Journal of KONBiN 42(2017)
ISSN 1895-8281
DOI 10.1515/jok-2017-0020 ESSN 2083-4608

APPLICATION OF FMEA METHOD IN RAILWAY SIGNALLING PROJECTS

ZASTOSOWANIE METODY FMEA W PROJEKTACH STEROWANIA RUCHEM KOLEJOWYM

Dariusz Szmel, Dominik Wawrzyniak

Thales Polska sp. z o.o.

***Abstract**: The article presents the FMEA method application, which is relevant in verification of design of two separated railway signalling systems. The efficiency of the method at the stage of the design was discussed. The method was identified as an important element of safety management process and as safety analysis method, which is included in the Safety Case and is applied for the sake of safety arguments and its assessment. Safety process management comprises several phases and appropriate actions, linked with each other in the way to create safety life cycle consistent with system life cycle. The safety case is a set of documents demonstrating that the product is compliant with defined safety requirements including analysis that indicates the correctness of the design and the correct reaction of the system to the failures, with appropriate and requested fail-safe reaction. It is necessary that railway signalling system should fulfil SIL4 requirement and remain safe in case of occurrence any kind of single failure of the equipment considered as possible.*

***Keywords:** FMEA method, safety case process, railway command-control systems*

***Streszczenie:** W artykule został zaprezentowany sposób zastosowania metody FMEA w celu weryfikacji projektu powiązania dwóch autonomicznych systemów srk. Omówiono istotę skuteczności wykorzystanej metody na etapie projektowania, jako istotny element procesu zarządzania bezpieczeństwem oraz jako analiza bezpieczeństwa wchodząca w skład Dowodu bezpieczeństwa wykorzystywanego do oceny i zarządzania argumentami na rzecz bezpieczeństwa. Proces zarządzania bezpieczeństwa składa się z szeregu poszczególnych faz oraz odpowiednich działań, powiązanych ze sobą w taki sposób, aby utworzyć cykl życia bezpieczeństwa, który powinien być spójny z cyklem życia systemu. Dowód bezpieczeństwa stanowi zestaw dokumentów wykazujący, że wyrób jest zgodny z określonymi wymaganiami bezpieczeństwa, w tym odpowiednie analizy potwierdzające poprawność projektu oraz prawidłową reakcję systemu na usterki wraz z właściwą, wymaganą reakcję bezpiecznościową. Konieczne jest, aby systemy wykorzystywane do sterowania ruchem kolejowym zapewniły spełnienie poziomu SIL 4 (Safety integrity level) i pozostały bezpieczne w przypadku wystąpienia jakiegokolwiek rodzaju pojedynczego defektu losowego sprzętu, który jest rozważany jako możliwy.*

***Słowa kluczowe:** metoda FMEA, proces dowodzenia bezpieczeństwa, sterowanie ruchem kolejowym*

APPLICATION OF FMEA METHOD IN RAILWAY SIGNALLING PROJECTS

1. Preface

The article presents the FMEA method application, which is relevant in verification of design of two separated railway signalling systems. The efficiency of the method at the stage of the design was discussed. The method was identified as an important element of safety management process and as safety analysis method, which is included in the Safety Case and is applied for the sake of safety arguments and its assessment. Safety process management comprises several phases and appropriate actions, linked with each other in the way to create safety life cycle consistent with system life cycle. The safety case is a set of documents demonstrating that the product is compliant with defined safety requirements including analysis that indicates the correctness of the design and the correct reaction of the system to the failures, with appropriate and requested fail-safe reaction. It is necessary that railway signalling system should fulfil SIL4 requirement and remain safe in case of occurrence any kind of single failure of the equipment considered as possible.

2. Introduction

The Failure Modes and Effects Analysis (FMEA) is a systematic system analysis technic applied in order to identify possible modes of failures, their causes and effects on the system performance. FMEA was first applied in 60's in USA to astronautics products. This method was used for verification of various elements of spaceships to ensure safety of the expedition and the crew. The success of the method in NASA resulted in application in aerospace and nuclear industry. In 70's and 80's methods was used in Europe and found new applications in chemical, electronic and automotive industry, where the best dynamic of its application have been observed. In 90's the method was adapted within scope of ISO 9000 standard and in particular QS 9000, which was dedicated for automotive industry.
Conducting of the analysis in the early stage of product development cycle guarantee removal or mitigation of the given failure mode and hence costs reduce of the failure detection. FMEA is applied on various levels of system decomposition, from the element or software command to higher level of system modules. It is the type of analysis called "from the part to the whole". At the figure 1 the relationship between failure modes and failure effect were presented, with consideration of a system hierarchy. FMEA is used to identify possible failure modes and delivers input data for identification of mitigation measures in order to minimalize the risk of hazard.

When conducting process of risk estimation it is possible to estimate probability of the occurrence of particular hazard related with specific failure mode.
FMEA considers the separate failure modes and separate failure effects for the system. It means that each failure mode is considered independently. For this reason the method has no application to analysis of dependent failures or failures resulted from sequence of events. In such situations for analysis it is useful to apply other analysis methods such as Fault Tree Analysis (FTA) or Markov process analysis. This is why the FMEA method has application to specific solutions, which comes from e.g. specific track layout at station. At the generic application level several other safety methods are also applied.

