P R A C E N A U K O W E P O L I T E C H N I K I W A R S Z A W S K I E J
z. 127 Transport 2019

Dariusz Szmel, Wiesław Zabłocki†, Przemysław Ilczuk, Andrzej Kochan
Politechnika Warszawska, Wydział Transportu

WYBRANE ZAGADNIENIA OCENY RYZYKA W ODNIESIENIU DO SYSTEMÓW STEROWANIA RUCHEM KOLEJOWYM

Rękopis dostarczono, październik 2019

Streszczenie: W artykule przedstawiono wybrane metody oceny i analizy ryzyka systemów sterowania ruchem kolejowym w odniesieniu do poziomu całego systemu kolejowego. Rozpatrywane są wybrane metody stosowane na początkowym etapie tworzenia wymagań bezpieczeństwa i odnoszące się do wstępnej definicji systemu określonej na dużym poziomie abstrakcji. Dyskutowane są także kwestie zastosowania podejścia holistycznego i zarządzania ryzykiem szczątkowym. Przedstawiono modele ryzyka oraz poszczególne kroki analizy, wyceny i oceny ryzyka obejmujące m.in. identyfikację zagrożeń, analizę skutków oraz wybór zasady akceptacji ryzyka. Kluczowym aspektem podjętym w artykule jest propozycja wyznaczania ilościowych celów bezpieczeństwa opartych o wskaźnik THR, jako istotnego parametru w dalszych analizach systemu w szczególności w zastosowaniach komputerowych. W rozważaniach uwzględniono aktualne podstawy normatywne oraz przepisy prawa regulujące obszar oceny ryzyka na kolei w tym dyrektywy i rozporządzenia dotyczące interoperacyjności i bezpieczeństwa.

Słowa kluczowe: analiza ryzyka, ocena ryzyka, THR

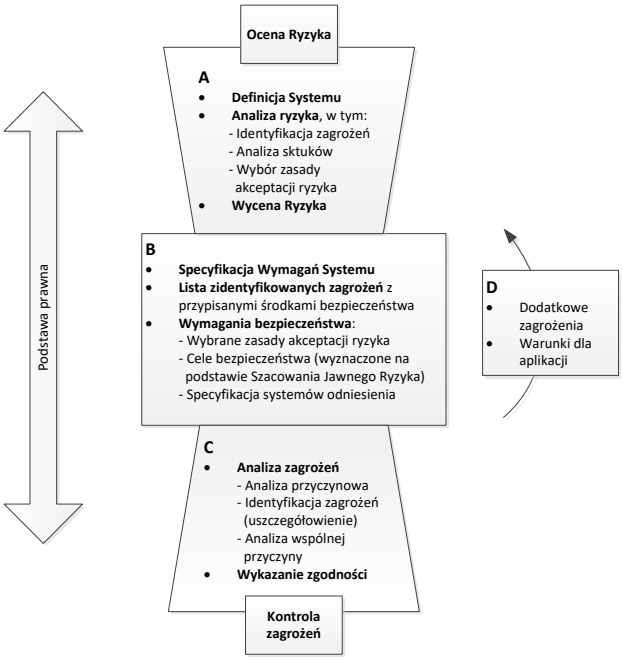
1. WSTĘP

Najbardziej zawodnym elementem niemal każdego systemu, w tym systemów sterowania ruchem kolejowym, jest człowiek. Nie chodzi jednak tylko o człowieka jako użytkownika urządzeń technicznych, ale bardziej o wpływ czynnika ludzkiego na etapie projektowania i wytwarzania urządzeń. Systemy sterowania ruchem stają się coraz bardziej złożone i skomplikowane, a głównym celem przy projektowaniu jest jak największa automatyzacja pracy w celu eliminacji błędów ludzkich w trakcie procesu sterowania. Dlatego też istotna grupa problemów bezpieczeństwa to problemy techniczne. Z powodu dużej różnorodności urządzeń i systemów problemy te mogą się od siebie istotnie różnić. Problemy te rozwiązywane są przez inżynierów głównie w fazie projektowania. Tak więc to na inżynierach spoczywa odpowiedzialność prawna i moralna za bezpieczeństwo przyszłych użytkowników projektowanych urządzeń. Inżynierowie projektują i także nadzorują procesy produkcji tych urządzeń w celu utrzymania założonego, wymaganego przepisami poziomu bezpieczeństwa [1]. Właśnie określenie oczekiwanego poziomu bezpieczeństwa jest szczególnie trudne i wiąże się z problemem społecznej akceptowalności ryzyka. W celu określenia poziomu bezpieczeństwa wykorzystujemy pojęcie ryzyka, które jest nieodłącznie związane z losowością

