Bezpieczeństwo i ryzyko na przykładzie urządzeń sterowania ruchem kolejowym

Andrzej BIAŁOŃ[1], Marek PAWLIK[2]

Streszczenie
Artykuł opisuje zasady oceny bezpieczeństwa stosowane w transporcie kolejowym na przykładzie oceny bezpieczeństwa urządzeń sterowania ruchem kolejowym. Analizie poddano metody opisane w normach europejskich oraz rozporządzeniach Komisji Europejskiej. Wskazano różne metody oceny bezpieczeństwa oraz opisano i porównano szacowanie bezpieczeństwa dla oceny kwalitatywnej i dla oceny kwantytatywnej. Na przykładzie urządzeń sterowania ruchem kolejowym opisano usterki i zagrożenia, do których mogą one prowadzić. Zgodnie z prawem wspólnotowym, ryzyko określono jako łączny wynik skali zagrożenia i prawdopodobieństwa wystąpienia (częstotliwości występowania danego zagrożenia). Pokazano jak tworzone są listy zagrożeń i jak szacowane jest ryzyko dla poszczególnych zagrożeń, które jest następnie porównywane z kryteriami akceptowalności ryzyka i uwzględniane w systemie zarządzania bezpieczeństwem zarządców infrastruktury i przewoźników kolejowych.
Słowa kluczowe: bezpieczeństwo, ryzyko, zagrożenia

1. Wprowadzenie

Analiza ryzyka jest niezwykle istotnym elementem przy projektowaniu, produkcji i eksploatacji urządzeń technicznych. Zapisy, pojawiające się w niektórych normach dotyczących urządzeń srk (sterowania ruchem kolejowym), szczególnie związanych z bezpieczeństwem, nakładają wręcz na zespoły projektujące i produkujące urządzenia obowiązek przeprowadzania analizy ryzyka. Można to pokazać na przykładzie normy PN-EN 50126 [3], w której pokazany jest cykl życia systemu (np. urządzeń srk). Analiza ryzyka jest tu, jak pokazano na rysunku 1, niezbędnym i istotnym elementem cyklu życia systemu.

Również w analizie bezpieczeństwa, niezbędnej do opracowania dowodu bezpieczeństwa, przeprowadzanej zgodnie z normą PN-EN 50129 [5], jednym z ważnych składników tej analizy jest analiza ryzyka. W odniesieniu do systemów programowalnych, a takimi są nowoczesne systemy sterowania ruchem kolejowym

[1] Dr inż., Instytut Kolejnictwa, e-mail:abialon@ikolej.pl, wkład merytoryczny autora 50%.
[2] Dr inż., Instytut Kolejnictwa, e-mail: mpawlik@ikolej.pl, wkład merytoryczny autora 50%.

(systemy srk), w analizie ryzyka często wykorzystuje się metodologię zdefiniowaną w normie PN-EN 50128 [4]. Analiza ryzyka i ryzyko są nierozerwalnie połączone z bezpieczeństwem systemu, dlatego też są jednym z istotnych elementów przy podejmowaniu decyzji o stosowaniu systemu.

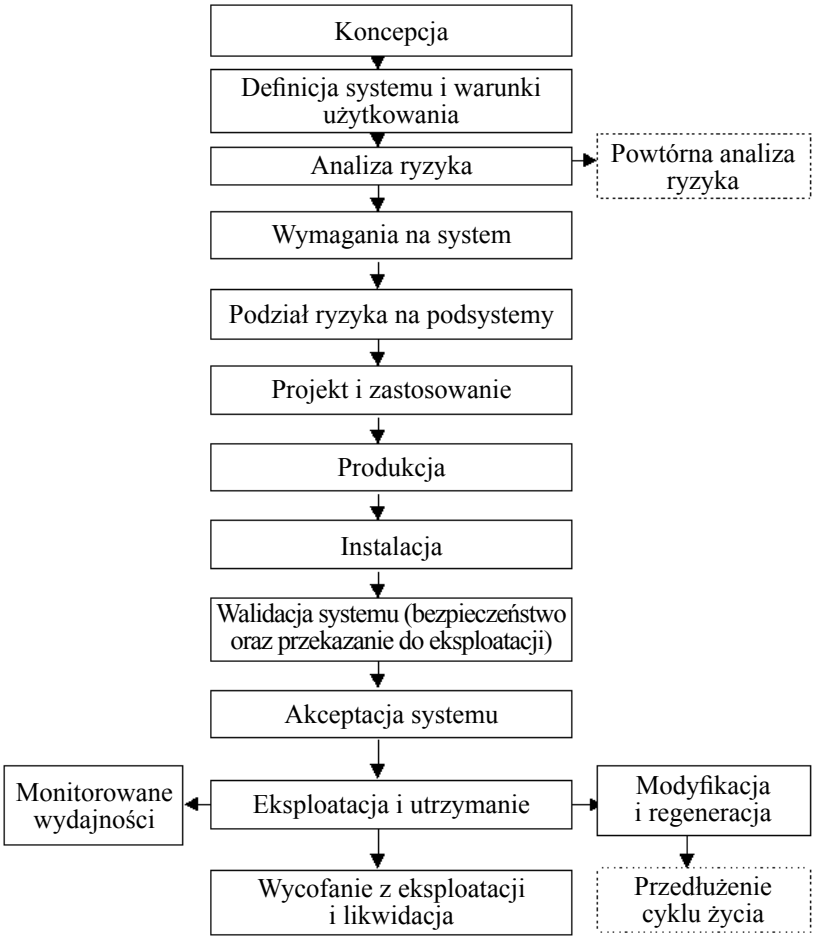
Według prawa wspólnotowego, bezpieczeństwo oznacza brak niedopuszczalnego ryzyka (czyli sytuację, w której częstotliwość występowania i skutki wszystkich zagrożeń uznaje się za akceptowalne). Obecnie, zgodnie z prawem wspólnotowym, w celu osiągnięcia bezpieczeństwa konieczne jest zarządzanie bezpieczeństwem [2, 9, 10, 11], obejmujące monitorowanie bezpieczeństwa i nadzorowanie bezpieczeństwa, oparte na zarządzaniu ryzykiem.

