APPLICATION OF UML MODELLING FOR ANALYSIS OF SAFETY INTEGRITY LEVEL IN RAILWAY TRAFFIC CONTROL SYSTEMS

Mateusz MARZEC, Tadeusz UHL, Tomasz BARSZCZ

AGH University of Science and Technology, Dept. of Mechanical Engineering and Robotics
Al. Mickiewicza 30, 30-059 Kraków, Polska, e-mail: tbarszcz@agh.edu.pl

Summary

Railway traffic control systems require extremely high level of operational safety. Due to very high costs of safety failure, this field is subject to the regulation by numerous norms, which describe formal methods of safety level calculation (denoted as Safety Integrity Level – SIL). Such an analysis is tedious and time consuming, especially in case of complex systems.

The paper proposes application of UML modeling approach to perform joint analysis of the system architecture and its operation. The approach also uses the Fault Tree Analysis (FTA) and can be used to identify the weakest links in the whole system. The method allows to quickly introduce changes in system architecture or parameters and evaluate the impact on the safety. The proposed approach was successfully applied to the real case of a railway system.

Keywords: railway transport, safety integrity level, UML modeling.

ZASTOSOWANIE JĘZYKA UML DO BADANIA POZIOMU NIENARUSZALNOŚCI EZPIECZEŃSTWA SYSTEMÓW STEROWANIA RUCHEM KOLEJOWYM

Streszczenie

Systemy SRK wymagają szczególnie wysokiego poziomu bezpieczeństwa eksploatacji. Ze względu na bardzo wysokie koszty awarii, dziedzina ta jest przedmiotem podlegającym regulacjom wielu norm opisujących formalne metody obliczania poziomu bezpieczeństwa (oznaczony, jako poziom nienaruszalności bezpieczeństwa – SIL). Analiza prowadząca do wyznaczenia poziomu SIL jest trudna i czasochłonna, zwłaszcza w wypadku bardzo skomplikowanych systemów.

Niniejsza praca proponuje aplikację podejścia z wykorzystaniem modelowania UML do przeprowadzania analizy architektury systemu i jego działania. Podejście to korzysta również z analizy drzewa błędów FTA i może być użyte do identyfikacji najsłabszych elementów systemu. Metoda ta pozwala również na szybkie wprowadzanie zmian w architekturze lub parametrach systemu, oraz pozwala obliczyć ich wpływ na bezpieczeństwo. Zaproponowane rozwiązanie zostało z powodzeniem zastosowane w prawdziwym systemie kolejowym.

Słowa kluczowe: ruch kolejowy, poziom nienaruszalności bezpieczeństwa, modelowanie UML.

1. INTRODUCTION

Railway traffic control systems have to conform to very high safety standards. For classification purposes, it is practiced to use the concept of safety integrity levels (SIL), which have been described in PN-EN 61508 norm. Safety integrity levels (SIL) define device/system/subsystem failure probability for the work in continuous or on demand mode. There are four SIL discrete levels under the condition that the level 4 is characterized by the highest safety and the level 1 by the lowest safety. Advanced railway traffic control systems have to conform to the standards of SIL 4, which means 1 failure for no more than 10,000 years. In order to estimate the safety integrity level for the given railway traffic control system, it is required to conduct a complicated reliability analysis based on modeling domain.

The basic aim of the modeling process is deduction about real railway traffic control system which reproduces control tasks [1]. Railway traffic control systems modeling is a very complicated process and both methods and tools used have been changing throughout the years. The present work utilizes the unified modeling language (UML) to describe the architecture and show the dependencies that are present in a prototype system for traffic control at the railway crossings. Created in this way models have considerably facilitated system reliability analysis with the use of fault tree analysis (FTA). Reliability analysis conducted for the described system allowed not only for estimating the safety integrity level (SIL) but also

for establishing weak components in order to increase the reliability.

