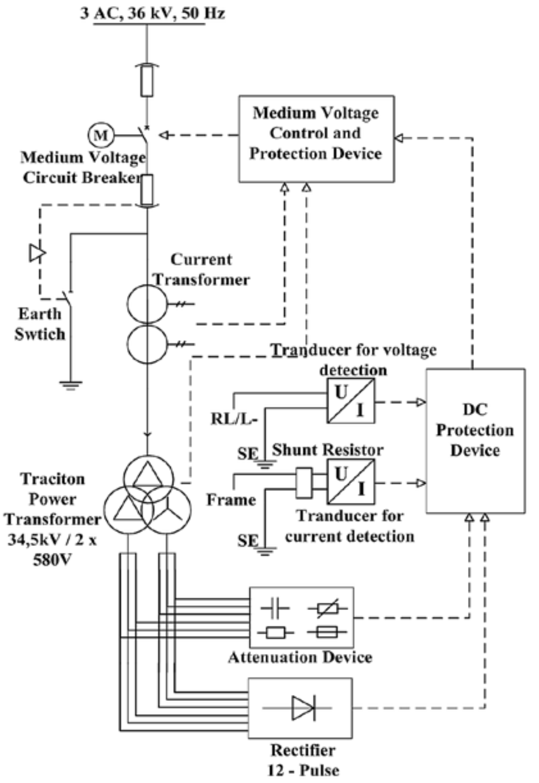
3 AC, 36 kV, 50 Hz
M
Medium Voltage Circuit Breaker
Medium Voltage Control and Protection Device
Current Transformer
Earth Swtich
Tranducer for voltage detection
U
I
RL/L-
SE
Shunt Resistor
DC Protection Device
Traciton Power Transformer 34,5kV / 2 x 580V
Frame
SE
Tranducer for current detection
Attenuation Device
Rectifier 12 - Pulse

Fig. 2. Electrical diagram of the power supply system

ers transform incoming 34,5 kV to 580V. Afterwards a rectifier converts 580 V. AC into 750 V. DC. Positive pole of the rectifier is connected to DC busbar via manual disconnector. From the DC busbar using DC cables, four DC circuit breakers and a manual disconnector the catenary line is energized. Rolling stocks get the power they need from this catenary line using a pantograph and the circuit is completed when the rails are connected to the negative pole of the rectifier by means of disconnector. In this study only the safety system of the traction power transformer's medium voltage circuit breaker is analyzed by taking account the protection functions which protect the traction power transformer and rectifier from the AC and DC side. The safety system consists of four safety related functions which cause a tripping of the traction power transformer's medium voltage circuit breaker as listed below. In the system two control systems are used, one for the DC section and another for the medium voltage section of the system. Voltage detection and current detection which are called frame leakage faults are first received by the control system which is on the DC section then later transferred to the medium voltage control system. In this paper medium voltage control system is considered as the main control system and DC control system is considered as the secondary control system.

Current inside the traction transformers phases is tracked by a connected current transformer. Secondary winding of the current transformer is connected to the main control system and if the current exceeds a predetermined threshold value the main control system sends an open command to the medium voltage circuit breaker.

- The temperature of the traction power transformer's coils is tracked using a thermistor. The temperature readings of the thermistor is monitored by a temperature relay and if the temperature exceeds a predetermined value the main control system sends an open command to the medium voltage circuit breaker.
- This SRF is one of two types of frame leakage fault detections. In this case the voltage between DC switchgear frame (structure earth) and traction earth (negative potential) is measured. This voltage detection identifies dangerous touch voltages which may occur in the switchgear. The measuring value is determined by means of a voltage transducer. If the voltage exceeds a predetermined value four DC circuit breakers through secondary control system and medium voltage circuit breaker through main control system are switched off.
- The other frame leakage fault detection is the current detection between DC switchgear and structure earth. If a current is detected between DC switchgear frame and structure earth this means the isolation between +750 V positive circuits and the frame failed. The measuring value is determined by means of a shunt resistor and a current transducer. If the current exceeds a predetermined value four DC circuit breakers through secondary control system and medium voltage circuit breaker through main control system are switched off.

The block diagram of the system is given in figure 3.