Przepisy polskich i europejskich norm nakładają obowiązek stosowania analizy ryzyka nie tylko przy analizie bezpieczeństwa, ale także wymagają, aby analiza ryzyka była obowiązkową częścią procesu podejmowania decyzji o wdrażaniu systemu do eksploatacji.

Zarządzanie ryzykiem jest to planowe stosowanie przez zarządców infrastruktury i przewoźników kolejowych polityki, procedur i praktyk zarządczych w zakresie analizy ryzyka oraz rejestrowania zagrożeń. Monitorowanie bezpieczeństwa to planowe stosowanie strategii, priorytetów i planów zarządczych przez tych samych zarządców i przewoźników w celu utrzymania bezpieczeństwa.

Nie oznacza to rezygnacji z już stosowanych środków bezpieczeństwa. Nie rezygnuje się ani z podziału torów na odcinki izolowane i odstępy blokowe, ani ze stosowania zasady *fail-safe*, ani ze stosowania analiz Poziomu Integralności Bezpieczeństwa SIL, ani z przepisów ruchowych. W zakresie analizy i zarządzania ryzykiem oznacza to uzupełnienie tych środków bezpieczeństwa dodatkowymi środkami, zmniejszającymi częstotliwość zagrożeń albo łagodzącymi ich skutki. Analiza ryzyka i identyfikacja stosowanych środków bezpieczeństwa ma miejsce podczas tworzenia i wdrażania, indywidualnego dla każdego zarządcy infrastruktury i przewoźnika kolejowego, Systemu Zarządzania Bezpieczeństwem (SMS). Ponieważ system kolejowy podlega zmianom, a system SMS musi podlegać doskonaleniu w celu utrzymywania bezpieczeństwa, zobowiązano zarządców i przewoźników do analizy zmian i oceny akceptowalności ryzyka. Szczególnie istotnymi stają się pytania, jak oceniać zmiany i jakie ryzyko jest akceptowalne.

Wprowadzanie analizy ryzyka w poszczególnych dziedzinach techniki jest bardzo zróżnicowane. W urządzeniach srk jej stosowanie datuje się od kilkudziesięciu lat. Normy dotyczące bezpieczeństwa, np. norma PN-EN 50126 i norma PN-EN 50129, uwzględniają analizę ryzyka w swoim zakresie (rys. 1). W normie PN-IEC 60300-3-9 [7] podano podstawowe pojęcia dotyczące analizy ryzyka.

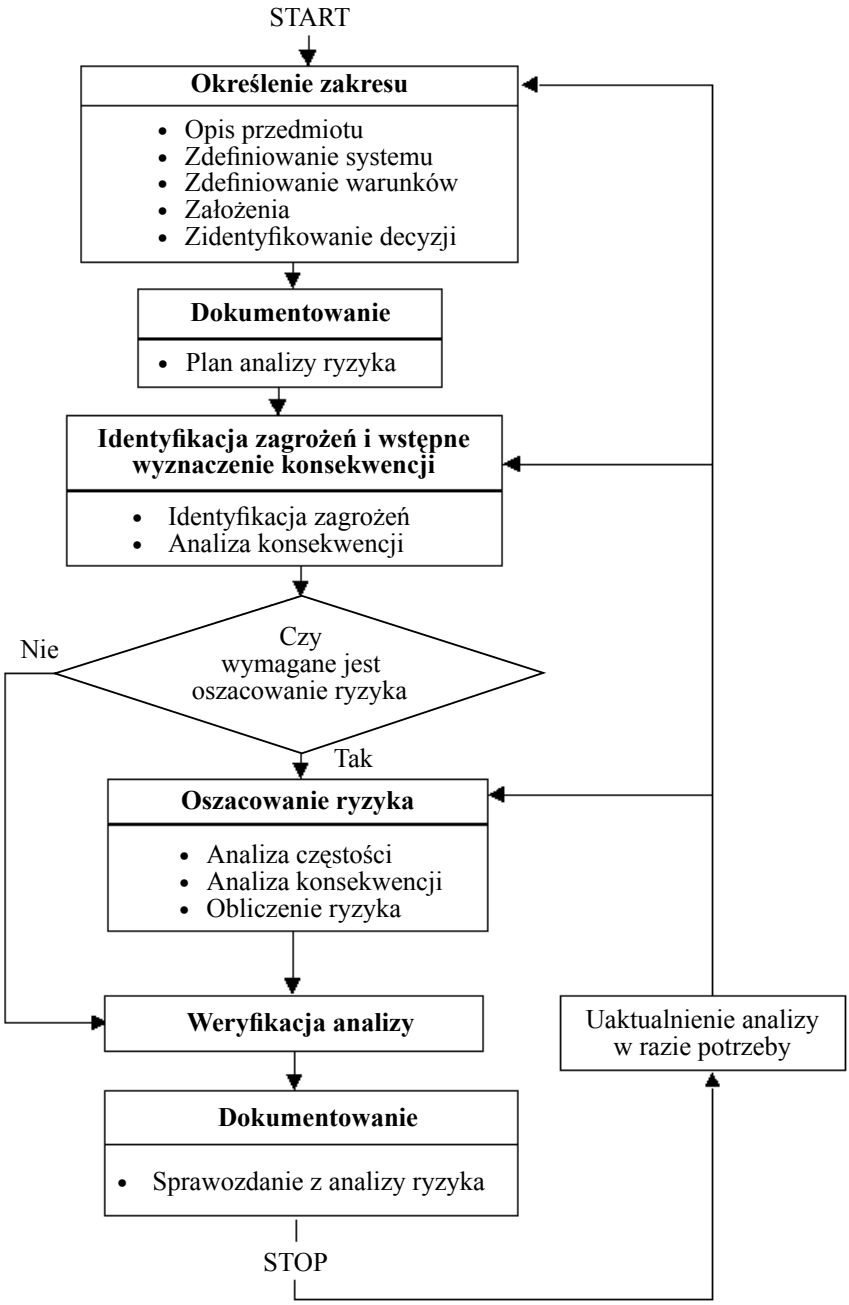


Rys. 1. Cykl życia systemu (np. srk) [3]