2. SYSTEM MODEL

Signaling system model has been shown in the Fig. 1

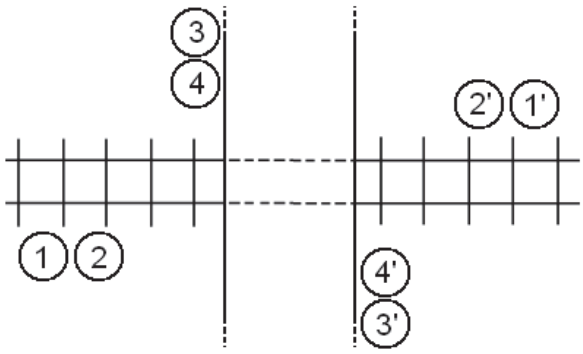

Fig.1 System model:
1, 1' – rangefinder; 2, 2' – camera: 3, 3' – LCD panel; 4, 4' - speaker

The main task of the chosen Signaling system is the improvement of safety at the railway crossings and intersections. The discussed system is a good alternative for the danger signs at the C and D category railway crossings meaning these which do not have their barriers. The main advantage of the system is its price, simplicity and the fact, that it works independently of the systems and devices of the railway traffic control system.

Functioning of the system is based on the detection of the coming to the railway crossing train and displaying the image of the coming train on the LCD panel. Additionally, there is a display of sign "STOP" and sounding of alarm.

3. SYSTEM ARCHITECTURE

The reliability analysis has to be preceded with a careful study of the system functioning and its architecture. The document that is indispensible for the architecture description is the circuit diagram. The circuit diagram shows how the electric and/or electronic elements have been joined together in the system without the reproduction of their physical location in the device. The diagram allows viewing the path of the signals within the device as well as understanding the rule on which basis the device functions. It also facilitates the device service and modifications. It includes information on types and measures of the components, often also the information on the typical voltage and electric current that are present in the circuit in the particular states of its functioning [2].

Electric circuit is very complex and includes much data that is not essential for the reliability test based on fault tree analysis. In order to simplify the circuit diagram, the modular diagrams are applied. They are used to show only signal type, direction and flow path between particular subassemblies. Fig. 2. shows the simplified modular diagram of the system.

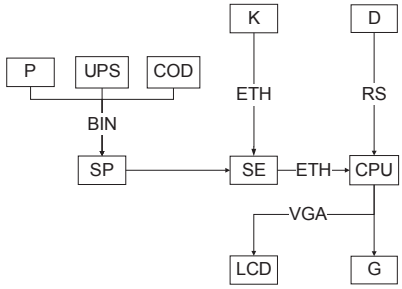

Fig. 2. System circuit diagram: K – camera, D – rangefinder, P – relay, UPS – uninterruptible power supply, COD – case open detector, SP – port server, SE – switch, CPU – computer, LCD – LCD panel, G – speaker

Modular diagrams are indispensible for the deduction about the causes for the function non-completion by particular subassemblies. The drawback of the modular diagrams is that they show only the statics of the system. In order to show dynamics of the system, the UML method has been used.

3.1. UML as a tool for the system dynamics description

In order to describe the operation part of the system, in a sense of the sequence of the conducted operations during a train ride, the UML has been used. The unified modeling language, in practice, has a form of graphical representation of the given system, consisting of logically connected diagrams [3]. Sequence diagram created using Visual Paradigm Software and shown in the Fig. 3. depicts operation of several subassemblies for their realization of the control function with highlighting of the time function. The diagram allows to determine the sequence of the communicates during certain time. UML modeling allows also determining the influence of failure of one element to the other. The drawback of the sequence diagrams is that they omit the secondary importance elements which do not take part in the flow of the main signal, such as the detector whether the case, in which the system is incorporated, is open which can have a critical influence on the reliability test. Modular diagrams and sequence diagrams complement each other and together show complete picture of the system operation describing system statics and dynamics. The discussed models constitute, together with the reliability coefficients, the input data for the reliability test with the use of FTA method.