Probability of someone getting harmed inside a power station is very unlikely but since the station feeds trams through the catenary line, high voltages or high currents or even the lack of power can indirectly harm many passengers, personnel and even people nearby tramlines. Based on figure 1, the risk parameters will be CD, FB, PA and W2 respectively. Based on these parameters the required SIL of the system have to be SIL 3 and from table 1 the of the system should be between.

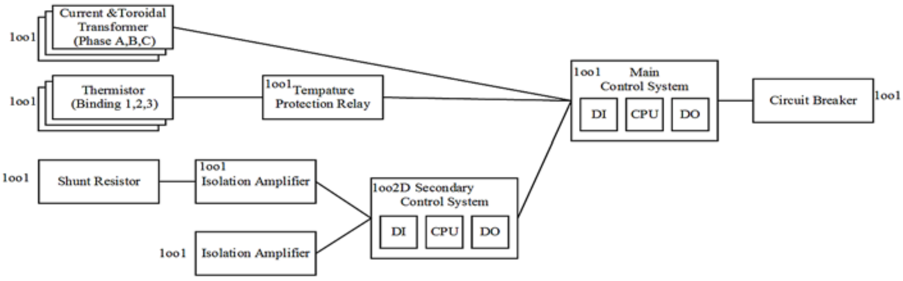
1oo1
Current &Toroidal Transformer (Phase A,B,C)
1oo1
Thermistor (Binding 1,2,3)
1oo1 Tempature Protection Relay
1oo1 Main Control System
DI
CPU
DO
Circuit Breaker
1oo1
1oo1
Shunt Resistor
1oo1 Isolation Amplifier
1oo2D Secondary Control System
DI
CPU
DO
1oo1
Isolation Amplifier

Fig. 3. The block diagram of the system

4. Reliability analysis of the power supply system

An SRS is made up of sensors, control units and actuators. For precise calculation the reliability parameters must be authentic, to ensure this data provided from the vendor and the OREDA (Offshore Reliability Data) has been used in this study and these failure rates of MV switchboard is given in table 5 [4]. There are 6 main SRFs in this safety system and they are described in table 4.

Table 4. The description of the SRFs

SRF Number	Description
SRF 1	Power transformers phase current is above limit detection function
SRF 2	Power transformers temperature is above limit detection function
SRF 3	Catenary voltage is above limit detection function
SRF 4	Catenary current is above limit detection function

Table 5. Failure rates of the MV switchboard

Parts and components	Failure Mode	Fault Type	Failure Rate	
Current & toroidal transformer	Burn out / loss of insulation	Dangerous undetected	λ_{Tdu}	0.28*10-6
Thermistor	Burn out / Faulty Measurement	Dangerous undetected	λ_{Thdu}	0.354*10-6
Main Control unit	Loss of function	Dangerous detected	λ_{Cdd}	0.322*10-6
Compartments of the Switchboard	Loss of insulation property & internal arc fault	Dangerous undetected	λ_{SBdu}	0.53*10-6
Apparatus Circuit Breaker	Spurious opening	Safe	λ_{Bs}	0.115*10-6
	Failure to close	Safe	λ_{Bs}	0.285*10-6
	Failure to open	Dangerous undetected	λ_{Bdu}	0.285*10-6
	Leakage of gas	Dangerous detected	λ_{Bdd}	0.148*10-6
Shunt Resistor	Faulty Measurement	Dangerous detected	λ_{SRdd}	2.0*10-9
	Loss of frame earthing	Dangerous detected	λ_{SRdd}	2.0*10-10
Isolation Amplifier	Faulty conversion	Dangerous detected	λ_{IAdd}	0.5930*10-6
	Failure of electrical isolation components	Dangerous detected	λ_{IAdd}	0.0053*10-6
Secondary Control Unit	Invalid info of switching status	Safe	λ_{DCPs}	0.3*10-6
	Faulty function of protection and control switchgear panel	Safe	λ_{DCPs}	1*10-6
	Faulty function of protection	Dangerous detected	λ_{DCPdd}	1.2*10-6
Temperature sensing element	Burn out / loss of insulation	Dangerous detected	λ_{Tsedd}	4.5*10-6
	Wire Short / Drift	Dangerous undetected	λ_{Tsedu}	0.25*10-6
Temperature transmitter	Loss of function	Dangerous detected	λ_{Ttdd}	0.193*10-6
	Loss of function	Dangerous undetected	λ_{Ttdu}	0.085*10-6

Calculations have been done with the following assumptions:

- For all SRF components proof test interval is assumed to be 1 year and testing is presumed to be ideal.
- All redundant components are assumed to have the same failure rate.
- Repair is presumed to be ideal and MTTR is presumed to be 8 hours.
- Cable and pipe installation failures are neglected.
- The beta factor is accepted as 2% which is recommended in IEC61508-6 Annex D.
- An exponential failure rate distribution is presumed for all components as suggested in the ABB Power Technologies handbook and OREDA.
- The detection time is assumed to be 1 hour.
- The probability of two or more components have state transitions at the same time is zero.