2. Proces analizy ryzyka

Norma PN-IEC 60300-3-9 zaleca przeprowadzanie analizy ryzyka w następującej kolejności:

1) określenie zakresu,
2) identyfikacja zagrożeń i wstępne wyznaczanie konsekwencji,
3) oszacowanie ryzyka (skutków i częstotliwości),
4) weryfikacja,
5) dokumentowanie,
6) uaktualnianie analizy.



Rys. 2. Proces analizy ryzyka [7]

Proces analizy ryzyka jest pokazany na rysunku 2. Zaleca się aby w analizie konsekwencji:

1) podstawą analizy były wyselekcjonowane niepożądane zdarzenia (zagrożenia),
2) opisane były wszystkie konsekwencje spowodowane niepożądanym zdarzeniem (zagrożeniem),
3) uwzględnione były środki łagodzące konsekwencje wraz ze stosowanym warunkami, które mają wpływ na te konsekwencje,
4) przedstawione były kryteria użyte do identyfikacji konsekwencji,
5) uwzględnione były zarówno konsekwencje bezpośrednie, jak i te, które mogą powstać po upływie pewnego czasu,
6) uwzględnione były wtórne konsekwencje, takie jak odnoszące się do sąsiadującego wyposażenia i systemów.

3. Metody analizy ryzyka

W analizie ryzyka, zarządzaniu ryzykiem, a także szacunkach ryzyka stosuje się wiele metod, do których należą między innymi:

- analiza drzewa zdarzeń,
- analiza rodzajów i skutków niezdatności, oraz analiza skutków i krytyczności niezdatności;
- analiza drzewa niezdatności,
- badania zagrożeń i gotowości operacyjnej,
- analiza niezawodności człowieka,
- wstępna analiza zagrożeń,
- schemat blokowy niezawodności,
- stopniowanie kategorii,
- listy sprawdzeń,
- analiza uszkodzeń jednakowego rodzaju,
- modele następstw,
- metoda delhijska,
- wskaźniki zagrożeń,
- symulacja Monte-Carlo i inne metody symulacyjne,
- porównania w parach,
- przegląd danych w retrospekcji,
- analiza śledząca.

Brane są pod uwagę zagrożenia rzadkie, o poważnych konsekwencjach (na przykład zderzenie czołowe pociągów spowodowane niewłaściwym działaniem urządzeń sterowania ruchem kolejowym), ale nie nieprawdopodobne (na przykład tsunami w polskich warunkach). Brane są także pod uwagę zdarzenia częściej występujące,

których konsekwencje są nieznaczne lub zazwyczaj nieznaczne (na przykład przejazd za sygnalizator wskazujący sygnał STÓJ w obszarze drogi ochronnej – czyli zasadniczo bez konsekwencji).

2.1. Kwalitatywne szacowanie ryzyka

Istnieje wiele metod kwalitatywnego szacunku ryzyka. W każdym przypadku bierze się pod uwagę tylko te czynniki ryzyka, które mają zasadniczy wpływ na ocenę skutków wystąpienia zagrożenia (wielkość szkód na chronionym obiekcie). Z licznych czynników, które mają wpływ na opracowanie bezpiecznych wymagań na system, który ma spełniać swoje funkcje ochronne (np. system srk), można wymienić:

- czas trwania zagrożenia D,
- zapobieganie zagrożeniu G,
- prawdopodobieństwo wystąpienia zagrożenia *W*.

Ryzyko szkód na ochranianym obiekcie zależy od obiektu (ludzie, aparatura, urządzenia itp.) i wielkościć potencjalnych szkód (szkody w ludziach, szkody materialne itp.) oraz częstotliwości występowania zagrożenia. Na przykład, jeżeli ochraniani są ludzie to uwzględnia się następujące zdarzenia (szkody):

- S1 – lekkie (lekkie obrażenia, lekka choroba zawodowa),
- S2 – poważne (poważne obrażenia jednej lub więcej osób lub śmierć jednej osoby),
- S3 – ciężkie (śmierć wielu osób),
- S4 – katastroficzne (bardzo wiele ofiar śmiertelnych i praktycznie całkowite zniszczenie zakładu lub systemu).

Przez czynnik „czas trwania zagrożenia" rozumie się czas trwania zagrożenia, a w przypadku ludzi czas znajdowania się w strefie zagrożenia. Można to określić jako:

- D1 – rzadki i częsty pobyt w strefie niebezpiecznej,
- D2 – bardzo częsty lub stały pobyt w strefie niebezpiecznej.

Czynnik „zapobieganie zagrożeniu" opisuje się sposobem prowadzenia eksploatacji (z dozorem lub bez, …), czasowym przebiegiem zagrożenia (szybki, powolny, …), sposobem „odwrócenia zagrożenia" (środkami technicznymi, organizacyjnymi, …), badaniami praktycznymi z wynikiem negatywnym (żadne, małe, duże, …), przewidywaniem zagrożeń i możliwościami zapobiegania (można …, można …, …). Na podstawie wymienionych danych, czynnik G można określić jako:

- G1 – możliwe w określonych warunkach,
- G2 – zawsze możliwe.