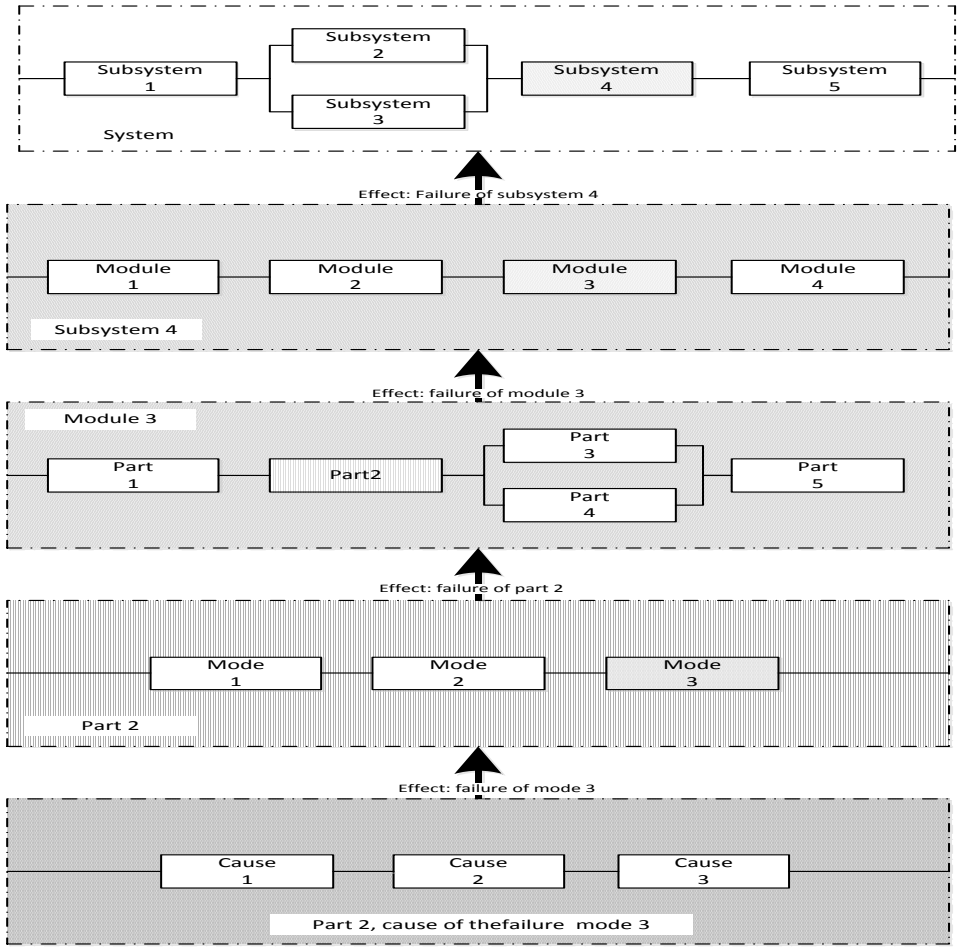


Fig. 1 The relationship between failure modes and effects, source [7]

3. Aim and subject of analysis

The reasons to apply the failure mode and effects analysis are the following:
- identification of failures that can cause undesirable effects during the system operation e.g. stop or degrade the operation or influence the user safety,
- to prove the fulfillment of contract requirements,
- to improve reliability and safety of the system,
- to improve maintainability (e.g. pay attention to risk areas).

From the above reasons the goals for conducting of analysis can be the following:
- complete identification and classification of all undesirable effects in scope of defined borders of the analyzed system and sequence of events caused by each identified failure mode from any causes on various levels of hierarchical system structure,
- assignment of identified failure modes according to characteristics like ease of detection, susceptibility for diagnostic and testability,
- identification of system functional failures and estimation of severity and probability measures,
- elaboration of improvement plan for the design in scope of effects mitigations related with given failure mode,
- to support development of efficient maintenance plan, with goal to mitigate or minimalize the probability of failure,
- to confirm the correctness of design, indicate the method of detection for particular failure modes and system reaction (e.g. fail-safe reaction).

The interface between two independent safety signalling systems can cause mutual interference, which as a result can cause occurrence of unexpected behavior of the particular system. The fulfillment of requirements, regulations and technical specifications by single system does not ensure safety for both connected systems. The hazard analysis is required at each phase of system life cycle. In order to eliminate the hazardous situations, which are the effect of failure of element that is a part of hardware interface, all scenarios should be analyzed at the stage of concept or design with consideration of both interfaced systems and its mutual influence. The reasons that application of FMEA is adequate for this type of the design are the following:
- it results from the detail hazard analysis model for design,
- the tool is adequate for small systems, modules and units,
- it requires comprehensive knowledge of failures characteristics,
- supports hazard identification and unacceptable failure effects
- adaptation to analysis of systems with large number of elements connected with series failure logic,
- identification of causative factor,
- can be used in preliminary design or in the final design (detail design),
- qualitative-quantitative analysis,
- is characterised by great accuracy level (detail level),
- method is inductive.

4. Method of application

The analysis of hardware part of the interface for signalling devices was conducted with consideration of impact of particular interface components failures to connected systems. Failure impact analysis has to verify if single failure of each component is detectable and if it does not lead to hazard. FMEA rely on identification and analysis of failure mechanism, failure causes and their effects. In the first phase the complementary scope of analysis is defined, where boundaries of two systems and components of interface were identified. Then the failures that can lead to hazard or cause lack of system safety reaction were indicated. Using the FMEA tool, the credible failure modes of each applied components were identified. The failure modes, which are considered during the design and analysis process are derived from the Appendix C of norm PN-EN 50129 [6]. The table of failure modes of hardware elements described in the Appendix have been elaborated based on many years of experience and based on other normative documents.

FMEA analysis as well as its extended version with critical states evaluation FMECA (Failure Mode Effects and Criticality Analysis) allows to conduct qualitative and quantitative reliability analysis, with the goal to identify hazards that has impact on correct operation of analyzed systems. For systems that ensure safety traffic control it is not advisable to hierarchy the criticality of the particular states. FMEA analysis were conducted in according to diagram of sequence of actions presented in the norm PN-EN 60812 [7] (see figure 2).

Based on the example of interface hardware design between computer interlocking type ESTW L90 5 from Thales and level crossing system type RBUT-PL of category A from Zelisko the method of FMEA application will be introduced.

First the hazards have been identified and for this purpose the Hazard and Operability Study (HAZOP) method was applied. This method allows to identify global hazards for interfaced system, so in this case:

- too early turning on the warning system on the level crossing,
- passage of train through level crossing with no warning system activated (barriers in up position).

Then the events were specified, which can be hazard from hardware part of interface and direct or indirect causes that lead to the described hazards:

- Wrong information about the state of interfaced devices sent to interlocking computer, which allows train driver to drive with speed higher than permitted (wrong confirmation of level crossing closure).