The Markov model developed for safety related function 3 is shown in figure 4, where μ_r, μ_{LT} and μ_d represents repair time, testing interval time and detection time respectively. Also μ_S is the addition of all safe failure rates. In the model, state 1 indicates that all components of the system are working flawlessly. State 6 shows the combined safe faults of all components and in this state the system is shut down until all detectable faults are fixed. Thus safe failures effects the reliability of the system negatively but does not affect the safety of the system. State 2 indicates that one of the two secondary control system have failed. Since the secondary control system is 1002D, SRS is still operational. From state 2 if the last secondary control system fails before fault is detected a transition is made to state 3 in which the SRS fails. States 9 and 5 represents when isolation amplifier and main control system fails respectively. If a failure is detected a transition is made to safe state immediately. Only exception being state 7 because it represents an error on the breaker, which is the component that transitions the system into safe state. Lastly states 4 and 5 represent where an undetectable dangerous fault happens on the switchboard and the breaker respectively. These faults are not repairable since they are not detected. Only in states 1, 2 and 6 our system is safe. From the Markov model in fig. 4 translation matrix and the constant matrix are obtained. Substituting probability vector of states, which is calculated from equation (8), into equation (9) PFD_{avg} values are calculated. Following a very similar path PFD_{avg} values for other SRFs can be calculated.

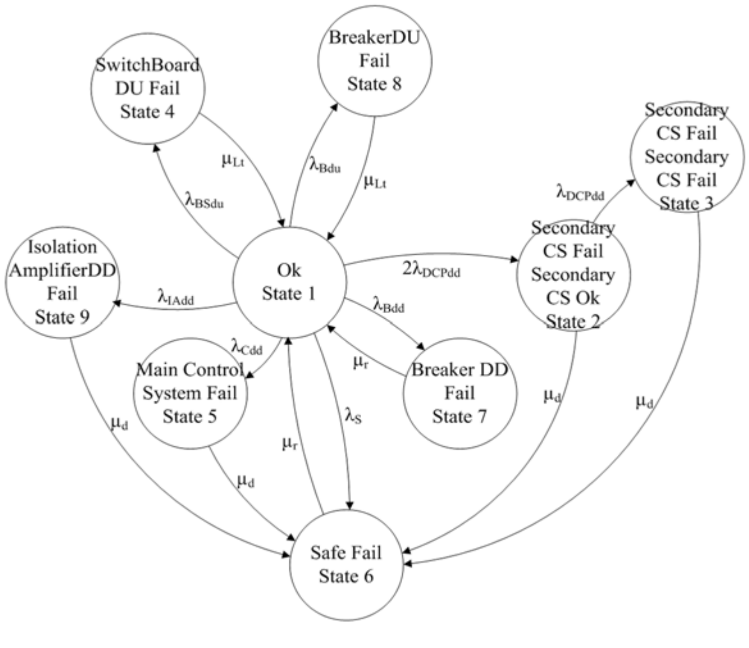
SwitchBoard DU Fail State 4
BreakerDU Fail State 8
Secondary CS Fail Secondary CS Fail State 3
Isolation AmplifierDD Fail State 9
Ok State 1
Secondary CS Fail Secondary CS Ok State 2
Main Control System Fail State 5
Breaker DD Fail State 7
Safe Fail State 6
μLt
λBSdu
λBdu
μLt
λDCPdd
2λDCPdd
λIAdd
λBdd
λCdd
μr
μr
λS
μd
μd
μd
μd

