SCENARIUSZ

oceny zmiany

dla zmiany technicznej polegającej na wprowadzeniu zmian w oprogramowaniu jako zmiany mającej wpływ na bezpieczeństwo ruchu kolejowego

Wstęp

Proces oceny zmiany, rozumiany jako ustalenie, czy zmiana wpływa na bezpieczeństwo, określenie jej znaczenia (dla zmian wpływających na bezpieczeństwo) oraz analiza ryzyka (dla zmian uznanych za znaczące), przebiega w kilku opisanych poniżej krokach.

Przedstawiony scenariusz opiera się na uproszczonym opisie podmiotu i w procesie zarządzania ryzykiem uwzględnia jedynie wybrane dane i informacje, w tym zagrożenia. Wdrażając w działaniach praktycznych zaproponowane w scenariuszu rozwiązania, należy uwzględnić specyficzne, rzeczywiste warunki i cechy systemu kolejowego podmiotu, dla którego mają być one zastosowane.

1. Ocena wpływu zmiany na bezpieczeństwo

Ocenę wpływu zmiany na bezpieczeństwo należy przeprowadzić w sposób opisany szczegółowo w publikacji Urzędu Transportu Kolejowego pt. *„Ekspertyza dotycząca praktycznego stosowania przez podmioty sektora kolejowego wymagań wspólnej metody bezpieczeństwa w zakresie oceny ryzyka (CSM RA) opracowana w formie przewodnika”*, dostępnej na stronie utk.gov.pl w zakładce:

Wprowadzona zmiana, polegająca na zaprojektowaniu i zainstalowaniu nowego oprogramowania w eksploatowanym systemie urządzeń komputerowych, dostosowując go do wymuszonych czynnikami zewnętrznymi zmian sprzętowych oraz współpracy z innymi wdrażanymi systemami nadzoru i sterowania ruchem kolejowym, bezpośrednio wpływa na poprawę bezpieczeństwa systemu kolejowego.

2. Ocena znaczenia zmiany

Ocenę znaczenia zmiany według kryteriów wymienionych i opisanych w art. 4 CSM RA należy przeprowadzić w sposób opisany szczegółowo w publikacji Urzędu Transportu Kolejowego pt. *„Ekspertyza dotycząca praktycznego stosowania przez podmioty sektora kolejowego wymagań wspólnej metody bezpieczeństwa w zakresie oceny ryzyka (CSM RA) opracowana w formie przewodnika”*, dostępnej na stronie utk.gov.pl w zakładce wskazanej powyżej w pkt 1.

2.1 Wstępna definicja zmiany

Zmiana dotyczy zaprojektowania i zainstalowania nowego oprogramowania w eksploatowanym systemie urządzeń komputerowych, dostosowując go do wymuszonych czynnikami zewnętrznymi zmian sprzętowych oraz współpracy z innymi wdrażanymi systemami nadzoru i sterowania ruchem kolejowym (np.: ERTMS/ETCS odpowiedniego poziomu) dla określonych węzłów, stacji oraz odcinków linii.

2.2 Kryterium „dodatkowość”

W ramach ocenianego systemu nie wystąpiły zmiany o charakterze technicznym, związane z bezpieczeństwem, ocenione jako nieznaczące z punktu widzenia bezpieczeństwa transportu kolejowego. Zdaniem zespołu kryterium dodatkowości **nie ma znaczenia** dla oceny przedmiotowej zmiany.

2.3 Kryterium „skutki awarii”

Najgorszym możliwym scenariuszem, wynikającym z wprowadzonej zmiany, jest zdarzenie kolejowe spowodowane niewłaściwą konfiguracją, uszkodzeniem systemu komputerowego bądź nieprzestrzeganiem zasad przez personel obsługi lub eksploatacji, polegające na kolizji lub najechaniu pociągów/pojazdów kolejowych, co oznacza poważny wypadek kolejowy z wieloma ofiarami śmiertelnymi. Kryterium to dla przedmiotowej zmiany **ma znaczenie**.

2.4 Kryterium „innowacja”

Wysoki stopień innowacyjności. Wprowadzana zmiana oprogramowania w eksploatowanym systemie urządzeń komputerowych – dostosowująca go do wymuszonych czynnikami zewnętrznymi zmian sprzętowych oraz współpracy z innymi wdrażanymi systemami nadzoru i sterowania ruchem kolejowym (np.: ERTMS/ETCS odpowiedniego poziomu) dla określonych węzłów, stacji oraz odcinków linii – nie był dotychczas w takiej konfiguracji sprzętowej eksploatowany na sieci zarządzanej przez zarządcę infrastruktury. Wprowadzane nowe oprogramowanie będzie wykorzystywało dotychczasowe zabudowane składniki interoperacyjności. Kryterium to dla przedmiotowej zmiany **ma znaczenie.**