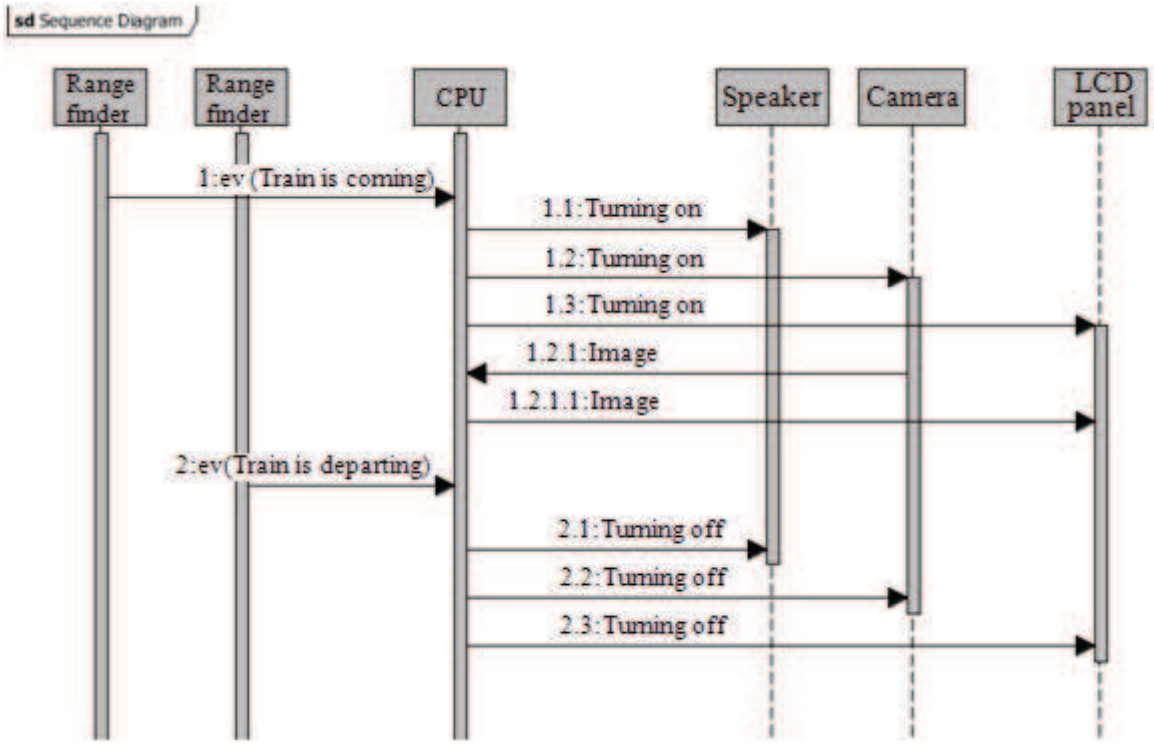

Fig. 3. Sequence Diagram

4. RELIABLITY ANALYSIS

In order to estimate the SIL of the system, the FTA method has been used. The method is based on the modular diagrams and UML sequence diagrams. Sequence diagrams allow to easily comprehend any interaction between specific components which makes the construction of fault tree (FTA) easier. The FTA is one of the most often used methods of system reliability tests. It has been discussed in the IEC1508 standard. The discussed method is a graphic representation of the logical connections with the use of AND, OR and XOR gateways between causes and basic events.

The system analysis with the use of fault tree allows not only to estimate the SIL but also to indicate all possible causes of system's failure. A part of the fault tree for the signaling system in question has been shown in the Fig. 4. Basic event being the top event is system failure, and the cause can be short circuit, unplugging or cut in the Ethernet camera cable.

The next step after the identification of the all possible failure causes is the determination, based on the UML diagrams, of what is the influence of the failure of a particular tree element on the whole system. The determination is made in order to estimate the fraction of safe failures (SFF), which in case of the particular signaling system equals to SFF=73%.

4.1. SIL determination

Subassemblies of the discussed system are widely available on the market, which considerably facilitates the SIL determination. Reliability rates of the assemblies are determined in the process of reliability analyses conducted by the producers, thanks to that subassemblies can be treated globally and assigned particular failure rate λ. In case of the lack of the information concerning reliability rate of a particular component, failure rates of the devices of the same purpose and similar structure have been used. When all the necessary reliability rates are available, they have to be assigned to the particular leaves of the tree and by the use of simple mathematical operations, in which the gateway OR is a multiplication, whereas AND is an addition, the system failure rate is determined, which amount to the level $\lambda=1{,}114\times10^{-5}$. Under the term of failure one has to understand the situations, when there is simultaneous lack of the camera image display, the STOP sign, and the alarm.