Czynnik „prawdopodobieństwo wystąpienia zagrożenia" określa się werbalnie prawdopodobieństwem wystąpienia zagrożenia przy czynności, która będzie realizowana bez funkcji ochronnych. Czynnik W można dzielić na:

- W1 – bardzo małe prawdopodobieństwo,
- W2 – małe prawdopodobieństwo,
- W3 – stosunkowo wysokie prawdopodobieństwo.

Przytoczone czynniki zagrożeń umożliwiają wytworzenie 48 ich kombinacji. Okazuje się, że praktyczne znaczenie ma 8 kombinacji czynników S, D, G. Na przykład, przy warunkach katastroficznych (czynnik S4) czynniki D i G mają bardzo mały wpływ na spełnienie ochronnych własności systemu.

Im więcej czynników zagrożeń bierze się pod uwagę i im dokładniejszy jest ich podział i określenie, tym bardziej obiektywnie można opracować wymagania dotyczące redukcji zagrożeń i bezpieczeństwa systemu. Czynniki zagrożeń wybrane do analizy zależą od konkretnego procesu sterowania dla którego mają być określone bezpieczne wymagania. Przyjmuje się na ogół cztery poziomy zagrożeń, którym można przypisać środki, jakie należy stosować:

1) **niedopuszczalne** – obniżenie prawdopodobieństwa wystąpienia zagrożenia jest niezbędne, w innym przypadku system nie może być dopuszczony do eksploatacji,
2) **niepożądane** – prawdopodobieństwa wystąpienia zagrożenia jest akceptowalne tylko wtedy, kiedy nakłady związane z jego obniżeniem są wyraźnie wyższe od osiągniętych efektów albo wtedy, gdy obniżenie ryzyka jest nieosiągalne,
3) **dopuszczalne** – prawdopodobieństwa wystąpienia zagrożenia jest akceptowalne tylko wtedy, gdy nakłady związane z jego obniżeniem są wyraźnie wyższe od osiągniętych efektów,
4) **pomijalne** – dalsze nakłady na obniżenie prawdopodobieństwa wystąpienia zagrożenia są niepotrzebne.

2.2. Kwantytatywne szacowanie ryzyka

Istnieje wiele metod kwantytatywnego szacowania ryzyka. Ogólnie należy przyjąć, że ryzyko jest kombinacją intensywności wystąpienia zagrożeń h i ich następstw S.

$$R = h \cdot S.$$

Ponieważ dla jednego systemu mamy do czynienia z wieloma zagrożeniami, całkowite ryzyko związane z użyciem systemu (np. srk) składa się z wielu występujących zagrożeń i ich konsekwencji, co można wyrazić wzorem:

$$R = \sum_{i=1}^{n} h_i \cdot S_i .$$

gdzie h_i – intensywność wystąpienia *i*-tego zagrożenia, S_i następstwa *i*-tego zagrożenia.

Prawdopodobieństwo wystąpienia *i*-tego zagrożenia można określić następująco:

$$P_i = \frac{h_i}{\sum_{i=1}^{n} h_1} .$$

Oczekiwana wielkość skutków na jednostkę czasu:

$$E_{(S)} = \sum_{i-1}^{n} S_i \cdot P_i$$

i w efekcie

$$R = E_{(S)} \cdot \sum_{i=1}^{n} h_i .$$

2.3. Identyfikacja zagrożeń w urządzeniach srk

W celu oszacowania ryzyka niezbędne jest określenie zagrożeń związanych ze sterowaniem procesem ruchu kolejowego (należy opracować listę zagrożeń). Listę zagrożeń można opracować na podstawie analiz i rozważań teoretycznych lub też na podstawie dotychczasowych doświadczeń z eksploatacji podobnych systemów i danych statystycznych. Lista zagrożeń jest najczęściej opracowywana jako kombinacja obu sposobów ze szczególnym uwzględnieniem bezpieczeństwa funkcjonalnego urządzeń srk [4]. Czynniki, które należy wziąć pod uwagę jako zagrożenie są zależne od poziomu analizy systemowej. Wynik analizy ryzyka nie zależy od kwantyfikacji identyfikowanych zagrożeń ale zależy od tego, jak jest określona przestrzeń niebezpiecznych stanów systemu. Ze statystyki można przyjąć, że przyczyną wystąpienia wypadku była błędna czynność w rozpatrywanym obiekcie (przestawienie zwrotnicy pod jadącym pociągiem, nieprawdziwe podawanie zajętości odcinka torów itp.) lub błąd w logice systemu. W obiektach kolejowych związanych ze sterowaniem ruchem kolejowym przykładowo można określić następujące zagrożenia:

dla semafora:

- wyświetlenie fałszywego sygnału zezwalającego (zezwolenie na jazdę, gdy powinien być wyświetlony sygnał zabraniający),
- niewyświetlenie sygnału zabraniającego,

- wyświetlenie sygnału zezwalającego na większą szybkość,
- i temu podobne;

dla zwrotnicy:
- przestawienie utwierdzonej zwrotnicy,
- przestawienie zwrotnicy pod taborem,
- błędna informacja o położeniu zwrotnicy
- i temu podobne;

dla odcinka torów:
- błędna informacja o niezajętości odcinka,
- błędna informacja o zajętości odcinka
- i temu podobne.