2.5 Kryterium „złożoność”

Wysoki stopień złożoności. Analizowana zmiana jest związana z wprowadzeniem do eksploatacji dotychczas nieeksploatowanych na sieci zarządcy infrastruktury zmian oprogramowania w eksploatowanym systemie urządzeń komputerowych. Zmiana ma na celu dostosowanie urządzeń komputerowych do, wymuszonych czynnikami zewnętrznymi, zmian sprzętowych oraz współpracy z innymi wdrażanymi systemami nadzoru i sterowania ruchem kolejowym dla określonych węzłów, stacji i odcinków linii. Opracowanie zmian w oprogramowaniu polegać będzie na zmianach w połączeniach wewnętrznych komputerowego systemy zależnościowego, w konfiguracji sprzętowej zainstalowanego systemu, na instalacji nowych interfejsów do współpracy z innymi systemami (np.: ERTMS/ETCS odpowiedniego poziomu) oraz na modyfikacji (likwidacji) wybranych stanowisk sterowania. Kryterium to dla przedmiotowej zmiany **ma znaczenie.**

2.6 Kryterium „monitoring”

Jednostki organizacyjne zarządcy infrastruktury będą monitorować system, wykorzystując istniejący podsystem TVU oraz Centrum Utrzymania i Diagnostyki (poprzez okresowe przeglądy i kontrole wykonywane przez pracowników funkcyjnych służb kontroli, eksploatacji, utrzymania i diagnostyki zarządcy infrastruktury) i mogą reagować na pojawiające się zagrożenia, opierając się na procedurach kontrolnych obowiązujących u zarządcy infrastruktury. Kryterium to dla przedmiotowej zmiany **nie ma znaczenia.**

2.7 Kryterium „odwracalność”

Wprowadzana zmiana z punktu widzenia technicznego jest w pełni odwracalna do poprzedniej wersji oprogramowania. Jednakże z technologicznego, ekonomicznego i eksploatacyjnego punktu widzenia powrót do systemu sprzed zmiany jest nieracjonalny i nieuzasadniony.

Powrót do stanu sprzed zmiany systemu spowodowałby przywrócenie istniejących poprzednio zagrożeń i ograniczeń eksploatacyjnych. Kryterium to dla przedmiotowej zmiany **nie ma znaczenia.**

2.8 Podsumowanie

Zdaniem Zespołu oceniającego z uwagi na kryteria „skutki awarii systemu”, „innowacyjność” oraz „złożoność” – uznane za mające znaczenie dla oceny przedmiotowej zmiany – („dodatkowość”, „monitoring”, „odwracalność” uznane za pozbawione znaczenia) przedmiotową zmianę wprowadzaną do systemu kolejowego należy uznać za **znaczącą**.

3. Proces zarządzania ryzykiem zmian uznanych za znaczące

Zarządzanie ryzykiem związanym ze zmianą uznaną za znaczącą należy przeprowadzić w sposób opisany szczegółowo w publikacji Urzędu Transportu Kolejowego pt. *„Ekspertyza dotycząca praktycznego stosowania przez podmioty sektora kolejowego wymagań wspólnej metody bezpieczeństwa w zakresie oceny ryzyka (CSM RA) opracowana w formie przewodnika”*, dostępnej na stronie utk.gov.pl w zakładce wskazanej w pkt 1.

3.1 Definicja zmiany

3.1.1 Cel systemu (zamierzone przeznaczenie)

Głównym celem wdrożenia zmiany jest zaprojektowanie i zainstalowanie nowego oprogramowania w eksploatowanym systemie urządzeń komputerowych, w celu dostosowania go do wymuszonych czynnikami zewnętrznymi zmian sprzętowych oraz współpracy z innymi wdrażanymi systemami nadzoru i sterowania ruchem kolejowym(np.: ERTMS/ETCS odpowiedniego poziomu) dla określonych węzłów, stacji i odcinków linii. Wprowadzany system nowego oprogramowania będzie pracował z wykorzystaniem istniejących lub dobudowanych składników interoperacyjności.

Zmiana ma bezpośredni wpływ na poprawę bezpieczeństwa systemu kolejowego, a także na zwiększenie stopnia wykorzystania zdolności przepustowej modernizowanej stacji lub odcinka linii kolejowej poprzez wielokrotne zwiększenie natężenia prowadzonego na tej linii ruchu kolejowego, wyrażanego liczbą par pociągów w dobie.

3.1.2 Funkcje i elementy systemu, jeżeli ma to zastosowanie (w tym element ludzki, techniczny i operacyjny)

Główne funkcje i elementy systemu, którego dotyczy zmiana oprogramowania, to:

- Centralny System Zależnościowy (CSZ) – wykonujący funkcje zależnościowe,
- System Sterowników Obiektowych (SSO), sterujący stacyjnymi obiektami przytorowymi, takimi jak: sygnalizatory, zwrotnice, wykolejnice, urządzenia samoczynnej i półsamoczynnej blokady liniowej lub stacyjnej (przekaźnikowej,

elektromechanicznej lub elektronicznej), systemy zabezpieczenia ruchu na przejazdach uzależnionych w systemie stacyjnym oraz inne systemy sterowania ruchem, sąsiadujące z CSZ,

– System Transmisyjny (ST), służący do komunikacji pomiędzy CSZ oraz SSO, a także do komunikacji z innymi współpracującymi systemami komputerowymi (licznik osi, blokada liniowa). Dla każdej konfiguracji należy odpowiednio skonfigurować odpowiedni podsystem transmisyjny ST.