zjawisk i zdarzeń zachodzących w otaczającym nas świecie. W strategii zarządzania bezpieczeństwem proces oceny ryzyka jest kluczowym elementem. W artykule autorzy skupili się na początkowym etapie procesu oceny ryzyka, zaczynając od definiowania systemu, a kończąc na określeniu wymagań bezpieczeństwa. Proces oceny ryzyka dla systemu kolejowego został określony w rozporządzeniu wykonawczym 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 [2]. Jeżeli ocena ryzyka jest wymagana w odpowiednich technicznych specyfikacjach interoperacyjności (TSI), w takim przypadku TSI określają, w razie potrzeby, które elementy niniejszego rozporządzenia mają zastosowanie i tak w przypadku systemu sterowania ruchem kolejowym rozporządzenie Komisji (UE) 2016/919 z dnia 27 maja 2016 r. w sprawie technicznej specyfikacji interoperacyjności w zakresie podsystemów „Sterowanie" systemu kolei w Unii Europejskiej wskazuje w tym zakresie stosowanie norm CENELEC [3], [4].
Publikacja powstała w trakcie badań w zakresie działalności statutowej i innych programów badawczych.

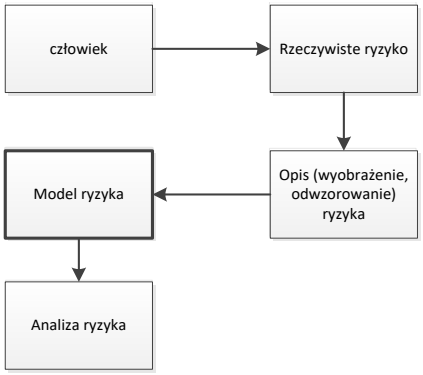
2. PROCES OCENY RYZYKA

Proces oceny ryzyka jest całościowym, wieloetapowym procesem obejmującym: zdefiniowanie systemu, identyfikację zagrożeń, szacowanie ryzyka oraz wycenę ryzyka. Proces oceny ryzyka jest powiązany z zarządzaniem zagrożeniami poprzez rejestr zagrożeń. Definicja systemu powinna m.in. określać cel systemu, funkcje i elementy systemu, jego granicę, interfejsy oraz otoczenie systemu. Po przeprowadzeniu procesu identyfikacji zagrożeń określa się dopuszczalność ryzyka z wykorzystaniem następujących zasad akceptacji ryzyka: stosowanie kodeksów postępowania, porównanie z podobnymi systemami i szacowanie jawnego ryzyka [2]. Na etapie wyceny ryzyka należy wykazać, że zasada akceptacji ryzyka została odpowiednio zastosowana. Zastosowanie tych zasad akceptacji ryzyka pozwoli zidentyfikować możliwe środki bezpieczeństwa, które sprawią, że ryzyko dotyczące ocenianego systemu stanie się dopuszczalne. Spośród zidentyfikowanych w ten sposób środków bezpieczeństwa zostaną wybrane środki służące do nadzoru ryzyka, które staną się wymogami bezpieczeństwa, jakie powinien spełniać system [2]. Cały powyższy proces powinien zostać udokumentowany w rejestrze zagrożeń, który oznacza dokument, w którym rejestruje się i opisuje zidentyfikowane zagrożenia, związane z nimi środki i źródła zagrożeń oraz wskazuje organizację, która ma nimi zarządzać. W nowej wersji normy PN-EN 50126 [3] oraz w rozporządzeniu [2] opis procesu oceny ryzyka jest zbliżony i różni się głównie poziomem szczegółowości na etapie implementacji. W normie [3] przedstawiono uproszczony model obrazujący działania związane z bezpieczeństwem, który określono jako model Hourglass i jego założeniem było oddzielenie procesu analizy ryzyka, stanowiącego część oceny ryzyka na etapie koncepcji systemu, od analizy zagrożeń, stanowiącego część procesu kontroli zagrożeń na etapie wdrożenia systemu.