Failure rate λ is the inverse of the MTBF value (Mean Time Between Failures). MTBF value for the particular signaling system amounts to $3{,}742\times10^{2}$ days. One must to be aware that MTBF value is not any guarantee or warrantee. The fact that the system is to work for days does not mean that the system will last so many days. A big role is played by the operational conditions as well as the intensity of the usage [4].

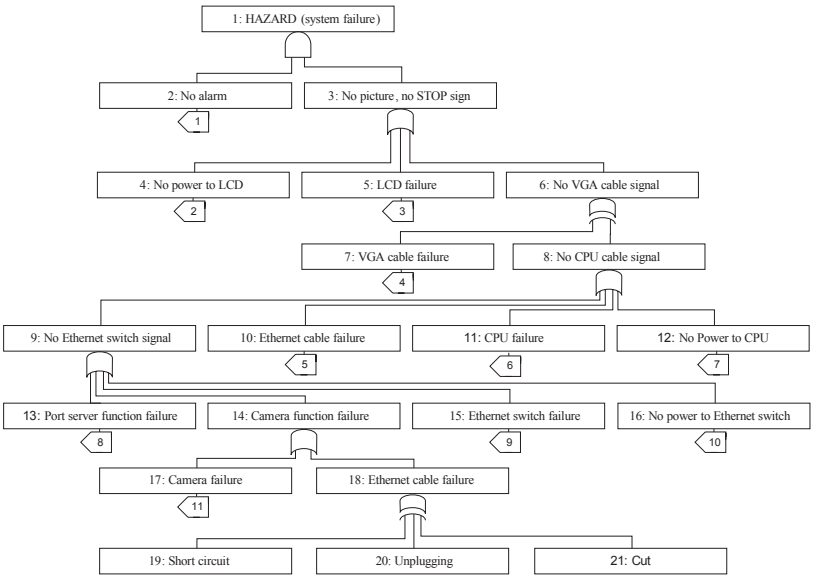

Fig. 4. Part of FTA tree for the Signaling system

System failure rate, determined on the basis of the failure rates of all modules and the possibility of adverse events, amounts to $\lambda=1{,}114\times10^{-5}$. As a consequence of having this value of the failure rate, the given system does not conform to any safety criteria and is not assigned a SIL.

4.2. Required SIL

Advanced railway traffic control systems have to conform to the safety requirements determined at SIL 4. The discussed herein system is not closely connected with railway traffic control, thus it does not have to comply to the safety standards determined at the SIL 4. In order to determine the required SIL of the system, it is necessary to use risk diagram which has been characterized in PN-EN 61508 norm. Risk diagram determines the required SIL on the basis of the consequences of the potential failure, time period, and frequency of finding oneself in the dangerous circumstances, as well as the possibility of the event avoidance and its occurrence probability. The required SIL for the system in question, determined by the use of risk diagram.

As the reliability analysis showed, the system did not met the SIL 1 standards. In further part of the present work, there will be discussed various methods that has led to the improvement in the reliability and as a consequence the system safety requirements have been fulfilled.

5. RELIABILITY IMPROVEMENT METHODS

The system failure rate $\lambda=1{,}114\times10^{-5}$ places itself within the range , which means that it does not meets any safety criteria and cannot have a SIL assigned. The purpose of this chapter is to obtain the SIL 1 as well as presentation of various means of the system reliability improvement.

5.1. The use of components of low failure rate

The use of components which are characterized by high reliability seems to be good way to improve the reliability of the whole system. It has to be noted, though, that the use of all components of high reliability can be uneconomical, what is more it may not improve considerably the overall system reliability. To determine, which components have considerable influence on the system reliability, there have been created graphs showing the relation between failure rates of the particular components (x-axis) and the reliability of the whole system (y-axis). Fig. 5, Fig. 6, Fig. 7, Fig. 8. Show respectively the graphs of the rangefinder, computer, ampfiler and CPU power pack reliability.