3.1.3 Elementy, z których zbudowany jest standardowy centralny system zależnościowy CSZ

W ramach centralnego systemu zależnościowego CSZ jednostki bezpiecznych sterowników BSA i BSB (komputer A i B) wykonują funkcje zależnościowe równolegle. Jednostka serwisowa (JS) (komputer C) wykonuje takie operacje, jak wejścia/wyjścia z/do centrum sterowania i systemu sterowników obiektowych (korzystając z systemu transmisyjnego). Interfejsy bezpiecznych sterowników A i B równocześnie wysyłają informację otrzymaną od centrum sterowania i systemu sterowników obiektowych i odbierają informacje wysłane przez centrum sterowania i system sterowników obiektowych.

Komputer zależnościowy CZ systemu zmiany oprogramowania powinien współpracować także ze sterownikami obiektowymi o budowie rozproszonej, stosowanymi przez zarządcę infrastruktury w poprzednich generacjach systemu komputerowego. Taka konfiguracja może wystąpić jedynie na tych stacjach, gdzie zainstalowano już wcześniej sterowniki systemu zabudowanego i zachodzi potrzeba wymiany komputera zależnościowego (na przykład ze względu na konieczność dodania interfejsu do ERTMS).

Program sterujący standardowego systemu zależnościowego realizuje:

– przetwarzanie prawidłowych sterowań z systemu nadrzędnego na rozkazy, które są bezpiecznie wysyłane do zwrotnic, sygnalizatorów, urządzeń sterowania zaporami itp.,

– blokowanie dostępu do obiektów, które biorą udział w przebiegu, dla użycia ich w innych przebiegach,

– zwalnianie zamkniętych obiektów po zakończeniu przejazdu przez pociąg.

Przygotowanie aplikacji zmiany oprogramowania zależnościowego dla dowolnej stacji powinno polegać na wprowadzeniu danych geograficznych stacji, charakterystyki obiektów przytorowych i powiązaniu obiektów logicznych z obwodami torowymi, nie ma potrzeby wprowadzania informacji o zależnościach. Podobnie wygląda zmiana oprogramowania podczas przebudowy stacji (fazowanie).

Testowanie funkcjonalne nowej lub zmienionej aplikacji komputera zależnościowego można przeprowadzić przed instalacją na obiekcie, wykorzystując symulator sterowników obiektowych oraz obiektów stacyjnych. W ten sposób sprawdzić można wszystkie zależności w systemie (tablica zależności, tablica wykluczeń, tablica sygnałów). Przyjęty sposób symulacji pozwala na sprawdzenie ostatecznej wersji systemu oraz wszystkich zależności w warunkach laboratoryjnych, bez konieczności powtarzania

testów na obiekcie.

Na obiekcie należy wykonać te testy, które wynikają z konkretnych uwarunkowań terenu, to znaczy przyporządkowanie obiektów stacyjnych do ich reprezentacji w komputerze zależnościowym, sterownikach obiektowych i odpowiednim systemie, poprawność połączeń do obiektów oraz interfejsy do innych systemów współpracujących.

3.1.4 Funkcjonalność dodatkowa sterowników obiektowych SO

W oprogramowaniu systemu sterowników obiektowych SO zaimplementowana jest z reguły dodatkowa warstwa przetwarzania, która umożliwia znacznie szybszą realizację zależności między obiektami, wykorzystywaną między innymi do implementacji takich funkcji, jak:

- wygaszanie sygnału zezwalającego na semaforze po zajęciu odcinka za semaforem (szybsza reakcja),
- uzależnienie przestawiania zwrotnicy od niezajętości odcinka (użyteczne przy sterowaniu lokalnym),
- funkcji blokady liniowej.

Funkcje diagnostyczne systemu komputerowego z nowym oprogramowaniem realizuje się poprzez**:**

- ciągłą diagnostyka pracy systemu,
- rejestrację zdarzeń i poleceń,
- rejestrację stanów.

Elementami operacyjnymi i ludzkimi są: zabudowa, testowanie, udział w odbiorach, serwis, przygotowanie wytycznych do eksploatacji i utrzymania wraz z przeszkoleniem pracowników użytkownika (które leżą po stronie Wykonawcy), natomiast odbiór, eksploatacja i utrzymanie leżą po stronie pracowników zarządcy infrastruktury.

3.1.5 Granice systemu z uwzględnieniem innych systemów, z którymi system ten wzajemnie oddziałuje

System komputerowy z zabudowaną zmianą oprogramowania może graniczyć z następującymi urządzeniami:

- Systemem samoczynnej sygnalizacji przejazdowej (SSP),
- Systemem Nadrzędnej Zdalnej Kontroli.

Powiązanie z urządzeniami zewnętrznymi realizowane jest poprzez specjalnie

dedykowane do tego celu moduły współpracy - **interfejsy**.

Na szlaku system komputerowy graniczy z systemem SSP poprzez interfejs przekaźnikowy lub komputerowy.

3.1.6 Interfejsy fizyczne (systemy, z którymi system ten wzajemnie oddziałuje) i funkcjonalne

Samoczynna Blokada Liniowa może współpracować z dowolnymi urządzeniami stacyjnymi srk poprzez:

- Interfejs przekaźnikowy,
- Interfejs komputerowy,
- Interfejs przekaźnikowo – komputerowy,
- Kombinacja powyższych interfejsów.

Zespół zidentyfikował następujące interfejsy funkcjonalne:

a) styk przewoźnik kolejowy – zarządca infrastruktury, w tym ustalenia w zakresie rozkładu jazdy,

b) styk ruch kolejowy – ruch drogowy,

c) styk zarządca infrastruktury – ośrodek szkolenia pracowników bezpośrednio związanych z bezpieczeństwem ruchu kolejowego,

d) styk pion utrzymaniowy – pion kadrowy w zakresie rekrutacji nowych pracowników i nadzoru szkoleniowego.