Przyczyną zagrożeń w eksploatacji systemu srk może być również pomyłka personelu obsługującego podczas wykonywania czynności bezpośrednio związanych z prowadzeniem ruchu pociągów. Można określić, że wpływ personelu obsługi na realizowanie funkcji związanych z prowadzeniem ruchu może być:
żaden – system funkcjonuje poprawnie i w pełnym zakresie kontroluje bezpieczeństwo przy dowolnych poleceniach wydawanych przez personel;
częściowy:
- system funkcjonuje, ale jego rozwiązanie techniczne nie pozwala na pełną kontrolę wszystkich poleceń personelu (również nieprawidłowych),
- system funkcjonuje częściowo, niektóre realizowane funkcje bezpiecznościowe wykonywane są przez personel obsługi bez nadzoru systemu;

całkowity – system nie funkcjonuje, wszystkie czynności związane z bezpieczeństwem wykonuje personel obsługujący bez kontroli przez system.

2.4. Analiza skutków zagrożeń

Tak, jak usterka może być przyczyną różnych zagrożeń, tak i zagrożenie, w zależności od konkretnych warunków eksploatacyjnych, może być przyczyną różnego rodzaju następstw. Dlatego przy analizie ryzyka, każde zagrożenie należy analizować z punktu widzenia wszystkich możliwych następstw, przy czym prawdopodobieństwo wystąpienia jednakowych następstw będzie różne i zależne od warunków eksploatacyjnych (na przykład od natężenia ruchu).

Zagrożenia związane z używaniem (eksploatacją) systemu srk mogą prowadzić do różnorakich następstw, a mianowicie:
- najechanie pojazdu trakcyjnego na tył poprzedzającego pojazdu trakcyjnego,
- uderzenie pojazdu trakcyjnego w bok innego pojazdu trakcyjnego,
- zderzenie czołowe pojazdów trakcyjnych,
- zderzenie pojazdu trakcyjnego z pojazdem drogowym,
- najechanie na pieszego,

- wykolejenie pojazdu trakcyjnego,
- i temu podobne.

Następstwem wypadku mogą być szkody materialne, narażenie ludzi lub inne szkody. Jeżeli istnieje realna groźba śmierci człowieka lub wyraźnego uszczerbku jego zdrowia, wtedy materialne szkody mogą być pomijalne i nie należy ich brać pod uwagę przy analizie ryzyka. Narażenie człowieka można określić liczbą śmiertelnych przypadków:

$$S_N = S_M + k_Z \cdot S_Z + k_L \cdot S_L ,$$

gdzie:

S_M – liczba wypadków śmiertelnych,
S_Z – liczba ciężkich obrażeń,
S_L – liczba lekkich obrażeń,
k_Z – współczynnik akceptacji ciężkich obrażeń,
k_L – współczynnik akceptacji urazów lekkich.

Na przykład, w części informacyjnej normy PN-EN 50126 przytoczono współczynniki $k_Z = 10$, $k_L = 100$.

3. Zmiany mające wpływ na bezpieczeństwo

Zmiany w urządzeniach kolejowych (w tym w urządzeniach srk) można podzielić na mające wpływ na bezpieczeństwo i nie mające wpływu na bezpieczeństwo. Gdy zmiana nie ma wpływu na bezpieczeństwo, nie ma konieczności stosowania procesu analizy i zarządzania ryzykiem, gdy wprowadzana zmiana ma wpływ na bezpieczeństwo, zarządca infrastruktury, przewoźnik, podmiot zamawiający, producent lub wykonawca, kierując się fachowym osądem, decyduje czy zmiana jest znacząca [8, 9]. Jeśli zmiana jest znacząca (podniesienie prędkości na linii, nowy typ taboru, nowy typ urządzeń sterowania ruchem kolejowym, w tym sygnalizacja kabinowa), to wówczas wycena ryzyka uwzględnia następujące kryteria:

Skutek awarii systemu – potencjalnie najpoważniejszy, ale wiarygodny skutek awarii ocenianego systemu (najgorszy scenariusz w przypadku awarii) przy uwzględnieniu istnienia barier zabezpieczających poza ocenianym systemem. Na przykład wymiana pulpitu nastawczego z kostkowego na komputerowy przy zachowaniu nastawnicy, czyli niezmienionych i bezpiecznych zależności pomiędzy poszczególnymi drogami przebiegu przez stację może być oceniona jako mająca wpływ na bezpieczeństwo, ale zabezpieczona zależnościami pozostającymi poza pulpitem nastawczym.

Innowacja wykorzystana przy wprowadzaniu zmiany – przekształcenie istniejących możliwości w nowe idee i wprowadzenie ich do praktycznego zastosowania w celu wprowadzenia pożądanej zmiany. Kryterium to obejmuje innowacje dotyczące zarówno całej branży kolejowej lub tylko organizacji wprowadzającej zmianę. Innowacje na skalę branży kolejowej mogą dotyczyć jednego typu podmiotów w wielu krajach Wspólnoty lub wielu podmiotów w jednym lub kilku krajach współtworzących system kolei. Na przykład, wdrożenie nowego typu klocków hamulcowych typu LL, które było testowane w projekcie „Eurotrain" na różnych sieciach kolejowych i w różnych warunkach pogodowych przy współpracy wielu przewoźników i zarządców infrastruktury, prowadzące do wprowadzenia innowacyjnych klocków LL przez przewoźników kolejowych z różnych krajów, należałoby do pierwszej grupy. Natomiast wprowadzenie zasady ruchomego odstępu blokowego w zarządzaniu następstwem pociągów jako wymagające bezpiecznej współpracy urządzeń pokładowych i przytorowych należałoby do drugiej grupy. Przykładem zmiany wprowadzanej przez jedną organizację może być wymiana blokady liniowej na blokadę nowszej generacji, w tym na blokadę mającą tymczasowe świadectwo typu dla urządzenia służącego do prowadzenia ruchu kolejowego na potrzeby testów w eksploatacji nadzorowanej, pod warunkiem zachowania istniejącego rozmieszczenia sygnalizatorów i zróżnicowania obrazów sygnałowych.