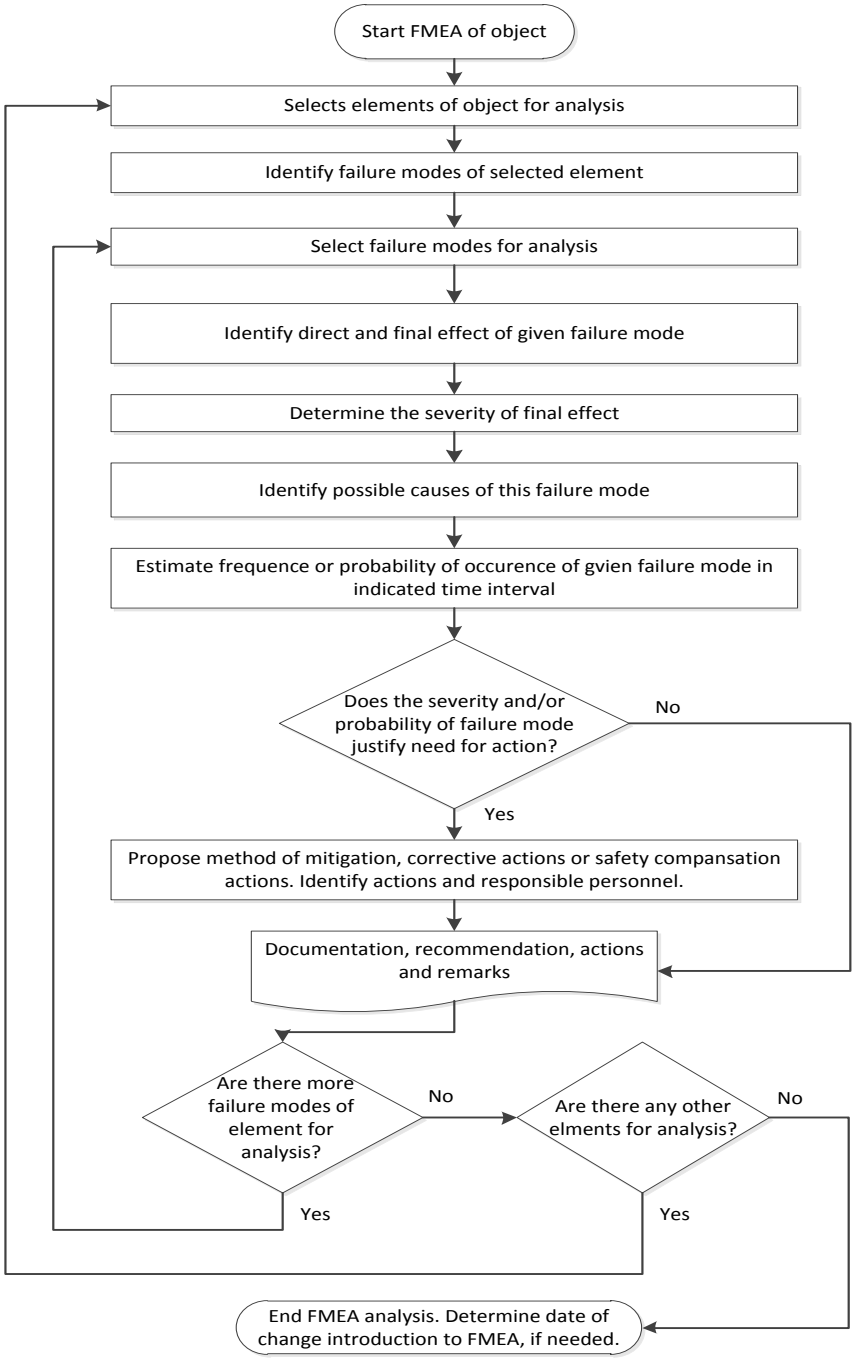


Fig. 2 Diagram of analysis, source: [7]

Next, prepared sheet of FMEA was fulfilled with the following:

- Define hardware elements for analysis (all elements between two independent systems),
- Define failure modes of given element, in case new failure mode was identified, which was considered as credible, but not described in the norm, it is also needed to consider it,
- Define effects of given failure and impact of components on other elements of the interface and on the connected systems,
- Determine detection measures of given failure (with lack of detection it is necessary to assume constant occurrence of given defect),
- Classify the level of hazard for given failure mode in according to table 1 below,
- Estimate risk for failure with different hazard level than C,
- Implement mitigation measures in order to mitigate hazard (e.g. change in the design, addition instruction / restrictions for operator),
- identify and indicate additional safety qualification tests when it is necessary to determine the system reaction in specific event sequence scenario.

Table 1. Hazard levels with description

HAZARD LEVEL	DESCRIPTION
A1	Single failure can lead to hazard.
A2	Multiple failures resulted from single cause can lead to hazard.
B1	Failure is not detected, but do not lead to direct hazard. It is possible that hazard occur when other independent failure occur.
B2	Failure is not detected, but do not lead to direct hazard. It is possible that hazard occur when other independent multiple failures occur.
B3	Failure is detected, but do not lead directly to hazard. It is possible that hazard occur when second independent failure occur.
B4	Failure is detected, but do not lead directly to hazard. It is possible that hazard occur when other independent multiple failures occur.
C	Failure do not lead to hazard.

The analysis for the sample design was conducted with the above description, while selected part of the FMEA sheet was presented in Table 2 below. Review of all failure effects, in the FMEA sheet, indicates that in all cases there is appropriate reaction of system to failure.