3.1.7 Otoczenie systemu

Otoczeniem systemu jest istniejąca infrastruktura kolejowa, posiadająca charakterystykę zdefiniowaną w dokumentacji zarządcy infrastruktury w zakresie charakterystyk linii kolejowych.

3.1.8 Istniejące środki bezpieczeństwa i definicja wymogów bezpieczeństwa

Jako istniejące środki bezpieczeństwa Zespół oceniający określił wszelkie regulacje wewnętrzne i procedury SMS obowiązujące w podmiocie kolejowym, a także adekwatne przepisy, w tym w zakresie prowadzenia szkoleń i autoryzacji na określone stanowiska pracy. Definicja wymogów bezpieczeństwa podana została w rejestrze zagrożeń.

3.1.9 Założenia określające progi mające zastosowanie do oceny ryzyka

Zespół ocenia przedmiotową zmianę na etapie planowania jej wdrożenia.

3.2 Identyfikacja zagrożeń

Zespół przeanalizował materiał dotyczący zaprojektowania i zainstalowania, podlegającego zmianie (nowego) oprogramowania w eksploatowanym systemie urządzeń komputerowych, dostosowując go do wymuszonych czynnikami zewnętrznymi zmian sprzętowych oraz współpracy z innymi wdrażanymi systemami nadzoru i sterowania ruchem kolejowym (np.: ERTMS/ETCS odpowiedniego poziomu) dla określonych węzłów, stacji i odcinków linii, która ma bezpośredni wpływ na poprawę bezpieczeństwa systemu kolejowego i realizowana jest w ramach obowiązującej umowy.

Zespół zidentyfikował jedno zagrożenie związane z zasadniczo dopuszczalnym ryzykiem – brak autoryzacji personelu.

Zespół zidentyfikował następujące obszary zagrożeń związane z przedmiotową zamianą:

- niedostateczne przeszkolenie pracowników w zakresie obsługi systemu,
- brak odpowiednich kwalifikacji i doświadczenia pracowników wykonawcy,
- niezgodna z projektem zabudowa hardware'u (błąd ludzki),
- zadziałanie urządzeń srk, umożliwiające podanie sygnału zezwalającego dla przebiegów sprzecznych,
- nieprawidłowe działanie urządzeń srk w skutek przeprowadzonej aktualizacji oprogramowania,
- brak możliwości integracji urządzeń srk w skutek niewłaściwej implementacji funkcji oprogramowania,
- uszkodzenia urządzeń przytorowych srk oraz okablowania,
- błędy w oprogramowaniu systemu komputerowego nieujawnione w czasie testów wewnętrznych, testów funkcjonalno-integracyjnych i sprawdzeń komisyjnych,
- nieprawidłowe działanie urządzeń komputerowych, powodujące nieosłonięcie sygnałem „Stój" na semaforze stacyjnym, spowodowane prowadzonymi pracami budowlanymi – przy niezastosowaniu się do przepisów kolejowych,
- niestosowanie się wykonawcy robót do zapisów regulaminu tymczasowego prowadzenia ruchu pociągów oraz przepisów wewnętrznych zarządcy infrastruktury kolejowej, skutkujące zagrożeniem bezpieczeństwa ruchu pociągów.

Ponieważ zdaniem zespołu oceniającego wyżej wymienione zagrożenia są stanami mogącymi prowadzić do wypadku w kontekście analizowanej zmiany, zostaną one ujęte i opisane w rejestrze zagrożeń.

3.3 Tworzenie i prowadzenie rejestru zagrożeń

Zespół oceniający zidentyfikował zagrożenia związane z wprowadzaną zmianą przy uwzględnieniu ograniczeń determinujących ocenę ryzyka (etap planowania zmiany) oraz odnotował je w rejestrze zagrożeń (patrz: Tabela Nr 2 *Rejestr zagrożeń – karta oceny ryzyka dla przedmiotowej zmiany*).

4. Ocena ryzyka

4.1 Wybór zasady akceptacji ryzyka

Zespół oceniający uznał, że dopuszczalność ryzyka dotyczącego zdefiniowanego systemu będzie zbadana przez zastosowanie kodeksów postępowania (tj. regulacji i norm uznanych w kolejnictwie, przepisów krajowych i regulacji wewnętrznych dostępnych dla organów oceny adekwatnych z punktu widzenia nadzoru nad zidentyfikowanymi zagrożeniami) oraz szacowanie i wycenę jawnego ryzyka według przyjętej przez podmiot metody FMEA. Wybór zastosowanej zasady akceptacji ryzyka w odniesieniu do zagrożeń określono w rejestrze zagrożeń. W rejestrze zagrożeń wskazano również wymogi bezpieczeństwa oraz dowody ich spełnienia.