Fig. 4. Markov model for SRF4

Table 6. PFD_{avg} calculation results

SRF Number	PFD_{avg} calculation using Tree Analysis	PFD_{avg} calculation using Markov Analysis	SFF(%)	HFT	SIL
SRF 1	$9.3\ 10^{-3}$	$7.2\ 10^{-3}$	62.50%	1	2
SRF 2	$6.9\ 10^{-2}$	$7.2\ 10^{-3}$	62.50%	1	2
SRF 3	$8.2\ 10^{-3}$	$3.5\ 10^{-3}$	65.25%	1	2
SRF 4	$8.2\ 10^{-3}$	$3.5\ 10^{-3}$	65.25%	1	2

Table 6 shows the results of the analysis and the PFD_{avg} values calculated using Fault Tree analysis. The safety level of the overall system is the minimum SIL of all SRFs. Therefore desired SIL level, which has been decided on as level 3, is not accomplished meaning this railway system is not safe as required.

There is a huge gap between PFD_{avg} values calculated from Fault Tree analysis and Markov model analysis such that in SRF 2 this difference causes the SIL level to appear as level 1 when it should be level 2. It should be noted that if there is inadequate information or less information about the system components then the obtained values from FTA and Markov are nearly same. On the other hand if detailed information is obtained about the system components like detailed failure modes, its failure rates, repair times, diagnostic coverage, proof test interval time, proof test coverage factor, etc. than the calculated PFD_{avg} values are seriously different. This is actually an expected variation as the dynamics of the system can be further expressed by Markov models.

Then these results support our view which is that power supply subsystems of railway systems must be considered and analyzed as a SRS and furthermore while analysing SRSs Markov models should be used because of Markov models highly detailed modelling capabilities.

5. Conclusion

Railway power supply systems are generally not considered as a safety system and therefore they are also not analysed as one. This is a significant hazard for not only human life but also for the system itself. In this paper railway power supply system's safety related functions are examined and each function is modelled in detail using Markov modelling method. The introduced models are modular and can easily be applied to all railway power supply systems. Also the desired safety integrity level of the power supply system is calculated by examining the risk factors. In this context, a power supply system of Istanbul Transportation Co. is analysed to demonstrate how to apply our modelling method and the results strengthen the claim that all railway supply systems should be considered and analysed as safety related systems. Furthermore when Markov modelling and Fault Tree modelling is compared using data from the analysis, the superiority of Markov modelling is observed for this problem. The reason behind this superiority is that the introduced Markov models represent the system failure dynamics better when detailed information on the failure modes of the system components are known.