Table 2. Part of the FMEA sheet for the design of the interface

Id.	Elements name	Failure Mode	Failure Effect	Failure Detection	Comment	References	Hazard Level
1	2	3	4	5	6	7	8
1	Diode Z1	break	In state of S1 – lack of control of input E1	Error on the interface of level crossing system (not allowed combination of inputs)	Load of output board of RBUT system is ca. 150mA, which in effect the short circuit do not release the overcurrent protection		C
2		Short circuit	In state other than S1 – short circuit between contacts 91 and 92 of system RBUT boards caused by rectifying diode on ESTW board.	RBUT system detects the potential difference between two output contacts, which will be detected as failure of category 1.			C
3		Increase of reverse current	In state other than S1 – short circuit can cause damage of diode and as a result short circuit between contact 91 and 92 at RBUT board.	RBUT system detects the potential difference between two output contacts, which will be detected as failure of category 1.			C
4		Decrease of reverse breakdown voltage	In state other than S1 – short circuit can cause damage of diode and as a result short circuit between contact 91 and 92 at RBUT board.	RBUT system detects the potential difference between two output contacts, which will be detected as failure of category 1.			C

5. Summary

In a result of FMEA analysis and classification of failure effects the hazards at level C were identified. Therefore analyzed failures do not lead to hazard (or probability of occurrence is acceptable low) in railway traffic, which is in accordance with requirements for design of signalling systems.

The report from FMEA analysis and their results serves in common safety method process in scope of risk evaluation and assessment (Common Safety Method on Risk Evaluation and Assessment - CSM-REA) to indicate mitigation of hazards for hardware part of the design in accordance to regulation 402/2013 [8].

The above mentioned report is also considered in Technical Safety Report, which is part of Specific Application Safety Case described in norm PN-EN 50129 [6]. The report confirms that system is in safe state in case of any single failure, which is considered as credible. Application of FMEA method allows to confirm that no single failure mode of hardware component is hazardous, regardless of the method or combination of fail-safe methods that were used.

6. Literature

[1] Ericson C.: Hazard analysis techniques for system safety, A John Wiley & Sons, INC., Publication
[2] Materials from Thales
[3] Materials from Zelisko
[4] Norm PN-EN 50126 Railway application. Specification of reliability, availability, maintainability and Safety.
[5] Norm PN-EN 50128 Railway application. Communication, Signalling and processing systems. Software for railway control and protection systems.
[6] Norm PN-EN 50129:2007 Railway applications - Communication, signalling and processing systems - Safety related electronic systems for signalling.
[7] Norm PN-EN 60812:2009 System reliability analysis technics. Failure mode and effects analysis (FMEA) procedure.
[8] Commission implementing regulation (EU) No 402/2013 of 30 April 2013 on the common safety method for risk evaluation and assessment and repealing Regulation (EC) No 352/2009.
[9] Szopa T.: Reliability and Safety, Printing house of Warsaw University of Technology, Warsaw 2009
[10] Ważyńska-Fiok K.: Basics of exploitation and reliability of transport systems, Printing house of Warsaw University of Technology, Warsaw 1993.

Dariusz Szmel MSc. Eng. *In 2005 graduated at Silesian University of Technology in Katowice, faculty Transport in department of Railway Transport. Since 2006 he is working in Thales Polska Ltd. He is responsible for Safety and quality management. In 2013 member of Certification Board at Railway Institute. In 2016 appointed to Committee to protect the impartiality of Transport Certification Centre at Transport Division of Warsaw University of Technology (Share 60%).*

Dominik Wawrzyniak Eng. *In 2013 graduated engineering study at Warsaw University of Technology in specialization railway traffic control. Practice diploma executed in Warsaw Metro in Signalling and communication department. Since 2013 he is working in Thales Polska Ltd. at position RAMS specialist. In 2016 he finished specialised training in Thales Training Centre in Stuttgart (Share 40%).*