Tabela Nr 1 **Ocena ryzyka dla zidentyfikowanych zagrożeń metodą FMEA**

Nr	*Zidentyfikowane zagrożenia*	Skutek	Pw	Pd	Ps	*RPN*	*Zalecane dodatkowe środki/wymogi bezpieczeństwa*	*Odpowiedzialny*	*Termin realizacji*	Pw	Pd	Ps	*RPN*
1	Braki w szkoleniu personelu służb eksploatacyjno – utrzymaniowych	Incydent	3	5	4	**60**							
2	Nieodpowiednia, niedostosowana do zmienionych warunków organizacja pracy służb eksploatacyjno - utrzymaniowych	Incydent	5	4	4	**80**	Dodatkowy audyt	Audytor, kierownik jednostki	Po zmianie	3	2	4	**24**
3	Niewłaściwa autoryzacja personelu służb eksploatacyjno - utrzymaniowych	Incydent	5	7	4	**140**	Dodatkowy audyt	Audytor, kierownik jednostki	Po zmianie	3	4	6	**72**
4	Nieprawidłowe działanie urządzeń srk w skutek przeprowadzonej aktualizacji oprogramowania	Poważny wypadek	4	7	10	**280**	Praca na symulatorze, dodatkowe testy	komisja odbioru kierownik jednostki	natychmiastowy	2	6	10	**120**
5	Brak możliwości integracji urządzeń srk w skutek niewłaściwej implementacji funkcji oprogramowania	Poważny wypadek	4	7	10	**280**	Praca na symulatorze, dodatkowe testy	komisja odbioru kierownik jednostki	natychmiastowy				
6	Niestosowanie się wykonawcy robót do zapisów „Regulaminu tymczasowego prowadzenia ruchu w czasie wykonywania robót" oraz regulacji wewnętrznych zarządcy infrastruktury kolejowej	Wypadek	4	3	8	**96**	Pouczenia, kontrole kwartalne	kontroler	Praca ciągła	2	3	8	**48**
7	Błędy w aktualizacji oprogramowania systemu komputerowego (na poziomie aplikacji zależnościowych) niewychwycone w czasie odpowiednich testów i sprawdzeń komisyjnych	Poważny wypadek	4	8	10	**320**	Dodatkowy audyt, testy– odbiór techniczny	Audytor, komisja odbioru kierownik jednostki	natychmiastowy	2	3	10	**60**

Objaśnienia do metody FMEA (szczegóły – patrz ZAŁĄCZNIK):
RPN (0-23) – ryzyko dopuszczalne pomijalne; niewymagany zwiększony nadzór
RPN (24-63) – ryzyko dopuszczalne akceptowalne; wymagany zwiększony nadzór bezpośredniego przełożonego RPN (64-124) – ryzyko dopuszczalne; wymagany zwiększony nadzór kierownika jednostki organizacyjnej
RPN (125-179) – ryzyko tolerowalne; należy określić dodatkowe środki kontroli ryzyka i wprowadzić je w ramach działań zapobiegawczych (kierownik jednostki organizacyjnej)
RPN (180-1000) – ryzyko nieakceptowalne; zaprzestanie prowadzenia prac lub wprowadzenie natychmiastowych działań korygujących i zapobiegawczych (kierownik jednostki organizacyjnej w porozumieniu z kierownictwem firmy lub bezpośrednie
działanie kierownictwa firmy)

Tabela Nr 2 **Rejestr zagrożeń – karta oceny ryzyka dla przedmiotowej zmiany**

Lp.	Obszar ryzyka	Rodzaj zagrożenia	Źródło/ przyczyna zagrożenia	Ewentualne maksymalne skutki	Zasada akceptacji ryzyka	Środki/ wymogi bezpieczeństwa	Działania mające na celu wdrożenie wymogów bezpieczeństwa	Wykazanie zgodności z wymogami/ dowody ich zrealizowania	Podmiot/osoby odpowiedzialne	Status zagrożenia/ czy zagrożenie przeniesione do podmiotu trzeciego?
1	2	3	4	5	6	7	8	9	10	11
1.	Dyżurni ruchu/obsługa	Brak precyzyjnych uregulowań w dokumentacji technicznej lub w regulacjach wewnętrznych	Nieprzestrzeganie norm i przepisów	Poważny wypadek kolejowy	Kodeks Postępowania	Dz. U. 2015.360, instrukcje: prowadzenia ruchu, sygnalizacji, urządzeń komputerowych	Audyty, kontrole, bieżący nadzór	Zatwierdzenie planów, raporty z audytów	Audytor, bezpośredni przełożony	Kontrolowalny/ Nie
2.		Niewłaściwa obsługa urządzeń komputerowych	brak odpowiednich uregulowań	Poważny wypadek kolejowy	Kodeks Postępowania	Dz. U. 2015.360, Dz. U. 2015.46, RTS, Instrukcje obsługi urządzeń komputerowych srk	Audyty, kontrole, bieżący nadzór, szkolenia	Zatwierdzenie planów, raporty z audytów, protokoły odbiorów	Audytor, bezpośredni przełożony, komisje odbiorcze	Kontrolowalny /Nie
3.	Degradacja infrastruktury	Niewłaściwe przeprowadzenie badań diagnostycznych urządzeń komputerowych	Nieprzestrzeganie norm, instrukcji	Incydent kolejowy	Kodeks Postępowania	Obowiązujące Instrukcje dla urz. komputerowych, DTR	Audyty, kontrole, bieżący nadzór	Dokumentacja badań diagnostycznych, zatwierdzenie planów, raporty z audytów, protokoły	Audytor, bezpośredni przełożony,	Kontrolowalny/ Nie
4.		Nieprawidłowo prowadzona obsługa techniczna urządzeń komputerowych	Nieprzestrzeganie norm, instrukcji	Incydent kolejowy	Kodeks Postępowania	Obowiązujące Instrukcje dla urz. komputerowych, DTR	Szkolenia, audyty, kontrole, bieżący nadzór	Dokumentacja badań diagnostycznych, zatwierdzenie planów, raporty z audytów, protokoły	Bezpośredni przełożony, audytor	Kontrolowalny/ Nie
5.	Personel	Braki w szkoleniu personelu służb eksploatacyjno-utrzymaniowych	Niedopełnienie obowiązków Błąd ludzki	Incydent kolejowy	Jawne Ryzyko (FMEA)	Bieżący nadzór na podstawie (*), pouczenia, szkolenia, autoryzacja	Egzamin autoryzacyjny, audyty, kontrole	Zatwierdzenie planów, raporty z audytów, dokumentacja autoryzacji	Audytor, bezpośredni przełożony	Kontrolowalny/ Nie