Rys. 1. Model Hourglass
Źródło: opracowanie własne na podstawie [3]

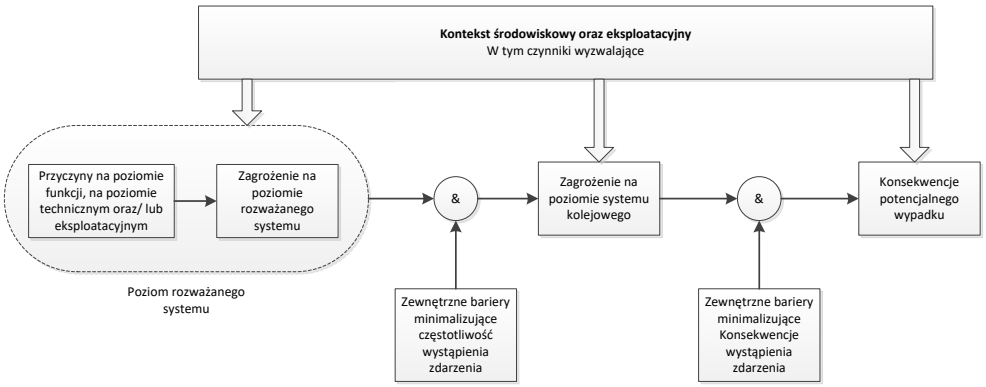
W rozważaniach oraz analizach w obszarze systemów bezpiecznych posługuje się pojęciem modelu ryzyka. Wynika to z braku pełnej wiedzy i możliwości w określeniu rzeczywistego ryzyka. Zatem analizę ryzyka musi poprzedzać opracowanie modelu ryzyka. Obrazuje to poniższy rysunek 2.



Rys. 2. Pojęcie modelu ryzyka
Źródło: opracowanie własne na podstawie [1]

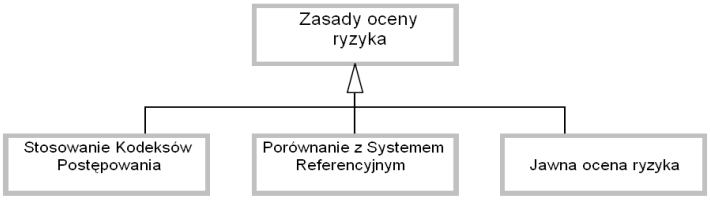
Model ryzyka przyjęty w [2] przedstawia relacje pomiędzy przyczynami, zagrożeniami oraz wypadkami i ich konsekwencjami. W szczególności przyjmuje się, że: pojedyncza przyczyna może prowadzić do kilku zagrożeń, zagrożenie może w konsekwencji prowadzić do różnego rodzaju wypadków w różnym kontekście, w zakresie procesu eksploatacji oraz parametrów środowiskowych i oczywiście wypadek może mieć różne skutki. Przykład modelu ryzyka przedstawiono na rys. 3. Określa on jak zagrożenie na poziomie rozważanego

podsystemu lub systemu, w wyniku czynników eksploatacyjnych lub technicznych, może przenieść się na poziom systemu kolejowego, z możliwością doprowadzenia do wypadku biorąc pod uwagę zdarzenia wyzwalające oraz dostępność zewnętrznych barier.



Rys. 3. Przykład modelu ryzyka
Źródło: opracowanie własne na podstawie [2]

Jednym z kluczowych i trudnych etapów analizy ryzyka jest identyfikacja zagrożeń. Proces identyfikacji jest ciągły i należy go przeprowadzać regularnie w całym cyklu życia systemu. W niniejszym rozważaniu opisywany jest proces identyfikacji zagrożeń na początkowym etapie realizacji systemu. W pierwszym kroku dokonuje się wyboru fragmentów systemu, w których może wystąpić zdarzenie niepożądane oraz określa się przyczyny tych zdarzeń i ich skutki. W tym zadaniu stosuje się wiele metod wpierających identyfikację zagrożeń. Jako najbardziej rozpowszechnione to metody FMECA i HAZOP, szczegółowo opisane w [5] i [6]. Wskazane jest również wcześniejsze ustanowienie zasad i kryteriów identyfikacji zagrożeń. Do uzupełnienia modelu ryzyka konieczna jest także informacja o skutkach wystąpienia potencjalnego wypadku. W tym celu stosuje się metody indukcyjne i dedukcyjne lub ich kombinację m.in. wymienione powyżej oraz takie metody jak ETA i FTA, szczegółowo opisane w [7] oraz [8]. Powyższe działania przygotowują informację niezbędną do klasyfikacji zagrożeń i szacowania ryzyka. W celu przeprowadzenia wyceny ryzyka niezbędne jest określenie kryteriów akceptacji ryzyka. Każda analiza rozpoczyna się podejściem jakościowym, a następnie ilościowym. Jednak oszacowanie ryzyka w sposób matematyczny nie zawsze jest możliwe. W [1], [2] przyjęto trzy kryteria akceptacji ryzyka: zastosowanie kodeksów postępowania, porównanie z systemem referencyjnym oraz szacowanie jawnego ryzyka (rys. 4). Takie podejście zapewnia całościowe spojrzenie na system, a nie tylko na część, którą można ocenić ilościowo.