ZASTOSOWANIE METODY FMEA W PROJEKTACH STEROWANIA RUCHEM KOLEJOWYM

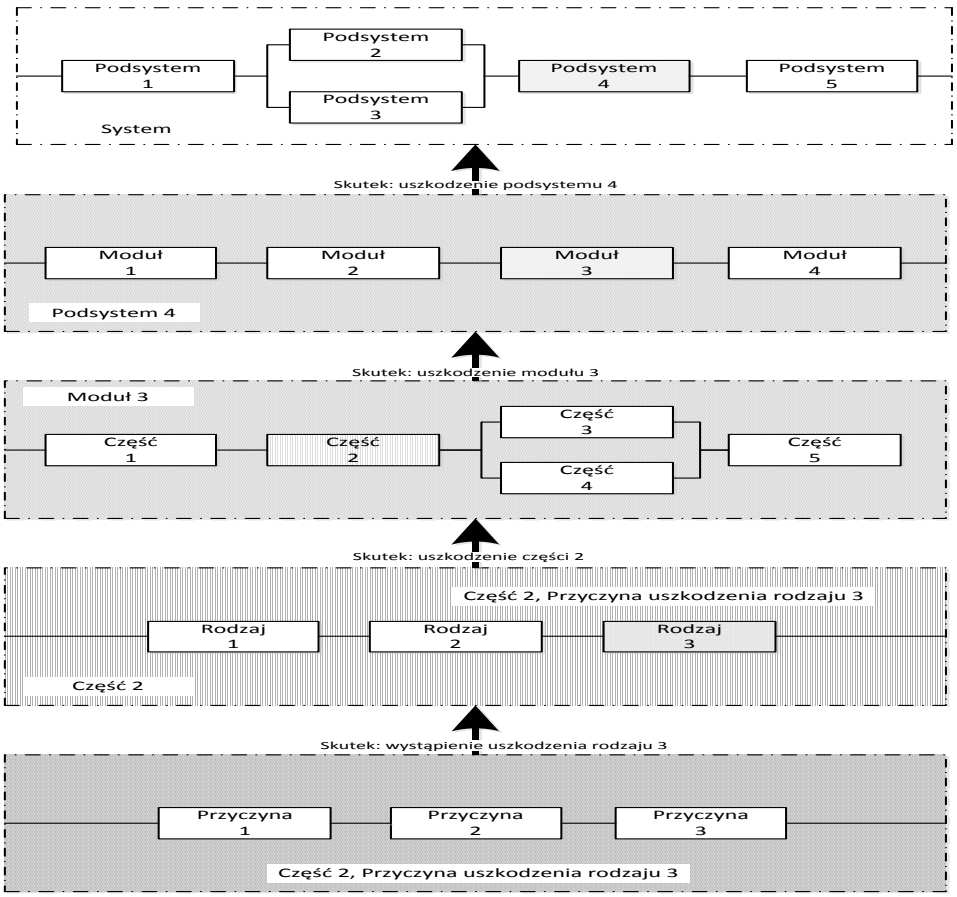
1. Wstęp

W artykule został zaprezentowany sposób zastosowania metody FMEA w celu weryfikacji projektu powiązania dwóch autonomicznych systemów srk. Omówiono istotę skuteczności wykorzystanej metody na etapie projektowania, jako istotny element procesu zarządzania bezpieczeństwem oraz jako analiza bezpieczeństwa wchodząca w skład Dowodu bezpieczeństwa wykorzystywanego do oceny i zarządzania argumentami na rzecz bezpieczeństwa. Proces zarządzania bezpieczeństwa składa się z szeregu poszczególnych faz oraz odpowiednich działań, powiązanych ze sobą w taki sposób, aby utworzyć cykl życia bezpieczeństwa, który powinien być spójny z cyklem życia systemu. Dowód bezpieczeństwa stanowi zestaw dokumentów wykazujący, że wyrób jest zgodny z określonymi wymaganiami bezpieczeństwa, w tym odpowiednie analizy potwierdzające poprawność projektu oraz prawidłową reakcję systemu na usterki wraz z właściwą, wymaganą reakcję bezpiecznościową. Konieczne jest, aby systemy wykorzystywane do sterowania ruchem kolejowym zapewniły spełnienie poziomu SIL 4 (Safety integrity level) i pozostały bezpieczne w przypadku wystąpienia jakiegokolwiek rodzaju pojedynczego defektu losowego sprzętu, który jest rozważany jako możliwy.

2. Wprowadzenie

Analiza rodzajów i skutków uszkodzeń (ang. Failure Mode and Effects Analysis - FMEA) jest systematyczną techniką analizy systemu w celu identyfikacji możliwych rodzajów uszkodzeń, ich przyczyn i skutków odnoszących się do osiągów systemu. FMEA zaczęto stosować w latach 60-tych w USA przy wyrobach dla astronautyki. Metodą tą weryfikowano projekty różnych elementów statków kosmicznych, by zapewnić bezpieczeństwo uczestnikom wyprawy. Sukces tej metody w NASA spowodował, że znalazła ona zastosowanie w przemyśle lotniczym i jądrowym. W latach siedemdziesiątych i osiemdziesiątych metoda ta zadomowiła się w Europie i znalazła nowe zastosowania w przemyśle chemicznym, elektronicznym, a także samochodowym, gdzie zaobserwowano największą dynamikę zastosowania tej metody. W latach dziewięćdziesiątych została zaadaptowana w ramach normy ISO 9000, a w szczególności w QS 9000 przeznaczonej dla przemysłu samochodowego.
Przeprowadzenie analizy we wczesnym okresie cyklu rozwoju gwarantuje usunięcie lub złagodzenie danego rodzaju uszkodzenia, a co za tym idzie, obniżenie skutków kosztowych wykrycia usterki. FMEA stosuje się na rożnych poziomach dekompozycji systemu, od poszczególnych elementów lub komendy oprogramowania w górę do najwyższego poziomu schematu blokowego. Jest to analiza „od szczegółu do ogółu”.

Na rysunku 1 przedstawiono związek pomiędzy rodzajami uszkodzeń i skutkami uszkodzeń, uwzględniający hierarchię systemu. FMEA służy do identyfikacji możliwych rodzajów uszkodzeń i dostarcza danych wejściowych do środków łagodzenia skutków w celu zmniejszenia ryzyka. Przy przeprowadzeniu procesu wyceny ryzyka istnieje możliwość oszacowania prawdopodobieństwa występowania poszczególnych zagrożeń związanych z konkretnym rodzajem uszkodzenia. FMEA powiązana jest z oddzielnymi rodzajami uszkodzeń i skutkami tych uszkodzeń dla systemu. Każdy rodzaj uszkodzenia jest rozpatrywany niezależnie. Z tego powodu analiza ta nie ma zastosowania do rozważania uszkodzeń zależnych lub uszkodzeń wynikających z sekwencji zdarzeń. W takich sytuacjach do analizy mogą być przydatne inne metody badawcze, takie jak analiza drzewa zdarzeń (ang. Fault Tree Analysis - FTA) lub analiza procesów Markowa. Dlatego też metoda FMEA ma zastosowanie do rozwiązań specyficznych wynikających np. z danego układu torowego. Na poziomie aplikacji generycznej (ogólnego zastosowania) stosowany jest szereg innych metod analiz bezpieczeństwa.



Rys. 1 Związek między rodzajami uszkodzeń i skutkami uszkodzeń, źródło [7]

3. Przedmiot i cel analizy

Powody dla których podejmuje się analizę rodzajów i skutków uszkodzeń:
- zidentyfikowanie uszkodzeń, które mogą wywołać niepożądane skutki podczas eksploatacji systemu, np. mogą uniemożliwiać albo istotnie pogarszać eksploatację lub wpływać na bezpieczeństwo użytkownika,
- udowodnienie spełnienia wymagań kontraktowych klienta,
- poprawa nieuszkadzalności lub bezpieczeństwa systemu,
- umożliwienie poprawy obsługiwalności (np. zwrócenie uwagi na obszary ryzyka),

Z powyższych powodów, cele przeprowadzenia analizy mogą być następujące:
- komplementarna identyfikacja i klasyfikacja wszystkich niepożądanych skutków w ramach określonych granic analizowanego systemu oraz sekwencji zdarzeń spowodowanych przez każdy zidentyfikowany rodzaj uszkodzenia, z jakichkolwiek przyczyn na różnych poziomach zhierarchizowanej struktury systemu,
- przyporządkowanie zidentyfikowanych rodzajów uszkodzeń zgodnie z charakterystykami, obejmującymi łatwość ich wykrycia, podatność diagnostyczną oraz testowalność,
- identyfikacja funkcjonalnych uszkodzeń systemu, oszacowanie miar ich dotkliwości i prawdopodobieństwa uszkodzenia,
- opracowanie planu poprawy projektu w zakresie mitygacji skutków związanych z danym rodzajem uszkodzenia,
- wsparcie rozwoju skutecznego planu utrzymania, mającego na celu złagodzenie lub zmniejszenie prawdopodobieństwa uszkodzenia,
- potwierdzenie poprawności projektu, wskazując sposób detekcji dla poszczególnych rodzajów uszkodzeń oraz reakcję systemu (np. fail-safe).