Lp.	Obszar ryzyka	Rodzaj zagrożenia	Źródło/ przyczyna zagrożenia	Ewentualne maksymalne skutki	Zasada akceptacji ryzyka	Środki/ wymogi bezpieczeństwa	Działania mające na celu wdrożenie wymogów bezpieczeństwa	Wykazanie zgodności z wymogami/ dowody ich zrealizowania	Podmiot/osoby odpowiedzialne	Status zagrożenia/ czy zagrożenie przeniesione do podmiotu trzeciego?
1	2	3	4	5	6	7	8	9	10	11
6.		Nieodpowiednia, niedostosowana do zmienionych warunków organizacja pracy służb eksploatacyjno-utrzymaniowych	Niedopełnienie obowiązków Błąd ludzki	Incydent kolejowy	Jawne Ryzyko (FMEA)	Bieżący nadzór na podstawie (*)..., szkolenia	Audyty, kontrole	Zatwierdzenie planów, raporty z audytów	Audytor, bezpośredni przełożony	Kontrolowalny/ Nie
7.		Niewłaściwa autoryzacja personelu służb eksploatacyjno-utrzymaniowych	Niedopełnienie obowiązków Błąd ludzki	Incydent kolejowy	Jawne Ryzyko (FMEA)	Bieżący nadzór na podstawie(*)...	Kontrole, Audyty	Zatwierdzenie planów, raporty z audytów	Audytor, bezpośredni przełożony	Kontrolowalny/ Nie
8.		Brak autoryzacji personelu służb eksploatacyjno-utrzymaniowych	Niedopełnienie obowiązków	Wypadek kolejowy	Zasadniczo dopuszczalne ryzyko					
9.	URZĄDZENIA KOMPUTEROWE	Przyjęcie błędnej koncepcji dla Projektu Wykonawczego zmian w oprogramowaniu komputerowych urządzeń sterowania ruchem kolejowym	Nieprzestrzeganie norm, wytycznych projektowania. Błąd ludzki	Incydent kolejowy	Kodeks Postępowania	Obowiązujące Instrukcje dla urz. komputerowych, DTR	Audyty, analiza planów	Raporty z audytów, dokumentacja autoryzacji, zatwierdzenie planów	Audytor, bezpośredni przełożony, osoba zatwierdzająca plany	Kontrolowalny/ Nie
10.		Niewłaściwe wykonanie prac związanych ze zmianą aplikacji oprogramowania	Nieprzestrzeganie norm, wytycznych programowania. Błąd ludzki	Incydent kolejowy	Kodeks Postępowania	Obowiązujące Instrukcje typu Ie- dla urz. komputerowych	Audyty, analiza planów, analiza projektów technicznych, przeprowadzenie testów	Raporty z audytów, zatwierdzenie planów, dokumentacja odbiorów, w tym testów	Audytor, bezpośredni przełożony, komisje odbiorcze	Kontrolowalny/ Nie

Lp.	Obszar ryzyka	Rodzaj zagrożenia	Źródło/ przyczyna zagrożenia	Ewentualne maksymalne skutki	Zasada akceptacji ryzyka	Środki/ wymogi bezpieczeństwa	Działania mające na celu wdrożenie wymogów bezpieczeństwa	Wykazanie zgodności z wymogami/ dowody ich zrealizowania	Podmiot/osoby odpowiedzialne	Status zagrożenia/ czy zagrożenie przeniesione do podmiotu trzeciego?
1	2	3	4	5	6	7	8	9	10	11
11.		Nieprawidłowe działanie urządzeń srk w skutek przeprowadzonej aktualizacji oprogramowania (w tym: powodujące nie osłonięcie sygnałem „Stój" na semaforach stacyjnych, nie ostrzeżenie i niezabezpieczenie użytkowników przejazdów uzależnionych, itp.)	Nieprzestrzeganie norm Niedopełnienie obowiązków Błąd ludzki	Poważny wypadek kolejowy	a) Kodeks Postępowania b) Jawne Ryzyko (FMEA)	Ad a) Dz. U. 2015.360, instrukcje: prowadzenia ruchu, sygnalizacji, urządzeń komputerowych Ad. b) szkolenia na symulatorze	Audyty, odbiory, testy	Protokoły z testów odbiorów technicznych, końcowych, raporty z audytów	Audytor, komisja odbiorcza	Kontrolowalny/ Nie
12.		Brak możliwości integracji urządzeń srk w skutek niewłaściwej implementacji funkcji oprogramowania	Nieprzestrzeganie norm Niedopełnienie obowiązków Błąd ludzki	Poważny wypadek kolejowy	a) Kodeks Postępowania b) Jawne Ryzyko (FMEA)	Dz. U. 2015.360, instrukcje: prowadzenia ruchu, sygnalizacji, SBL Ad b) szkolenia na symulatorze	Odbiory techniczne, testy, audyty	Protokoły z testów odbiorów technicznych, końcowych, raporty z audytów	Audytor, komisja odbiorcza	Kontrolowalny/ Nie
13.		Niestosowanie się wykonawcy robót do zapisów „Regulaminu tymczasowego prowadzenia ruchu w czasie wykonywania robót" oraz regulacji wewnętrznych zarządcy infrastruktury kolejowej	Niedopełnienie obowiązków Błąd ludzki	Poważny wypadek kolejowy	Jawne Ryzyko (FMEA)	Odprawy, pouczenia, szkolenie wewnętrzne Wykonawcy	Kontrole i audyty	Protokoły pokontrolne, raporty z audytów	Audytor, kontroler, osoba nadzorująca przebieg prac ze strony inwestora	Kontrolowalny/ Nie