References

1. Börcsök J., "Functional Safety - Basic Principles of Safety - Related Systems. Huthig Gmbh & Co. KG Heidelberg, Germany, 2007.
2. CENELEC(European Committee for Electrotechnical Standardization). 2011. Railway Applications -Communication, Signaling and Processing Systems - Software for railway control and protection systems. EN 50126 London: British Standard Institution.
3. Collong S. and Kouta R. - Fault tree analysis of proton exchange membrane fuel cell system safety. Int. J. Hydrogen Energy 2015; 40 (25): 8248–8260, http://dx.doi.org/10.1016/j.ijhydene.2015.04.101.
4. DNV (Det Norske Veritas). 2002. OREDA, Offshore Reliability Data Handbook. 4th. ed. Norway: Det Norske Veritas AS (DNV).
5. Eliassi M., Dashtaki A. Khoshkholgh, Seifi H., Haghifam M.-R., and Singh C. - Application of Bayesian networks in composite power system reliability assessment and reliability-based analysis. IET Gener. Transm. Distrib. 2015; 9 (13): 1755–1764, http://dx.doi.org/10.1049/iet-gtd.2014.0660.
6. Eom B. G. and Lee H. S. - Assessment of running safety of railway vehicles using multibody dynamics. Int. J. Precis. Eng. Manuf. 2010: 11 (2): 315–320, http://dx.doi.org/10.1007/s12541-010-0036-x.
7. He J., Sun Y., Kirschen D. S., Singh C., and Cheng L. - State-space partitioning method for composite power system reliability assessment. IET Gener. Transm. Distrib. 2010; 4 (7): 780-785, http://dx.doi.org/10.1049/iet-gtd.2009.0281.
8. Hellmich M. and Berg H. P. - Markov analysis of redundant standby safety systems under periodic surveillance testing. Reliab. Eng. Syst. Saf. 2015; 133: 48–58, http://dx.doi.org/10.1016/j.ress.2014.08.007.
9. IEC (International Electrotechnical Commission). 2002. Electrical/Electronic/Programmable Electronic Safety-Related Systems. IEC 61508. New York: IEEE Standards Association.
10. International Electrotechnical Commission, "BS EN 50128:2011 "Railway applications. Communication, signalling and processing systems. Software for railway control and protection Systems", IEC Standards Online, 2011.
11. Kaymakci O. T., Ustoglu I., and Divriklioglu E. -Reliability assessment of fire safety systems in railway industry: a case study. Journal of the Chinese Institute of Engineers 2015; 38 (3): 286-296, http://dx.doi.org/10.1080/02533839.2014.981208.
12. Longhi A. E. B., A. A. Pessoa, and P. A. D. A. Garcia - Multiobjective optimization of strategies for operation and testing of low-demand safety instrumented systems using a genetic algorithm and fault trees. Reliab. Eng. Syst. Saf. 2015; 142: 525–538, http://dx.doi.org/10.1016/j.ress.2015.06.010.
13. Macii D., Dalpez S., Passerone R., Corrà M., Avancini M., and Benciolini L. - A safety instrumented system for rolling stocks: Methodology, design process and safety analysis. Measurement 2015; 67: 1–13, http://dx.doi.org/10.1016/j.measurement.2015.01.002.
14. Marquez F. P. G., Weston P., and Roberts C. - Failure analysis and diagnostics for railway trackside equipment. Eng. Fail. Anal. 2007; 14 (8): 1411–1426, http://dx.doi.org/10.1016/j.engfailanal.2007.03.005.
15. Mechri W., Simon C., Bicking F., and Othman K. Ben - Fuzzy multiphase Markov chains to handle uncertainties in safety systems performance assessment. J. Loss Prev. Process Ind. 2013; 26 (4): 594–604, http://dx.doi.org/10.1016/j.jlp.2012.12.002.
16. Purba J. H. - A fuzzy-based reliability approach to evaluate basic events of fault tree analysis for nuclear power plant probabilistic safety assessment. Ann. Nucl. Energy 2014; 70: 21–29, http://dx.doi.org/10.1016/j.anucene.2014.02.022.

17. Rausand M. and Høyland A. - System Reliability Theory: Models, Statistical Methods and Applications. Hoboken: John Wiley 2004.
18. Rocha J. M., Henriques A. a., Calçada R., and Rønnquist A. -Efficient methodology for the probabilistic safety assessment of high-speed railway bridges. Eng. Struct. 2015; 101: 138–149, http://dx.doi.org/10.1016/j.engstruct.2015.07.020.
19. Rosinski A, Dabrowski T. - Modelling reliability of uninterruptible power supply units. Eksploatacja i Niezawodnosc – Maintenance and Reliability 2013; 15 (4): 409–413.
20. Shalev D. M. and Tiran J. - Condition-based fault tree analysis (CBFTA): A new method for improved fault tree analysis (FTA), reliability and safety calculations. Reliab. Eng. Syst. Saf. 2007; 92 (9): 1231–1241, http://dx.doi.org/10.1016/j.ress.2006.05.015.
21. Shu Y. and Zhao J. - A simplified Markov-based approach for safety integrity level verification. J. Loss Prev. Process Ind. 2014; 29 (1): 262–266, http://dx.doi.org/10.1016/j.jlp.2014.03.013.
22. Villa-Jaén A. de la, Martínez-Laca-ina P. J., and Martínez-Ramos J. L. - Hybrid procedure including subtransmission systems and substations for reliability assessment. IET Gener. Transm. Distrib. 2013; 7 (12): 1461–1472, http://dx.doi.org/10.1049/iet-gtd.2012.0748.
23. Zhang T., Long W., and Sato Y. - Availability of systems with self-diagnostic components - Applying Markov model to IEC 61508-6. Reliab. Eng. Syst. Saf. 2003; 80 (2): 133–141, http://dx.doi.org/10.1016/S0951-8320(03)00004-8.

Muhammet Ali OZ
Ozgur Turay KAYMAKCI
Department of Control and Automation Engineering
Yildiz Technical University
Esenler/Istanbul, 34220 Turkey

Ayhan KOYUN
Department of Maintenance
Istanbul Transportation Co.
Esenler/Istanbul, 34200 Turkey

E-mails: maoz@yildiz.edu.tr, kaymakci@yildiz.edu.tr, ayhankyn@gmail.com