Powiązanie dwóch osobnych bezpiecznych systemów srk może powodować wzajemną ingerencję, w wyniku której możliwe jest wystąpienie nieoczekiwanego zachowania poszczególnych systemów. Spełnienie wymagań, przepisów oraz specyfikacji technicznych przez pojedynczy system nie zapewni nam bezpieczeństwa dla obu powiązanych ze sobą systemów. Analiza zagrożeń wymagana jest na każdym etapie w trakcie całego cyklu życia systemu. W celu eliminacji sytuacji niebezpiecznych będących skutkiem uszkodzenia elementu wchodzącego w skład części sprzętowej powiązania należy na etapie koncepcji lub projektu przeanalizować wszystkie scenariusze uwzględniające powiązane systemy wraz z ich wzajemnym oddziaływaniem. Dlatego zastosowanie techniki FMEA będzie odpowiednie dla tego rodzaju projektu, ponieważ jest to narzędzie:
- wynikające z modelu szczegółowej analizy zagrożeń projektu,
- odpowiednie dla małych systemów, modułów, zespołów,
- wymagające wyczerpującej wiedzy o charakterystyce uszkodzeń,
- identyfikujące zagrożenia oraz nieakceptowalne skutki uszkodzeń,
- dostosowane do rozpatrywania systemów zawierających dużą liczbę elementów powiązanych szeregową logiką uszkodzeń,

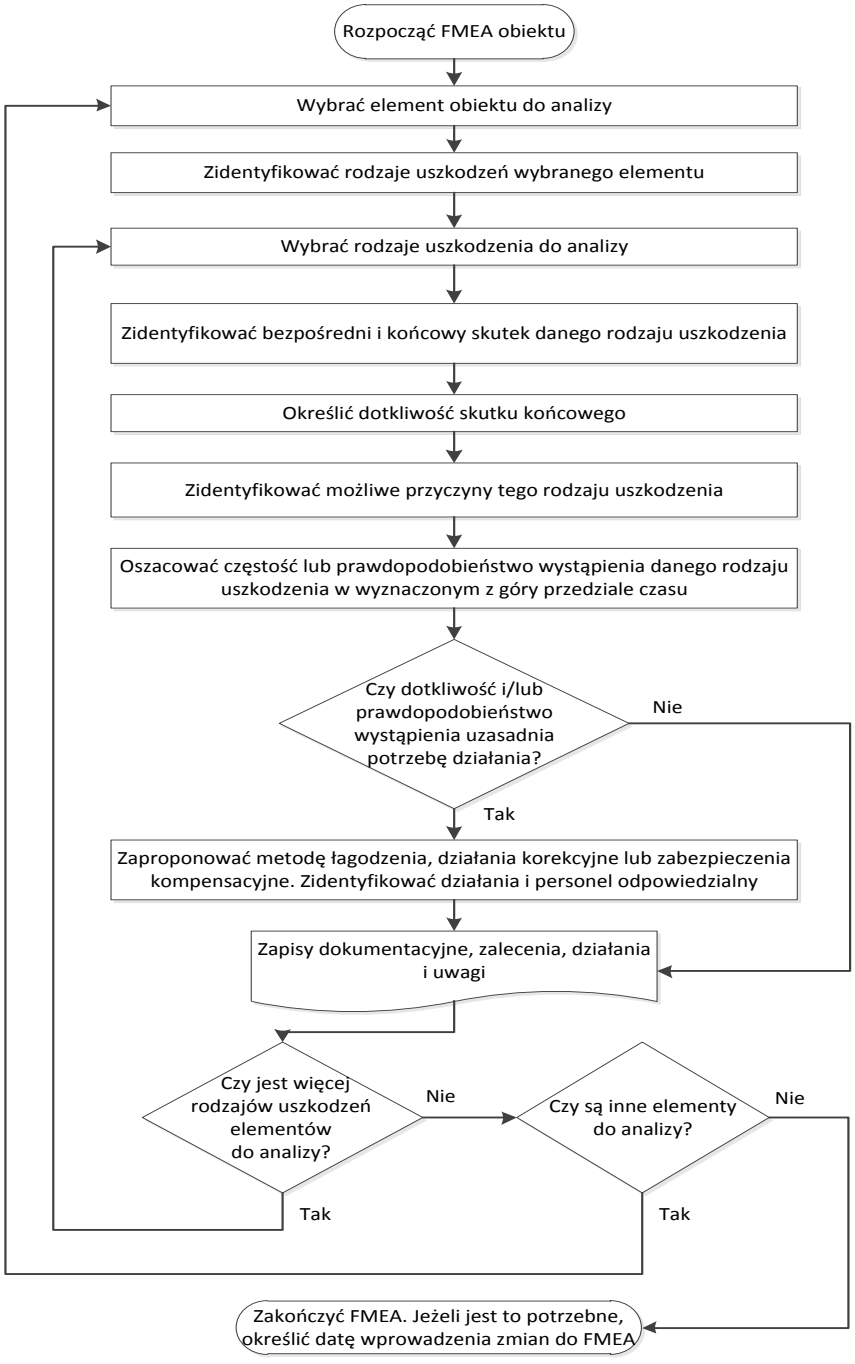
- identyfikujące czynniki sprawcze,
- mogące być użyte w fazie cyklu życia dla projektu wstępnego lub projektu docelowego (projekt szczegółowy),
- jakościowo-ilościowe,
- charakteryzujące się dużym stopniem dokładności (szczegółowości),
- indukcyjne.