14.		Błędy w aktualizacji oprogramowania systemu urządzeń komputerowych (na poziomie aplikacji zależnościowych) niewychwycone w czasie odpowiednich testów i sprawdzeń komisyjnych	Niedopełnienie obowiązków Błąd ludzki	Poważny Wypadek kolejowy	Jawne Ryzyko (FMEA)	Bieżący nadzór na podstawie (*), autoryzacja, praca na symulatorze	Odbiory techniczne, egzamin autoryzacyjny	Zatwierdzenie planów, raporty z: audytów, powtórnej oceny zmiany, świadectwa szkoleń i egzaminów, dokumentacja autoryzacji,	Kierownik jednostki, komisja odbiorcza, kierownik działu szkoleń	Kontrolowalny/ Nie

Objaśnienia:

Dz. U. 2015.46 – rozporządzenie Ministra Infrastruktury i Rozwoju w sprawie pracowników zatrudnionych na stanowiskach bezpośrednio związanych z prowadzeniem i bezpieczeństwem ruchu kolejowego oraz z prowadzeniem określonych rodzajów pojazdów kolejowych

Dz. U 2015.360 – rozporządzenie Ministra Infrastruktury w sprawie ogólnych warunków prowadzenia ruchu kolejowego i sygnalizacji PUK – Protokół Ustaleń Końcowych

RTS – Regulamin Techniczny Stacji

(*)- wskazówka autorów - *należy wymienić procedurę/instrukcję/regulamin/wytyczne, itp., na podstawie której/go zespół oceniający stwierdza, że środki bezpieczeństwa w nich zapisane gwarantują utrzymywanie ryzyka dla zidentyfikowanego zagrożenia na poziomie dopuszczalnym.*

4.2 Lista wymogów bezpieczeństwa

1) Szkolenia dyżurnych ruchu/obsługi na symulatorach,
2) Szkolenia zawodowe pracowników,
3) Autoryzacja pracowników,
4) Szkolenie pracowników w zakresie serwisowania i utrzymania zabudowanego oprogramowania dla urządzeń komputerowych srk.
5) Szkolenie pracowników działu eksploatacji ze znajomości i obsługi zabudowanego oprogramowania dla urządzeń komputerowych srk,
6) Aktywny udział w testach fabrycznych, technicznych, funkcjonalno-integracyjnych zabudowanego oprogramowania dla urządzeń komputerowych srk,
7) Odbiór zabudowanego oprogramowania dla urządzeń komputerowych srk ,
8) Przekazanie do wstępnej eksploatacji zabudowanego oprogramowania dla urządzeń komputerowych srk,
9) Przeprowadzenie oceny znaczenia zmiany na etapie eksploatacji wstępnej.

4.3 Wykazanie zgodności z wymogami

W rejestrze zagrożeń dla przedmiotowej zmiany zespół określił wykazanie zgodności z wymogami bezpieczeństwa . Polega ono na przedstawieniu wszelkich zdefiniowanych w rejestrze zagrożeń dokumentów, takich jak: świadectwa odbytych szkoleń, protokoły z egzaminów, dokumentacja procesu autoryzacji pracowników, protokoły odbioru urządzeń po modernizacji, raporty z audytów.

5. Wnioski

5.1 Z uwagi na duży wpływ kryteriów innowacyjności, złożoności oraz skutki awarii systemu Zespół oceniający Wnioskodawcy stwierdził, iż zmiana jest zmianą znaczącą.

5.2 Z uwagi na znaczenie zmiany Zespół zidentyfikował najważniejsze zagrożenia wynikające z charakteru wprowadzonej zmiany.

5.3 Zespół określił podstawowe elementy systemu podlegające zmianie i podmioty/stanowiska odpowiedzialne za realizację zmiany w danym zakresie.