Rys. 4. Zasady akceptacji ryzyka
Źródło: opracowanie własne

Propozycje szacowania jawnego ryzyka przedstawiono w kolejnych rozdziałach niniejszej publikacji. Poprzez zastosowanie kodeksu postępowania lub porównanie z systemem referencyjnym można kontrolować zagrożenia. Kodeksem postępowania mogą być zasady uznane i stosowane dotychczas w środowisku kolejowym (np. norma PN-EN 50159 [4], albumy schematów kolejowych). Można zastosować nowe zasady, ale muszą one spełniać wymagania podane w rozporządzeniu [2] oraz uzasadnioną argumentację ich zastosowania. Porównanie z systemem referencyjnym polega na zastosowaniu środków bezpieczeństwa sprawdzonych już w systemie, który ma akceptację bezpieczeństwa i jest w eksploatacji. W kwestii ryzyka szczątkowego istotne znaczenia ma proces zarządzania warunkami bezpiecznego zastosowania aplikacji SRAC (ang. *Safety Related Application Conditions*).

2. WYBRANE METODY OKREŚLANIA KRYTERIÓW AKCEPTACJI JAWNEGO RYZYKA

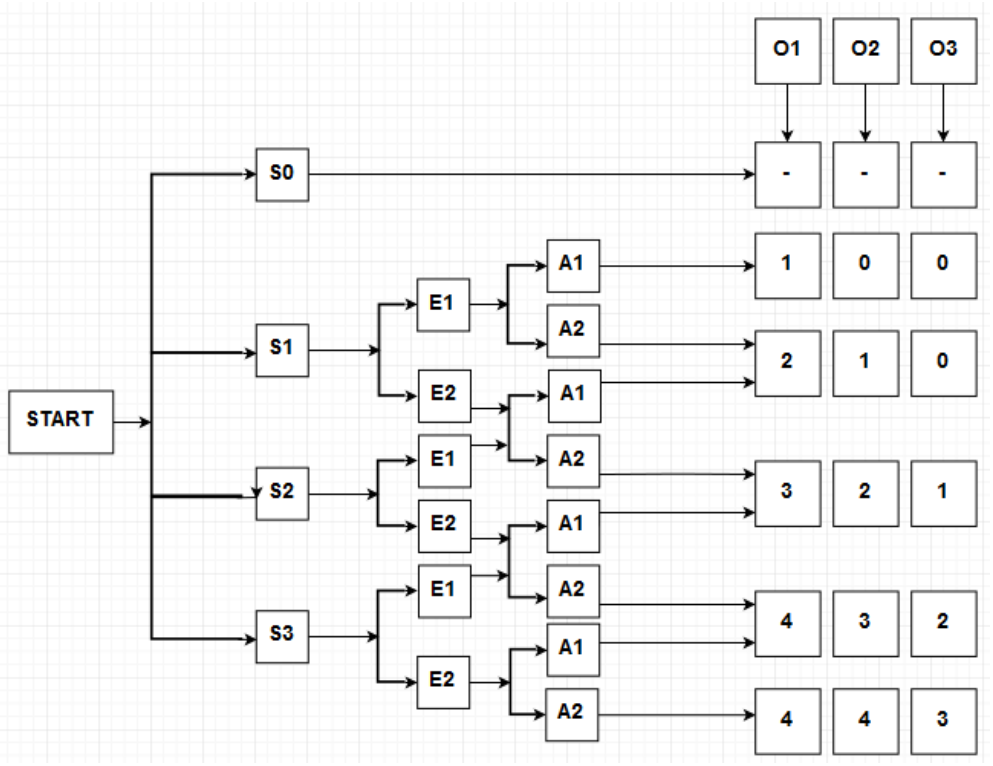
W celu zastosowania szacowania jawnego ryzyka jako zasady akceptacji ryzyka konieczne jest określenie akceptowalnego poziomu ryzyka. Szacowanie jawnego ryzyka jest możliwe poprzez określenie częstotliwości wystąpienia zagrożenia oraz jego wagi. Częstotliwość i powagę można określić ilościowo lub jakościowo (np. przez metody matrycowe lub wskaźnikowe). Dla potrzeb systemów technicznych, biorąc pod uwagę częstotliwość oraz powagę zagrożenia wyznacza się cel bezpieczeństwa w postaci parametru THR (ang. *Tolerable Hazard Rate*), który determinuje określenie poziomu SIL (ang. *Safety Integrity Level*). W niniejszym rozdziale opisano metodę grafu ryzyka, wraz z wyliczeniem indywidualnego ryzyka śmierci *IRF* (ang. *Individual Risk of Fatality*), rekomendowaną przez standard [9] oraz metodę FMEA jako metodę stosowaną przez PKP PLK S.A.