Złożoność zmiany – skala zróżnicowania elementów składowych systemu i relacji między nimi. Przykładowo, z wysoką złożonością zmiany będziemy mieli do czynienia przy wprowadzaniu mechatronicznych wózków kolejowych. W założeniu, takie wózki powinny lepiej współpracować zarówno z infrastrukturą, jak i w istotny sposób poprawiać komfort jazdy. Wózki takie mają wiele elementów i urządzeń wykorzystujących różne technologie. Ponadto, relacje między urządzeniami i elementami współtworzącymi takie wózki są na tyle skomplikowane, że prace utrzymaniowe, nawet przy pełnej dostępności urządzeń i elementów, wymagają wysokich kwalifikacji personelu i dedykowanych narzędzi.

Monitoring – zdolność bądź jej brak do monitorowania wprowadzonej zmiany podczas całego cyklu życia systemu i dokonywania odpowiednich interwencji. Przykładowo, wprowadzenie nowej generacji systemów kontroli niezajętości torów wykorzystujących Globalny System Pozycjonowania (GPS), nie umożliwia ani monitorowania zmiany, ani dokonywania interwencji w całym cyklu życia systemu.

Odwracalność zmiany – zdolność bądź niezdolność powrotu do systemu sprzed zmiany lub zabezpieczenia się przed konsekwencjami wprowadzenia zmiany. Wprowadzenie sygnalizacji kabinowej, jako uzupełnienia sygnalizacji przytorowej czyli z jej zachowaniem, najczęściej zapewnia możliwość powrotu do systemu sprzed zmiany, nawet przez wyłączenie zasilania przytorowych urządzeń przekazujących dane do pojazdów. Będzie znacznie trudniej wrócić do sta-

rego systemu łączności bezprzewodowej, szczególnie jeśli poprzednie urządzenia zostały zdemontowane albo wygasło prawo do korzystania z częstotliwości wykorzystywanych przez poprzednie urządzenia. Utrzymywanie starych urządzeń łączności bezprzewodowej prowadzi do utrudnień eksploatacyjnych. Z powodu tych utrudnień dąży się do maksymalnego skracania okresu wykorzystywania dwóch systemów. Dodatkowo systemy mogą się wzajemnie zakłócać, co wymaga stosowania drogich filtrów częstotliwościowych.

Dodatkowość – znaczenie zmiany z uwzględnieniem wszystkich przeprowadzonych niedawno zmian ocenianego systemu, które były związane z bezpieczeństwem i nie zostały ocenione jako znaczące. Przykładowo, prowadzone i oceniane niezależnie: przebudowa tunelu, podbicie torów i wymiana sieci trakcyjnej mogłyby być uznane za mające wpływ na bezpieczeństwo, ale nie stanowiące znaczącej zmiany. Zakup taboru piętrowego do obsługi przewozów po linii wykorzystującej zmodernizowany tunel wymaga wymiany informacji pomiędzy zaangażowanymi stronami, bo mimo że sam zakup taboru istniejącego typu może być uznany za mający wpływ na bezpieczeństwo, ale nie stanowiący znaczącej zmiany, to w powiązaniu ze zmianami wprowadzonymi w infrastrukturze może prowadzić do zmiany znaczącej. Taką zmianą jest nadmierne zbliżenie do stropu tunelu górnych przewodów jezdnych podczas przejazdu piętrowego taboru, wywołujące na przykład ryzyko porażenia prądem pasażerów. Zastosowanym środkiem bezpieczeństwa może być na przykład warstwa izolacyjna naniesiona na strop tunelu.

Każda decyzja przesądzająca o tym, czy zmiana ma lub nie ma wpływu na bezpieczeństwo oraz jeśli ma wpływ na bezpieczeństwo, to czy jest to zmiana znacząca lub nie, musi być uzasadniona, a stosowna dokumentacja musi być odpowiednio przechowywana przez zarządcę infrastruktury, przewoźnika kolejowego, podmiot zamawiający, producenta lub wykonawcę. Jeśli zmiana jest znacząca, to konieczna jest ocena, czy ryzyko jest akceptowalne. Przy ocenie systemów sterowania ruchem kolejowym od wielu lat w tym zakresie stosuje się analizę poziomu integralności bezpieczeństwa SIL.

4. Wycena ryzyka i kryteria akceptowalności ryzyka

Zarządcy infrastruktury i przewoźnicy kolejowi, wprowadzając zmiany w swojej działalności, jak również akceptując zmiany u podwykonawców, niezależnie od tego czy zmiany te mają charakter techniczny (na przykład zmiana procesu utrzymania taboru lub infrastruktury), czy eksploatacyjny (na przykład zmiana przepisów ruchowych), czy organizacyjny (na przykład podział lub łączenie jednostek eksploatacyjnych oraz zmiana skali *outsourcingu*) są zobowiązani do wyceny ryzyka, czyli oceny akceptowalności ryzyka wprowadzanego przez daną

zmianę. Do takiej oceny są także zobowiązane podmioty zamawiające oraz producenci i wykonawcy jeśli angażują jednostkę notyfikowaną do przeprowadzenia procedury weryfikacji WE podsystemu. Wymóg ten w przejrzysty sposób wiąże zasady ujęte w europejskiej dyrektywie w sprawie interoperacyjności kolei [1] i europejskiej dyrektywie w sprawie bezpieczeństwa kolei [2]. Upraszczając, można powiedzieć, że dyrektywa w sprawie interoperacyjności dotyczy przekazywania do eksploatacji nowobudowanych, modernizowanych i odnawianych podsystemów współtworzących system kolei, a dyrektywa w sprawie bezpieczeństwa dotyczy zarządzania bezpieczeństwem, w tym zarządzania ryzykiem w eksploatacji. Wymóg ten oznacza zobowiązanie podmiotów zamawiających, producentów i wykonawców do prowadzenia oceny akceptowalności ryzyka wprowadzanego przez budowę, modernizację, odnowę podsystemu (drogi kolejowej, zasilania trakcyjnego, sterowania i łączności oraz taboru czy systemów bezpiecznej kontroli jazdy pociągów).