5.4 Zespół wskazał najważniejsze, zdaniem Zespołu, interfejsy, które wymagają nadzoru ze strony zarządcy infrastruktury.

5.5 Zespół stwierdził, że możliwa jest akceptacja ryzyka opierająca się na korzystaniu z kodeksów postępowania oraz szacowaniu i wycenie jawnego ryzyka, tak aby zagwarantować kompleksowe nadzorowanie ryzyka i jego utrzymanie na dopuszczalnym poziomie.

5.6 W wyniku przeprowadzonej analizy (w zakresie ograniczeń determinujących ocenę ryzyka badanego systemu) dla poszczególnych zagrożeń określono potencjalne skutki wprowadzonej zmiany, środki i wymogi bezpieczeństwa oraz

podmioty odpowiedzialne za ich stosowanie wraz z dokumentami to potwierdzającymi (wykazanie zgodności z wymogami bezpieczeństwa). Wyniki tej pracy zapisano w rejestrze zagrożeń.

5.7 Za dopuszczalne uważa się ryzyka dla zagrożeń wynikających z przedmiotowej zmiany kontrolowanych za pomocą kodeksów postępowania, uwzględniając zapisy Rozporządzenia Wykonawczego Komisji (UE) 402/2013 z dnia 30 kwietnia 2013 r. w sprawie wspólnej metody oceny bezpieczeństwa w zakresie wyceny i oceny ryzyka i uchylającego Rozporządzenie (WE) nr 352/2009.

5.8 Zespół stwierdza, iż spełnienie wskazanych w opracowaniu i ujętych w rejestrze zagrożeń wymogów bezpieczeństwa zapewni bezpieczną integrację systemu z całym systemem kolejowym.

ZAŁĄCZNIK

badanie jawnego ryzyka metodą FMEA

Tabela Nr 4 **Wykaz i opis parametrów stosowanych w metodzie FMEA**

Waga	Parametr wystąpienia (Pw)
1	Prawie niewyobrażalne, że zagrożenie wystąpi.
2	Bardzo małe prawdopodobieństwo. Zagrożenia nie występowały w trakcie innych, podobnych zadań realizowanych przez wykonawcę.
3	Małe prawdopodobieństwo. Występowały pojedyncze zagrożenia w trakcie innych, podobnych zadań realizowanych przez wykonawcę.
4 - 6	Średnie prawdopodobieństwo. Zagrożenia występowały czasami w trakcie innych, podobnych zadań realizowanych przez wykonawcę.
7 - 8	Duże prawdopodobieństwo. Zagrożenia występowały często w trakcie innych, podobnych zadań realizowanych przez wykonawcę.
9- 10	Bardzo duże prawdopodobieństwo. Zagrożenia występowały bardzo często w trakcie innych, podobnych zadań realizowanych przez wykonawcę.
Waga	**Parametr detekcji (Pd)**
1 - 2	Wykrycie zagrożenia jest pewne. Wszystkie środki kontroli ryzyka funkcjonują prawidłowo.
3 - 4	Możliwość wykrycia zagrożenia jest wysoka. Stosowane są środki kontroli ryzyka pozwalające na wykrycie zagrożenia z dużym prawdopodobieństwem. 3 – podmioty nadzorujące ryzyko mają już doświadczenie, 4 – podmioty nadzorujące ryzyko mają małe lub żadne doświadczenie.
5 - 6	Średnia wykrywalność zagrożenia. Środki kontroli ryzyka częściowo nie funkcjonują (np. są częściowo nie przestrzegane). 5 – jeszcze żadne zagrożenia się nie ziściły, 6 – dane zagrożenie już wystąpiło.
7 - 8	Wykrycie zagrożenia jest trudne. Środki kontroli nie funkcjonują (np. nie są przestrzegane). 7 – jeszcze żadne zagrożenia się nie ziściły, 8 – dane zagrożenie już wystąpiło.
9 - 10	Wykrycie zagrożenia jest niezmiernie trudne lub niemożliwe. Brak jest środków kontroli ryzyka. 9 – jeszcze żadne zagrożenia się nie ziściły, 10 – dane zagrożenie już wystąpiło.

Waga	Parametr skutków (Ps)
1	Zagrożenie nie powoduje skutków dla transportu kolejowego. Bez kosztów.
2 - 3	Zagrożenie może powodować nieznaczne ograniczenia ruchu kolejowego, nieznaczne straty ekonomiczne (2 – do 10 000 EUR, 3 – do 50 000 EUR).
4 - 6	Zagrożenie może powodować incydenty kolejowe oraz wypadki niewielkie skutki dla zdrowia osób (osoby ranne). Straty materialne (4 – do 100 000 EUR i/lub 1 osoba lekko ranna, 5 – do 250 000 EUR i/lub 2-4 osoby lekko ranne 6 – do 500 000 EUR i/lub więcej niż 4 osoby lekko ranne).
7 - 8	Zagrożenie może powodować wypadki kolejowe, poważne skutki dla zdrowia osób (osoby ciężko ranne). Straty materialne (7 – do 750 000 EUR i/lub 1 osoba ciężko ranna, 8 – do 1 000 000 EUR i/lub od 2 do 4 osób ciężko rannych).
9 - 10	Zagrożenie może powodować poważne wypadki kolejowe, poważne skutki dla zdrowia i życia osób (osoby zabite i ciężko ranne). Straty materialne (9 – do 2 Mln EUR i/lub więcej niż 4 osoby ciężko ranne, 10 – powyżej 2 Mln EUR i/lub 1 lub więcej osoba zabita).