Metoda grafu ryzyka zgodnie z zaleceniami normy IEC 61508 [9] oraz także normy PN-EN 50126 [3] umożliwia szacowanie ryzyka oraz wyznaczenie wymaganego poziomu nienaruszalności bezpieczeństwa (z ang. *safety integrity level targets*) lub też poziomu THR wykorzystując następujące elementy ryzyka

$$SIL = f(S; E; A; O) \tag{1}$$

gdzie:

SIL – poziom nienaruszalności bezpieczeństwa (z ang. *safety integrity level targets*)
S – potencjalne skutki zdarzenia
E – ekspozycja (czas / częstość narażenia na zdarzenie)
A – możliwość uniknięcia lub ograniczenia szkód
O – prawdopodobieństwo wystąpienia zdarzenia



Rys. 5. Graf ryzyka
Źródło: opracowanie własne na podstawie [9]

Graf ryzyka jest często wykorzystywany w transporcie kolejowym. Metoda jest łatwa w użyciu oraz uwzględnia kilka parametrów w wyznaczaniu poziomu ryzyka. Wymaga jednak dostosowania do odpowiedniej aplikacji.
Metoda ilościowa polegająca na wyliczeniu indywidualnego ryzyka śmierci *IRF* (ang. *Individual Risk of Fatality*) przedstawiona jest zależnością:

$$IRF_i = N_i \times \Sigma\{(HR_j \times D_j + HR_j \times E_{ij}) \times \Sigma(C_{jk} \times F_{ik})\} \tag{2}$$

gdzie:
N_i – częstotliwość użytkowania *i*-tego systemu (na godzinę lub na rok),
E_{ij} – czas narażenia *i*-tego systemu na *j*-te zagrożenie (wyrażony w godzinach np. czas trwania podróży),
HR_j – intensywność występowania j-tego zagrożenia wyrażona jako liczba j-tych zagrożeń na godzinę,
D_j – czas trwania j-tego zagrożenia
C_{jk} – prawdopodobieństwo wystąpienia k-tego wypadku jako konsekwencja j-tego zagrożenia
F_{ik} – powaga wypadku określona jako prawdopodobieństwo śmierci jednej osoby w wyniku *k*-tego wypadku w *i*-tym systemie.

Celem bezpieczeństwa dla systemu w powyższym wyrażeniu będzie intensywność zagrożeń HR. Można ją wyznaczyć przyjmując wartość *IRF* oraz odpowiednio przekształcając

wyrażenie. Wyznaczenie pozostałych danych należy wykonać stosując metody identyfikacji zagrożeń (np. HAZOP) oraz analizy konsekwencji (np. ETA). Wyznaczony HR stanowi THR (ang. *Tolerable Hazard Rate* – Tolerowany Wskaźnik Intensywności Zagrożeń) dla danego systemu.

Metodą stosowaną przez PKP PLK S.A. jest metoda oparta o analizę FMEA oraz RPN (ang. *Risk Priority Number*). Metodę tę reguluje procedura Oceny ryzyka technicznego i operacyjnego [11]. Do wyceny ryzyka stosuje się metodę FMEA (ang. Failure Mode and Effect Analysis – analiza przyczyn i skutków wad) i dokonuje się jej poprzez określenie, dla każdego zagrożenia ujętego w Rejestrze zagrożeń, liczby ryzyka „R" przyjmującej wartość całkowitą od 1 do 1000. Liczbę ryzyka „R" określa się jako iloczyn trzech czynników: „P", „W" i „S":

P – częstotliwość wystąpienia zdarzenia wynikającego z danego zagrożenia. Liczba „P" przyjmuje wartość całkowitą od 1 do 10;

W – prawdopodobieństwo wykrycia zagrożenia przy dotychczas stosowanych środkach kontroli ryzyka. Liczba „W" przyjmuje wartość całkowitą od 1 do 10;

S – liczby określającej wartość skutków przypadających na zdarzenie a w przypadku wystąpienia w poddanym ocenie okresie więcej niż jednego zdarzenia wartość średnią dla skutków wynikających z danego zagrożenia. Liczba „S" przyjmuje wartość całkowitą od 1 do 10;

$$R = P \times W \times S \tag{3}$$

Dla każdego z czynników przyjęto kryteria oparte o wartości ilościowe i jakościowe. Liczba ryzyka R przyjmuje zakres wartości dla następujących poziomów ryzyka: dopuszczalne, tolerowalne oraz nieakceptowalne.