Kryteria akceptowalności ryzyka są to kryteria, na podstawie których jest oceniana dopuszczalność danego ryzyka; kryteria te stosuje się, aby ustalić czy poziom ryzyka jest na tyle niski, że nie jest konieczne podejmowanie natychmiastowych działań w celu jego zredukowania. Ocenę ryzyka wynikającego ze znaczącej zmiany prowadzi się przez weryfikację stosowania kodeksów postępowania lub przez porównanie z podobnymi systemami albo przez jawne szacowanie ryzyka. Metody te mogą być stosowane samodzielnie, jak również w dowolnej kombinacji. Wybór metody należy do zarządcy infrastruktury, przewoźnika, podmiotu zamawiającego, producenta lub wykonawcy, który prowadzi ocenę akceptowalności ryzyka wynikającego ze znaczącej zmiany i nie może być narzucany przez niezależną Jednostkę Oceniającą (AsBo).

Ocena akceptowalności ryzyka przez weryfikację stosowania kodeksów postępowania wykorzystuje powszechnie uznane i jednocześnie publicznie dostępne kodeksy postępowania (na przykład normy, specyfikacje TSI, jeśli te specyfikacje nie wymagają oceny akceptowalności ryzyka, karty UIC oraz krajowe przepisy dotyczące bezpieczeństwa, jeśli były notyfikowane). Wykorzystywanie kodeksów postępowania jest możliwe jeśli są one właściwe z punktu widzenia nadzoru nad rozważanymi zagrożeniami, powodowanymi przez znaczące zmiany. Jeżeli zagrożenie lub zagrożenia są kontrolowane za pomocą takich kodeksów postępowania, to uznaje się, że ryzyko jako pozostające poniżej kryterium akceptowalności ryzyka jest dopuszczalne, a zastosowanie kodeksów postępowania odnotowuje się w rejestrze zagrożeń. Jeśli kodeks postępowania nie jest w pełni stosowany, to konieczne jest wykazanie, że nie obniża to bezpieczeństwa.

Ocena akceptowalności ryzyka przez porównanie do systemu odniesienia wykorzystuje występowanie w podobnym systemie zagrożenia lub zagrożeń powodowanych przez znaczące zmiany. Korzystanie z systemu odniesienia jest możliwe tylko wówczas, gdy łącznie spełnione są następujące warunki: system

odniesienia jest eksploatowany w podobnych warunkach eksploatacyjnych i środowiskowych jak system oceniany, system odniesienia ma podobne funkcje i interfejsy jak system oceniany oraz system odniesienia sprawdził się już w praktyce jako system o dopuszczalnym poziomie bezpieczeństwa i również obecnie spełniłby warunki wymagane do jego zatwierdzenia. Porównanie do systemu odniesienia pozwala na stwierdzenie, że ryzyko związane z zagrożeniami uwzględnionymi w systemie odniesienia uważa się za pozostające poniżej kryterium akceptowalności ryzyka, czyli dopuszczalne pod warunkiem stosowania tych samych środków bezpieczeństwa. Środki te odnotowuje się w rejestrze zagrożeń. Jeżeli występują różnice pomiędzy ocenianym systemem a systemem odniesienia, wycena ryzyka powinna wykazać, że oceniany system cechuje co najmniej taki sam poziom bezpieczeństwa jak system odniesienia.

Ocena akceptowalności ryzyka przez szacowanie i wycenę jawnego ryzyka wykorzystuje ilościowe i jakościowe szacowanie ryzyka i wynikających z niego zagrożeń z uwzględnieniem istniejących środków bezpieczeństwa. Metodę taką, ze względu na jej wysoką pracochłonność i kosztochłonność, stosuje się jako metodę uzupełniającą ocenę według kodeksu postępowania i ocenę według systemu odniesienia. Wymaga się, aby zagrożenia uważać za pozostające poniżej kryterium akceptowalności ryzyka, jeśli spełniają kryteria wywodzące się z prawa wspólnotowego lub przepisów prawa krajowego, jeśli były notyfikowane. Dla systemów technicznych, nie objętych kodeksami postępowania, ani nie uznanych za dopuszczalne przez porównanie z systemem odniesienia, dla których w przypadku awarii zachodzi wiarygodne prawdopodobieństwo katastroficznych konsekwencji, jako kryterium akceptowalności ryzyka dla systemów sterowania ruchem kolejowym przyjmuje się częstotliwość takich awarii równą lub mniejszą niż 10^{-9} na godzinę pracy systemu. Jeżeli ryzyko związane z zagrożeniem lub zagrożeniami jest uważane za dopuszczalne, zidentyfikowane środki bezpieczeństwa zostają odnotowane w rejestrze zagrożeń.

Niezależnie od przyjętej metody wyceny ryzyka i powiązanego z nią kryterium akceptowalności ryzyka, jeśli szacowane ryzyko nie jest dopuszczalne, należy określić i wdrożyć dodatkowe środki bezpieczeństwa, aby zredukować ryzyko do dopuszczalnego poziomu.

5. Podsumowanie

Analiza ryzyka i zarządzanie ryzykiem jest dziedziną skomplikowaną i rozległą. Dotyczy to wszystkich systemów technicznych. Dla systemów związanych z bezpieczeństwem, w tym urządzeń srk, brakuje do tej pory konkretnych szczegółowych wytycznych do przeprowadzania prac związanych z analizą ryzyka. Wydaje się niezbędne prowadzenie prac na polskich kolejach, mających na celu

wdrożenie analizy ryzyka przy projektowaniu, produkcji i eksploatacji urządzeń związanych z bezpieczeństwem. W pierwszej kolejności dotyczy to urządzeń srk. Analiza ryzyka jest niezbędna przy podejmowaniu decyzji o wdrażaniu systemów srk do eksploatacji. Wymagają tego zarówno przepisy, jak i potrzeba podejmowania racjonalnych decyzji o wdrażaniu systemów.