4. Sposób zastosowania

Analizę części sprzętowej powiązania dla urządzeń srk przeprowadzono pod kątem oddziaływania uszkodzeń poszczególnych komponentów interfejsu na łączone systemy. Analiza oddziaływania uszkodzeń musi zweryfikować czy pojedyncze uszkodzenie każdego komponentu jest wykrywalne oraz czy nie powoduje zagrożenia. Technika FMEA polega na zidentyfikowaniu i przeanalizowaniu mechanizmu uszkodzeń, przyczyn uszkodzeń oraz ich skutków. W pierwszej kolejności określono komplementarny zakres analizy, gdzie stwierdzono granice obu systemów oraz zdefiniowano części składowe interfejsu. Następnie wskazano uszkodzenia, które mogą być niebezpieczne lub spowodować brak reakcji bezpiecznościowej systemu na zaistniały defekt. Stosując narzędzie FMEA zidentyfikowano wiarygodne rodzaje uszkodzeń każdego z zastosowanych elementów składowych. Rodzaje uszkodzeń, które uwzględniono podczas procesu projektowego i analizy, opisane są w Załączniku C normy PN-EN 50129 [6]. Tablice rodzajów uszkodzeń podzespołów sprzętowych podane w tym załączniku zostały opracowane na podstawie wieloletnich doświadczeń oraz na podstawie innych dokumentów normatywnych.
Analiza FMEA, jak i jej rozszerzona wersja o ocenę stanów krytycznych FMECA (ang. Failure Mode Effects and Criticality Analysis) pozwala na przeprowadzenie jakościowo-ilościowej analizy niezawodności, która ma na celu identyfikację zagrożeń, mających wpływ na poprawne działanie rozważanych systemów. Dla systemów zapewniających bezpieczne sterowanie ruchem nie można poddawać hierarchizacji krytyczności poszczególnych stanów. Analizę FMEA przeprowadzono zgodnie z diagramem sekwencji działań przedstawionych w normie PN-EN 60812 [7] (patrz rys. 2).
Na przykładzie wybranego projektu części sprzętowej powiązania pomiędzy nastawnicą komputerową ESTW L90 5 firmy Thales, a sygnalizacją przejazdową RBUT-PL kategorii A firmy Zelisko zostanie przedstawiony sposób zastosowania techniki FMEA.
Na wstępie zidentyfikowano zagrożenia, w tym celu przeprowadzono analizę zagrożeń metodą analizy zagrożeń i zdolności operacyjnych (ang. Hazard and Operability Study - HAZOP).

Metoda ta pozwoliła zidentyfikować zagrożenia globalne dla powiązywanych systemów, w tym przypadku:

- przedwczesne włączenie ostrzegania na przejeździe,
- przejazd pociągu przez skrzyżowanie kolejowo-drogowe przy otwartych rogatkach.



Rys. 2 Diagram analizy, źródło: [7]

Wyspecyfikowano zdarzenia uznane za zagrożenia ze strony części sprzętowej powiązania, które mogą stanowić bezpośrednie lub pośrednie przyczyny prowadzące do wyżej opisanych zagrożeń:

- Błędna informacja o stanie urządzeń powiązanych wysyłana do komputera zależnościowego, która umożliwi realizację jazdy pociągu z prędkością wyższą niż dopuszczalna (potwierdzenie zamknięcia przejazdu).

Następnie uzupełniono przygotowany arkusz FMEA, w którym należy:

- określić podzespoły sprzętowe podlegające analizie (wszystkie elementy pomiędzy dwoma niezależnymi systemami),
- określić rodzaje uszkodzeń danego elementu, w przypadku zidentyfikowania nowego rodzaju uszkodzenia nieuwzględnionego w normie, ale potraktowanego jako wiarygodne, należy również je uwzględnić,
- zdefiniować skutki danego uszkodzenia oraz wpływ komponentów na pozostałe elementy interfejsu oraz na powiązywane systemy,
- określić sposób detekcji danego uszkodzenia (przy braku detekcji należy założyć stałe wystąpienie danego defektu),
- sklasyfikować poziom zagrożenia dla danego rodzaju uszkodzenia, zgodnie z Tabelą 1,
- ocenić ryzyko dla uszkodzeń o innym poziomie ryzyka niż C,
- wdrożyć środki zapobiegawcze w celu mitygacji zagrożeń (np. zmiany w projekcie, dodatkowe instrukcje/obostrzenia dla użytkownika),
- zidentyfikować i wyspecyfikować dodatkowe testy kwalifikacji bezpieczeństwa w przypadku konieczności określenia reakcji systemu przy ustalonym scenariuszu zdarzeń.

Tabela 1. Poziomy zagrożeń wraz z opisem

POZIOM ZAGROŻENIA	OPIS
A1	Uszkodzenie pojedyncze może prowadzić do zagrożenia.
A2	Uszkodzenia wielokrotne wywołane wspólną przyczyną mogą prowadzić do zagrożenia.
B1	Uszkodzenie jest niewykrywane, ale nie prowadzi bezpośrednio do zagrożenia. Możliwe jest powstanie zagrożenia przy drugim niezależnym uszkodzeniu.
B2	Uszkodzenie jest niewykrywane, ale nie prowadzi bezpośrednio do zagrożenia. Możliwe jest powstanie zagrożenia przy wielu niezależnych uszkodzeniach.
B3	Uszkodzenie jest wykrywane, ale nie prowadzi bezpośrednio do zagrożenia. Możliwe jest powstanie zagrożenia przy drugim niezależnym uszkodzeniu.
B4	Uszkodzenie jest wykrywane, ale nie prowadzi bezpośrednio do zagrożenia. Możliwe jest powstanie zagrożenia przy wielu niezależnych uszkodzeniach.
C	Uszkodzenie nie stwarza zagrożenia.

Analiza dla przykładowego projektu została przeprowadzona zgodnie z powyższym opisem, a wybrany fragment arkusza FMEA znajduje się w Tabeli 2. Przegląd wszystkich skutków uszkodzeń, zawartych w arkuszu FMEA, pokazuje, że we wszystkich przypadkach występuje odpowiednia reakcja systemu na uszkodzenie.