4. PRZYKŁAD WYZNACZANIA PARAMETRÓW ILOŚCIOWYCH DLA URZĄDZEŃ TECHNICZNYCH ZA POMOCĄ GRAFU RYZYKA

Analiza ryzyka z wykorzystaniem metody grafu ryzyka zastosowana została dla Systemu Wymiany Informacji (SWI) pomiędzy dyżurnym ruchu i dróżnikiem przejazdu kolejowego. Metodę przeprowadzono w celu wyznaczenia wymaganej wartości parametrów THR oraz SIL dla poszczególnych funkcji systemu i w celu weryfikacji parametru SIL4 (ang. *Safety Integrity Level* – Poziom Nienaruszalności Bezpieczeństwa poziomu 4) narzuconego przez Zarządcę Kolejowego na cały system SWI. W pierwszym etapie analizy przeprowadzono analizę instrukcji kolejowych regulujących wymagania dla systemu SWI oraz przeprowadzono analizę funkcjonalną. W wyniku analizy funkcjonalnej wyznaczono funkcje systemu dla której przypisano numer identyfikacyjny i wstępnie określono przepływ informacji wymaganych w ramach realizacji funkcji.

Tab. 1

Przykład funkcji systemu SWI

F1	Powiadomienie dróżnika przejazdowego o wyprawieniu pociągu na szlak	Inf_1	Wysłanie powiadomienia o wyprawieniu pociągu na szlak
		Inf_10	Wysłanie potwierdzenia otrzymania powiadomienia o wyprawieniu pociągu na szlak
		Inf_12	Potwierdzenie zamknięcia przejazdu dla pociągu
		Inf_23	Potwierdzenie przejazdu pociągu

Na podstawie wyznaczonych funkcji opracowano wymagania systemowe oraz przeprowadzono analizę HAZOP (ang. Hazard and Operability study) z zastosowaniem słów kluczowych przedstawionych w tab. 2.

Tab. 2

Słowa kluczowe zastosowane w analizie HAZOP

Utrata funkcji/ *Loss of function*
Nadmiarowa funkcja/ *Excess of function*
Funkcja realizowana odwrotnie od zamierzonego działania/ *Inverse of intended function*
Funkcja realizowana zbyt wcześnie/ *Function done too early*
Funkcja realizowana zbyt późno/ *Function done too late*
Funkcja realizowana inaczej niż założone działanie/ *Other than intended function*

W wyniku analizy HAZOP określono skutki nieprawidłowego zadziałania danej funkcji oraz przypisano zagrożenia, które zostały wcześniej zidentyfikowane w wyniku wstępnej analizy zagrożeń.

Kolejnym krokiem w analizie było zastosowanie grafu ryzyka z rys. 6 dla którego przyjęto następujące parametry:

START - warunki początkowe do analizy

1) Istnieje procedura dwukierunkowej komunikacji dyżurnego z dróżnikiem (obecnie realizowana w sposób analogowy, łączność telefoniczna) – patrz instrukcja Ir-1 i Ir-7
2) Nie ma uzależnienia pomiędzy urządzaniami srk stacyjnymi i szlakowymi z urządzeniami komunikacji dyżurny – dróżnik
3) System SWI nie może być gorszy od istniejącego systemu łączności

S – potencjalne skutki zdarzenia

S0 – zdarzenie nie wpływające na bezpieczeństwo
S1 – zdarzenie wpływające na bezpieczeństwo (brak ofiar śmiertelnych)
S2 – zdarzenie prowadzące do poważnego skutku (1 ofiara śmiertelna)

S3 – zdarzenie prowadzące do katastrofalnych skutków (więcej niż 1 ofiara śmiertelna)
E – ekspozycja (czas / częstość narażenia na zdarzenie)
E1 – możliwe narażenie na zdarzenie
E2 – częste narażenie na zdarzenie
A – możliwość uniknięcia lub ograniczenia szkód
Ze względów technicznych (wyposażenie systemu w istniejące techniczne środki bezpieczeństwa), ludzkich (umiejętności, świadomość, wiedza, predyspozycje psychofizyczne) i organizacyjnych.
A1 – możliwe unikniecie lub znaczne ograniczenie szkód
A2 – nie jest możliwe
O – prawdopodobieństwo wystąpienia zdarzenia
Historia zdarzeń wypadkowych dla takich samych lub podobnych systemów.
O1 - zdarzenie może występować często (częściej niż 1 raz / 10 lat: 1x10^-5)
O2 - zdarzenie może występować czasami podczas życia systemu
O3 - zdarzenie może wystąpić rzadko (rzadziej niż 1 raz / 20 lat; 5x10^-6).