Zobowiązanie podmiotów branży kolejowej do stosowania zarządzania ryzykiem z pewnością uporządkuje stosowane w transporcie kolejowym środki bezpieczeństwa. Jest to szczególnie istotne w dobie liberalizacji transportu kolejowego, której przejawem jest między innymi podział kolei narodowych na wiele podmiotów gospodarczych. Dzięki wprowadzeniu zarządzania ryzykiem, będą uporządkowane środki bezpieczeństwa stosowane przez indywidualne podmioty. Uporządkowane będą wymagania w zakresie jakości i bezpieczeństwa zamawianych materiałów i usług mających wpływ na bezpieczeństwo. Analizowane będą interakcje pomiędzy podmiotami w celu określania środków bezpieczeństwa koniecznych do minimalizacji częstotliwości i skutków występowania zagrożeń powodowanych przez ryzyko resztkowe, nie uwzględnione w indywidualnych procesach zarządzania ryzykiem.

Literatura

1. DYREKTYWA PARLAMENTU EUROPEJSKIEGO I RADY 2008/57/WE z dnia 17 czerwca 2008 r. w sprawie interoperacyjności systemu kolei we Wspólnocie (przekształcenie).
2. DYREKTYWA 2004/49/WE PARLAMENTU EUROPEJSKIEGO I RADY z dnia 29 kwietnia 2004 r. w sprawie bezpieczeństwa kolei.
3. PN-EN 50126:2002/AC:2011: Zastosowania kolejowe – Specyfikacja niezawodności, dostępności, podatności utrzymaniowej i bezpieczeństwa.
4. PN-EN 50128:2011: Zastosowania kolejowe – Systemy łączności, przetwarzania danych i sterowania ruchem – Oprogramowanie kolejowych systemów sterowania i zabezpieczenia.
5. PN-EN 50129:2007/AC:2010: Zastosowania kolejowe – Systemy łączności. przetwarzania danych i sterowania ruchem – Elektroniczne systemy sterowania ruchem związane z bezpieczeństwem.
6. PN EN 61508-1/2010: Bezpieczeństwo funkcjonalne elektrycznych/elektronicznych/programowalnych systemów związanych z bezpieczeństwem – Część 1: Wymagania ogólne.
7. PN IEC 60300-3-9:1999P: Zarządzanie niezawodnością – Przewodnik zastosowań – Analiza ryzyka w systemach technicznych.
8. ROZPORZĄDZENIE KOMISJI (WE) NR 352/2009 z dnia 24 kwietnia 2009 r. w sprawie przyjęcia wspólnej metody oceny bezpieczeństwa w zakresie wyceny i oceny ryzyka, o której mowa w art. 6 ust. 3 lit. a) dyrektywy 2004/49/WE Parlamentu Europejskiego i Rady.
9. ROZPORZĄDZENIE 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 352/2009.
10. ROZPORZĄDZENIE KOMISJI (UE) NR 1077/2012 z dnia 16 listopada 2012 r. w sprawie wspólnej metody oceny bezpieczeństwa w odniesieniu do nadzoru sprawowanego przez krajowe organy ds. bezpieczeństwa po wydaniu certyfikatu bezpieczeństwa lub autoryzacji bezpieczeństwa.
11. ROZPORZĄDZENIE KOMISJI (UE) NR 1078/2012 z dnia 16 listopada 2012 r. w sprawie wspólnej metody oceny bezpieczeństwa w odniesieniu do monitorowania, która ma być stosowana przez przedsiębiorstwa kolejowe i zarządców infrastruktury po otrzymaniu certyfikatu bezpieczeństwa lub autoryzacji bezpieczeństwa oraz przez podmioty odpowiedzialne za utrzymanie.

Safety and Risk for Example Signaling Equipment

Summary
Article describes safety estimation rules used in railway transport on the example of control command and signalling systems safety estimation. Methods described in the European standards as well as methods described in the European Commission Regulations have been analysed. Different safety assessment methods were pointed and qualitative and quantitative safety estimation methods were described and compared. Taking control command and signalling systems as an example article describes possible faults and threats which may be caused by them. In accordance with the European Community law risk is described as a joint result of single threat consequences and its' probability (threat frequency). Article describes ways used to create lists of threats. Risk for different threat is then estimated and compared with risk acceptance criteria and included in safety management systems of the railway infrastructure managers and railway undertakings.

Keywords: safety, risk, threats

Безопасность и риск на примере устройств сигнализации, централизации и блокировки (СЦБ)

Резюме
В статье описаны принципы оценки безопасности, применяемые в железнодорожном транспорте, на примере оценки безопасности устройств сигнализации, централизации и блокировки (СЦБ). Проанализированы методы, описанные в европейских стандартах и распоряжениях Европейской комиссии. Указаны разные методы оценки безопасности, а также описано и сравнено оценивание безопасности для оценки квалитативной и квантитативной. На примере устройств СЦБ описаны недостатки и опасности, к которым они могут привести. В соответствии с законодательством ЕС риск представлен как общий результат масштаба угрозы и вероятности возникновения (частоты возникновения данной угрозы). Показано каким образом создаются списки угроз и как оценивается риск для отдельных угроз, который затем сравнивается с критериями допустимости риска и учитывается в системе управления безопасностью в инфраструктуре и железнодорожных перевозках.

Ключевые слова: безопасность, риск, угроза