Tabela 2. Fragment arkusza FMEA dla projektu powiązania

L.p.	Nazwa elementu	Rodzaj uszkodzenia	Skutek uszkodzenia	Detekcja uszkodzenia	Komentarz	Odniesienie	Poziom zagrożenia
1	2	3	4	5	6	7	8
1	Dioda Z1	Przerwa	W stanie S1 - brak wysterowania wejścia E1	Błąd na interfejsie do urządzeń przejazdowych (niedozwolona kombinacja wejść).	obciążalność wyjścia karty systemu RBUT wynosi około 150mA, skutkiem czego zwarcie nie wyzwoli zabezpieczeń nadprądowych		C
2		Zwarcie	W stanie innym niż S1 - zwarcie pomiędzy zaciskami 91 a 92 karty systemu RBUT spowodowane przez diodę prostowniczą na karcie ESTW.	System RBUT wykryje brak różnicy potencjałów pomiędzy oboma zaciskami wyjścia, co zostanie zdiagnozowane jako usterka kat. 1			C
3		Zwiększenie prądu wstecznego	W stanie innym niż S1 - może spowodować uszkodzenie diody a w następstwie może spowodować zwarcie pomiędzy zaciskami 91 a 92 karty systemu RBUT.	System RBUT wykryje brak różnicy potencjałów pomiędzy oboma zaciskami wyjścia, co zostanie zdiagnozowane jako usterka kat. 1			C
4		Zmniejszenie wstecznego napięcia przebicia	W stanie innym niż S1 - może spowodować uszkodzenie diody a w następstwie może spowodować zwarcie pomiędzy zaciskami 91 a 92 karty systemu RBUT.	System RBUT wykryje brak różnicy potencjałów pomiędzy oboma zaciskami wyjścia, co zostanie zdiagnozowane jako usterka kat. 1			C

5. Podsumowanie

W wyniku analizy FMEA i klasyfikacji skutków uszkodzeń zidentyfikowano poszczególne poziomy zagrożeń na poziomie C. Zatem analizowane uszkodzenia nie prowadzą bezpośrednio do zagrożenia (albo prawdopodobieństwo ich wystąpienia jest akceptowalnie małe) bezpieczeństwa ruchu kolejowego, co jest zgodne z wymaganiami dla projektowania urządzeń srk.

Raport z analizy FMEA i jego wyniki służą w procesie wspólnej metody oceny bezpieczeństwa w zakresie wyceny i oceny ryzyka (ang. Common Safety Method on Risk Evaluation and Assessment - CSM-REA) do wykazania mitygacji zagrożeń dla projektu części sprzętowej powiązania zgodnie z Rozporządzeniem 402/2013 [8]. Powyższy raport jest uwzględniony w Raporcie bezpieczeństwa technicznego, który jest częścią Dowodu bezpieczeństwa określonego zastosowania opisanego w normie PN-EN 50129 [6].

Raport z analizy potwierdza, że system pozostaje bezpieczny w przypadku jakiegokolwiek rodzaju pojedynczego defektu losowego, który jest rozważany jako możliwy. Użycie metody FMEA pozwala na potwierdzenie, że żaden pojedynczy, losowy rodzaj uszkodzenia podzespołu sprzętowego nie jest niebezpieczny, bez względu jaki sposób lub kombinacja sposobów fail-safe została przyjęta.

6. Literatura

[1] Ericson C.: Hazard analysis techniques for system safety, A John Wiley & Sons, INC., Publication
[2] Materiały firmy Thales
[3] Materiały firmy Zelisko
[4] Norma PN-EN 50126 Zastosowania kolejowe. Specyfikacja niezawodności, dostępności podatności utrzymaniowej i bezpieczeństwa
[5] Norma PN-EN 50128 Zastosowania kolejowe. Systemy łączności, przetwarzania danych i sterowania ruchem. Oprogramowanie kolejowych systemów sterowania i zabezpieczenia
[6] Norma PN-EN 50129:2007 Zastosowania kolejowe. Systemy łączności, przetwarzania danych i sterowania ruchem. Elektroniczne systemy sterowania ruchem związane z bezpieczeństwem
[7] Norma PN-EN 60812:2009 Techniki analizy nieuszkadzalności systemów Procedura analizy rodzajów i skutków uszkodzeń (FMEA)

[8] Rozporządzenie Wykonawcze Komisji (UE) NR 402/2013 z dnia 30 kwietnia 2013 r. w sprawie wspólnej metody oceny bezpieczeństwa w zakresie wyceny i oceny ryzyka i uchylające rozporządzenie (WE) nr 352/2009
[9] Szopa T.: Niezawodność i bezpieczeństwo, Oficyna Wydawnicza Politechniki Warszawskiej, Warszawa 2009
[10] Ważyńska-Fiok K.: Podstawy teorii eksploatacji i niezawodności systemów transportowych, Wydawnictwa Politechniki Warszawskiej, Warszawa 1993.

Mgr inż. Dariusz Szmel. *W 2005 roku ukończył Politechnikę Śląską w Katowicach, Wydział Transportu, Katedra Transportu Szynowego. Od 2006 roku pracuje w firmie Thales Polska sp. z o.o. W firmie jest odpowiedzialny za zarządzanie bezpieczeństwem oraz jakością. W roku 2013 był członkiem Rady ds. Certyfikacji przy Instytucie Kolejnictwa. W 2016 roku został powołany do Komitetu chroniącego bezstronność Ośrodka Certyfikacji Transportu na Wydziale Transportu Politechniki Warszawskiej (Udział 60%).*

Inż. Dominik Wawrzyniak*. W 2013 ukończył studia inżynierskie na Politechnice Warszawskiej, kierunek Transport, specjalizacja sterowanie ruchem kolejowym. Praktykę dyplomową realizował w Metrze Warszawskim – w dziale automatyki i łączności. Od 2013 roku pracuje w firmie Thales Polska sp. z o.o. na stanowisku specjalisty ds. RAMS. W 2016 ukończył specjalistyczne szkolenie w Centrum Szkoleniowym w Stuttgarcie (Udział 40%).*