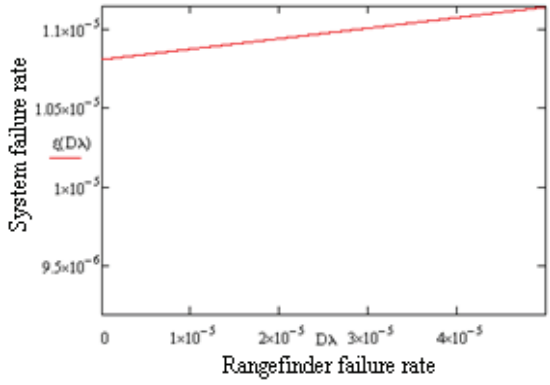

Fig. 5. Rangefinder reliability graph

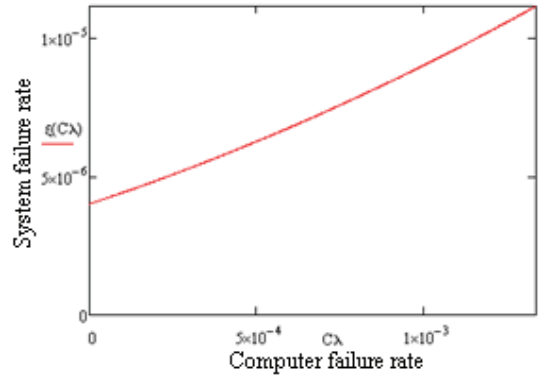

Fig. 6. Computer reliability graph

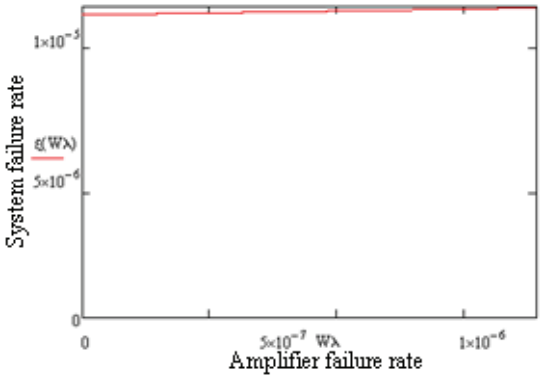

Fig. 7. Amplifier reliability graph

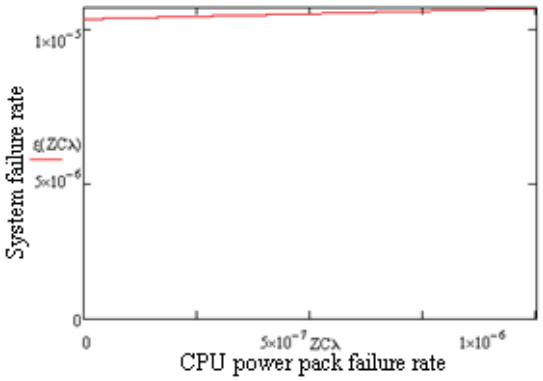

Fig. 8. CPU power pack reliability graph

Analyzing the graphs leads to conclusion that the more inclination to the perpendicular of the curve the more efficiently the reliability of the whole system can be improved by the increase in the reliability of the given component. It appears from the analysis conducted that the greatest influence on the decrease in the failure rate of the system has the computer and the rangefinder, and the smallest: the amplifier, the CPU power pack, and the accumulator. This is why the use of the amplifier, the CPU power pack, and the accumulator with very low failure rate would have no point. It could only increase the costs.

5.2. Application of the right circuit pat tern

It has been calculated on the basis of the fault tree [7] that the smallest failure rate that can be obtained for the discussed circuit pattern amounts to $\lambda=3{,}164\times10^{-6}$, thanks to which the system conforms to the safety standards of the SIL 1. To obtain greater safety, it would be necessary to prevent adverse events such as voltage surge, short circuit, unplugging. It has to be noted that the aim of the present chapter is obtaining by the systems the SIL 1. The applied uninterrupted power supply system (UPS), case open detector (COD), rely, miniature circuit breakers (MCB), and sent systematically to the central office data on the current state of the system results in the fact that the present system architecture ensures the required by the analysis SIL 1.

5.3. Application of the redundancy principles

Redundancy, in practice means the increase in number of a particular component to have greater reliability. Before planning redundancy, one has to consider the consequences of the use of additional subassemblies. In many cases the use of redundant components can have the opposite effect from what has been intended. Additionally, fully redundant system will have double price of the subassemblies.