Na podstawie powyższych danych opracowano raport z analizy ryzyka. Poniżej przedstawiono wyniki dla przykładowej funkcji.

Tab. 3

Przykładowy wynik analizy ryzyka

ID_SRS	**SRS_001**
Funkcja	Powiadomienie dróżnika przejazdowego o wyprawieniu pociągu na szlak
S - potencjalne skutki zdarzenia	W najgorszym przypadku awarii funkcji nie można poinformować o zaistniałej sytuacji innych użytkowników.
Poziom S	S3
E - ekspozycja	Procedury prowadzenia ruchu implikują częstą realizację funkcji
Poziom E	E2
A - możliwość uniknięcia lub ograniczenia szkód	W przypadku uszkodzenia/ awarii modułu komunikacyjnego SWI użytkownicy są zobligowani do korzystania z łączności strażnicowej (zgodnie z par.8 p.4 instrukcji Ie-113 [12])
Poziom A	A1
O - prawdopodobieństwo wystąpienia zdarzenia	Analizując raporty roczne PKBWK (lata 2011-16) [13], [14], [15], [16], [17] określono częstotliwość występowania sytuacji niebezpiecznych polegających na najechaniu pojazdu kolejowego na pojazd drogowy na przejazdach kolejowych kat. A wynosi 8 razy/ 7 lat, czyli ok. 1/rok
Poziom O	O1
Wyznaczony poziom SIL	4 (Na podstawie tabeli z normy [4] wyznaczono THR na poziomie $10^{-9} \geq THR \geq 10^{-8}$

Wyniki analizy dla wszystkich realizowanych przez system funkcji zostały przedstawione zarządcy infrastruktury, a następnie wspólnie przeprowadzono jej przegląd. W wyniku tego

działania zmniejszono wartość parametru „O" z uwagi na fakt, że system SWI tylko w części może się przyczynić do wypadków na przejazdach kolejowych polegających na najechaniu pojazdu kolejowego na pojazd drogowy. Ponadto w związku z wczesnym etapem analizy, gdzie zestaw urządzeń techniczny realizujący określone funkcje nie był jasno zdefiniowany i traktowany jak „czarna skrzynka", przyjęto zasadę z normy [3] określając: „worst possible scenario", „reasonable estimates", „reasonable worst case". Uwzględniono także zasadę wprowadzoną w [2], która stanowi, że ryzyko związane z systemami technicznymi, w przypadku których zachodzi wiarygodne prawdopodobieństwo katastroficznych konsekwencji w bezpośrednim wyniku awarii działania, nie musi być dalej redukowane, jeżeli częstotliwość takich awarii jest równa lub mniejsza niż 10^{-9} na godzinę pracy systemu. Na podstawie powyższych czynności przypisano wymagany poziom SIL oraz THR dla każdej funkcji systemu, zamiast jak to miało miejsce we wcześniejszych analizach prowadzonych przez zarządcę infrastruktury - dla systemu jako całości.

5. PODSUMOWANIE

W artykule przedstawiono ogólny opis procesu oceny ryzyka i w konsekwencji wyznaczania wymagań bezpieczeństwa. W szczególności przedstawiono sposoby realizacji jawnego szacowania ryzyka w oparciu o metody wskazywane w obowiązujących standardach oraz normach dedykowanych dla systemów sterowania ruchem kolejowym. Następnie przedstawiono przykładową realizację oceny ryzyka z wykorzystaniem grafu ryzyka dla jednego z systemów stosowanych w sterowaniu ruchem kolejowym. System został wybrany ze względu na stosunkowo krótki okres eksploatacji oraz ze względu na opracowane nowe wymagania przez Zarządcę Infrastruktury. Biorąc to pod uwagę przeprowadzenie oceny ryzyka było trudnym zadaniem. Zastosowanie grafu ryzyka pozwoliło efektywnie wyznaczyć cele bezpieczeństwa i spotkało się z pozytywną reakcją zarządcy infrastruktury. Metodę tę można stosować do klasyfikacji wymagań bezpieczeństwa. Dalszą część rozważań można ukierunkować na powiązanie wyników grafu ryzyka i wymagań bezpieczeństwa opartych o wskaźnik THR z wynikami analizy realizowanej w oparciu o procedurę FMEA i RPN.