To obtain the correct redundancy, it is necessary to conduct the analysis of the whole system. In case of the discussed system, the component which decreases the reliability to the most extent is the computer. The use of the second computer is connected with the use of additional power pack, USB hub, VGA switch and RS serial adapters.

In order to show redundancy in the modular diagram, it is necessary to introduce in brief the structure of the system reliability. Reliability structure connects functional failures of the particular components with the failure of the whole system. In classical reliability theory there are distinguished several basic reliability structures, which allows for modeling of functionalities of the analyzed objects. The discussed system has serial reliability structure, in a sense that one component failure causes the failure of the whole system. [5]. System reliability structure with the applied redundancy has been shown in the Fig. 9. The use of the second computer guarantees the safety integrity on the SIL 1, the system failure rate will then amount to $\lambda=3{,}164\times10^{-6}$.

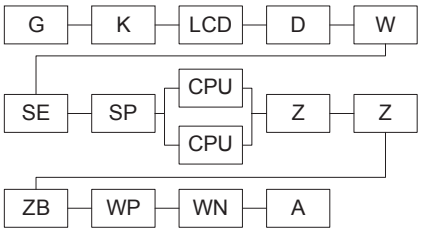

Fig. 9. Reliability structure with redundancy applied: G – speaker, K – camera, LCD – LCD panel, D – rangefinder, W – amplifier, SE – Ethernet switch, SP – port server, CPU – computer, Z – CPU power pack, ZB – buffer power pack, WP – power plug, WN – miniature circuit breaker, A – accumulator

6. SUMMARY

The reliability analysis conducted in the present work has allowed to determine the SIL of the railway system, as well as to indicate all possible causes of the system failure and the systems' weak components. Apparently, UML is a good tool to be used for the description of the system architecture as well as for the simple description of its operation. The use of UML facilitate considerably the reliability analysis with the use of FTA which allows for drawing up conclusions on the influence of the given failure on the particular subassemblies.

BIBLIOGRAPHY

[1] Zabłocki W.: *Modelowanie systemów sterowania ruchem kolejowym – struktury informacji i elementy opisu formalnego*. Prace Naukowe Politechniki Warszawskiej. Transport 2006, z. 57, s. 23-48.
[2] Pełka A.: *Diagnozowanie urządzeń sterowania ruchem kolejowym na przykładzie napędu zwrotnicowego*
. Akademia Górniczo-Hutnicza, Kraków 2009.
[3] Chudzikiewicz A. Uhl T.: *Modelowanie procesów występujących na liniach mało obciążonych*. Prace Naukowe Politechniki Warszawskiej. Transport 2009, z. 69, s. 43-52.
[4] Jones, James V.: *Integrated Logistics Support Handbook*.
[5] Pietrzyk A. Piskorz Z.: *Optymalizacja serwisowania urządzeń technicznych z zastosowaniem algorytmów genetycznych*. Akademia Górniczo-Hutnicza, Kraków 2003.
[6] Polska Norma PN EN IEC 61508.
[7] Marzec M.: *Modelowanie systemów sterowania ruchem kolejowym*. Akademia Górniczo-Hutnicza, Kraków 2011.

Inż. **Mateusz MARZEC** absolwent Wydziału Inżynierii Mechanicznej i Robotyki, Akademii Górniczo – Hutniczej w Krakowie.

Prof. dr hab. inż. **Tadeusz UHL** jest kierownikiem Katedry Robotyki i Mechatroniki, Akademii Górniczo – Hutniczej w Krakowie. W swoich pracach zajmuje się zagadnieniami dynamiki konstrukcji, a zwłaszcza ich analizy modalnej oraz diagnostyki opartej na modelu. Jego zainteresowania obejmują także układy aktywnej redukcji drgań oraz szeroko pojętą mechatronikę.

Dr inż. **Tomasz BARSZCZ**. Pracuje jako adiunkt w Katedrze Robotyki i Mechatroniki. Zajmuje się diagnostyką maszyn oraz systemami monitoringu i diagnostyki. Jest autorem 4 książek i ponad 60 publikacji. Opracowane przez niego systemy pracują na ponad stu kilkudziesięciu instalacjach.