Bibliografia

1. Szopa T., Niezawodność i bezpieczeństwo, Oficyna Wydawnicza Politechniki Warszawskiej, Warszawa 2009
2. 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
3. Norma PN-EN 50126:2018 Zastosowania kolejowe -- Specyfikacja niezawodności, dostępności, podatności utrzymaniowej i bezpieczeństwa
4. Norma PN-EN 50129:2007 Zastosowania kolejowe -- Systemy łączności, przetwarzania danych i sterowania ruchem -- Elektroniczne systemy sterowania ruchem związane z bezpieczeństwem
5. Norma PN-EN 60812:2009 Techniki analizy nieuszkadzalności systemów. Procedura analizy rodzajów i skutków uszkodzeń (FMEA)
6. Norma PN-EN 61882:2016-07 Badania zagrożeń i zdolności do działania (badania HAZOP). Przewodnik

zastosowań
7. Norma PN-EN 62502:2011 Techniki analizy niezawodności. Analiza drzewa zdarzeń (ETA)
8. Norma PN-EN 61025:2007 Analiza drzewa niezdatności (FTA)
9. Norma PN-EN 61508-1:2010 Bezpieczeństwo funkcjonalne elektrycznych / elektronicznych / programowalnych elektronicznych systemów związanych z bezpieczeństwem - Część 1: Wymagania ogólne
10. H. J. Jo, J. G. Hwang, Y. K. Kim, Risk assessment method for guaranteeing safety in the train control system, Urban Transport XIII: Urban Transport and the Environment in the 21st Century 567
11. SMS/MMS-PR-02 Ocena Ryzyka technicznego i operacyjnego – procedura PKP PLK S.A
12. PKP PLK S.A., Ie-113, Wymagania na system wymiany informacji pomiędzy pracownikami posterunków ruchu biorącymi udział w obsłudze przejazdu kolejowo-drogowego i pracownikiem obsługi przejazdu kolejowo-drogowego, Warszawa 2015
13. Państwowa Komisja Badania Wypadków Kolejowych Ministerstwo Infrastruktury i Budownictwa, Raport roczny za rok 2016 z działalności Państwowej Komisji Badania Wypadków Kolejowych (Załącznik do obwieszczenia Ministra Infrastruktury i Budownictwa z dnia 4 paź. 2017 r. (poz. 68))
14. Państwowa Komisja Badania Wypadków Kolejowych Ministerstwo Infrastruktury i Rozwoju, Raport roczny za rok 2014 z działalności Państwowej Komisji Badania Wypadków Kolejowych (Załącznik do obwieszczenia Ministra Infrastruktury i Rozwoju z 30 września 2015 r. (poz. 51))
15. Państwowa Komisja Badania Wypadków Kolejowych Ministerstwo Infrastruktury i Rozwoju, Raport roczny za rok 2013 z działalności Państwowej Komisji Badania Wypadków Kolejowych (Załącznik do obwieszczenia Ministra Infrastruktury i Rozwoju z dnia 28 września 2014 r. (poz. 79))
16. Państwowa Komisja Badania Wypadków Kolejowych Ministerstwo Transportu, Budownictwa i Gospodarki Morskiej, Raport roczny za rok 2012 z działalności Państwowej Komisji Badania Wypadków Kolejowych (Załącznik do obwieszczenia Ministra Transportu, Budownictwa i Gospodarki Morskiej z dnia 9 października 2013 r. (poz. 61))
17. Państwowa Komisja Badania Wypadków Kolejowych Ministerstwo Transportu, Budownictwa i Gospodarki Morskiej, Raport roczny za rok 2011 z działalności Państwowej Komisji Badania Wypadków Kolejowych (Załącznik do obwieszczenia Ministra Transportu, Budownictwa i Gospodarki Morskiej z dnia 6 września 2012 r. (poz. 64))

SELECTED ISSUES OF RISK ASSESSMENT IN RELATION TO RAILWAY SIGNALLING SYSTEMS

Summary: In the article the selected methods of the risk assessment and analysis of signalling railway systems in reference to the whole railway system were introduced. The selected methods applied at the very first stage of safety requirements definition within the preliminary system definition described at high level of abstraction will be considered. It will be discussed the application of holistic approach with management of residual risk. The risk models will be presented as well as steps of the assessment, analysis and evaluation of risk including hazard identification, consequences analysis and selection of risk acceptance principles. Key aspect in the article will be the determination of quantitative safety targets based on THR indicator as an important parameter for further hazard analysis of the system in particular in computer application. Normative and legislation requirements in scope of risk assessment for the railway system will be taken into consideration including the interoperability and safety directives and decrees regulations

Keywords: risk analysis, risk assessment, THR