Europejska Agencja Kolejowa

Przykłady oceny ryzyka i ewentualnych narzędzi pomocniczych do rozporządzenia w sprawie wspólnych metod oceny bezpieczeństwa (CSM)

Nr referencyjny w ERA:	ERA/GUI/02-2008/SAF
Wersja w ERA:	1.1
Data:	06/01/2009

Dokument opracowany przez	Europejska Agencja Kolejowa Marc LEFRANCQ, 120 BP 20392 F-59307 Valenciennes Cedex Francja
Typ dokumentu:	Guide
Status dokumentu	Public

	Imię i Nazwisko	**Funkcja**
Dopuszczone do druku przez	Marcel VERSLYPE	Dyrektor wykonawczy
Przeglądu dokonali	Anders LUNDSTRÖM Thierry BREYNE	Kierownik Jednostki ds. Bezpieczeństwa Kierownik Działu ds. Oceny Bezpieczeństwa
Napisane przez (autor)	Dragan JOVICIC	Jednostka ds. Bezpieczeństwa – Kierownik projektu

European Railway Agency ● Marc LEFRANCQ, 120 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

INFORMACJE NA TEMAT DOKUMENTU

Spis poprawek

Tabela 1: Status dokumentu

Wersja Data	Autor/ Autorzy	Numer części	Opis zmian
Stary tytuł i układ dokumentu: *„Wytyczne stosowania Zaleceń w sprawie pierwszego pakietu wspólnych metod oceny bezpieczeństwa (CSM)”*			
Wersja wytycznych 0.1 15/02/2007	Dragan JOVICIC	Wszystkie	Pierwsza wersja „wytycznych stosowania” powiązana z wersją 1.0 „pierwszego pakietu zaleceń CSM”. Jest to również pierwsza wersja dokumentu przekazanego grupie roboczej ds. CSM do formalnego przeglądu.
Wersja wytycznych 0.2 07/06/2007	Dragan JOVICIC	Wszystkie	Zmiana układu dokumentu tak, by dopasować go do układu wersji 4.0 zaleceń CSM. Aktualizacja a formalny proces przeglądu wersji 1.0 zaleceń, przeprowadzony przez grupę roboczą ds. CSM.
		Wszystkie	Aktualizacja dokumentu dodatkowymi informacjami zebranymi podczas wewnętrznych spotkań Agencji, a także wnioskami grupy zadaniowej i grupy roboczej ds. CSM na temat opracowania nowych punktów.
		Schemat 1	Modyfikacja schematu przedstawiającego „ramy zarządzania ryzykiem w odniesieniu do pierwszego pakietu wspólnych metod oceny bezpieczeństwa” zgodnie z zaleceniami wynikającymi z przeglądu i terminologią ISO.
Wersja wytycznych 0.3 20/07/2007	Dragan JOVICIC	Załączniki	Zmiana układu załączników i utworzenie nowych. Nowy załącznik zawierający diagramy, które służą jako ilustracja graficzna ułatwiająca czytanie i zrozumienie przewodnika;
		Wszystkie części	Dokonano aktualizacji dokumentu, aby: • jak najbardziej poszerzyć istniejące x części; • szerzej przedstawić, czego dotyczy „wykazanie zgodności systemu z wymogami bezpieczeństwa”; • pokazać związek z modelem V wg CENELEC (tj. schematem 8 a schematem 10 EN 50 126); • dalej określić potrzebę współpracy i koordynacji między różnymi podmiotami sektora kolejowego, których działania mogą mieć wpływ na bezpieczeństwo systemu kolejowego; • wprowadzić objaśnienia w odniesieniu do materiału dowodowego (np. dziennika zagrożeń i uzasadnienia bezpieczeństwa) mającego na celu wykazanie organom dokonującym oceny, że proces oceny ryzyka CSM został właściwie zastosowany; Dokument zaktualizowany również zgodnie z pierwszym przeglądem dokonanym wewnętrznie przez Agencję.
Wersja wytycznych 0.4 16/11/2007	Dragan JOVICIC	Wszystkie części	Dokument zaktualizowany, po formalnym procesie przeglądu, zgodnie z komentarzami otrzymanymi do wersji 0.3 od następujących członków grupy roboczej ds. CSM lub następujących organizacji, i uzgodnionymi telefonicznie: • krajowych organów ds. bezpieczeństwa z Belgii, Hiszpanii, Finlandii, Norwegii, Francji i Danii; • przedsiębiorstwa SIEMENS (członka UNIFE); • zarządcy infrastruktury norweskiej (Jernbaneverket – członka EIM);
Wersja wytycznych 0.5 27/02/2008	Dragan JOVICIC	Wszystkie części	Dokument zaktualizowany zgodnie z komentarzami otrzymanymi do wersji 0.3 od członków grupy roboczej CSM lub organizacji i uzgodnionych podczas rozmów telefonicznych: • Stowarzyszenia Kolei Europejskich (CER) • holenderskiego krajowego organu ds. bezpieczeństwa
		Wszystkie	Dokument aktualizowany zgodnie z podpisaną wersją zaleceń CSM.

European Railway Agency ● Marc LEFRANCQ, 120 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

Tabela 1: Status dokumentu

Wersja Data	Autor/ Autorzy	Numer części	Opis zmian
		części	Dokument aktualizowany zgodnie z komentarzami z wewnętrznego przeglądu Agencji (autorzy komentarzy: Christophe CASSIR i Marcus ANDERSSON).
		Wszystkie części załączniki	Zmiana numeracji punktów w dokumencie stosownie do zalecenia. Dołączenie przykładów stosowania zaleceń CSM.
Nowy tytuł i układ dokumentu: ***„Przewodnik stosowania rozporządzenia CSM”***			
Wersja przewodnika 0.1 23/05/2008	Dragan JOVICIC	Wszystkie	Pierwsza wersja dokumentu powstała w wyniku podziału wersji 0.5. „wytycznych stosowania” na dwa uzupełniające się dokumenty.
Wersja przewodnika 0.2 03/09/2008	Dragan JOVICIC	Wszystkie	Aktualizacja dokumentu zgodna z: • rozporządzeniem CSM Komisji Europejskiej {Ref. 3}; • komentarzami zebranymi podczas warsztatów przeprowadzonych w dniu 1 lipca 2008 r. z udziałem członków Komitetu ds. Interoperacyjności i Bezpieczeństwa Kolei (RISC); • komentarzami członków grupy roboczej CSM (krajowych organów ds. bezpieczeństwa z Norwegii, Finlandii, Zjednoczonego Królestwa i Francji, Stowarzyszenia Kolei Europejskich, komitetu EIM, Jensa BRABANDA [UNIFE] i Stéphane’a ROMEI [UNIFE])
Wersja przewodnika 1.0 10/12/2008	Dragan JOVICIC	Wszystkie	Aktualizacja dokumentu zgodna z rozporządzeniem CSM Komisji Europejskiej w zakresie wyceny i oceny ryzyka {Ref. 3} przyjęta przez Komitet ds. Interoperacyjności i Bezpieczeństwa Kolei (RISC) na posiedzeniu plenarnym w dniu 25 listopada 2008 r.
Wersja przewodnika 1.1 06/01/2009	Dragan JOVICIC	Wszystkie	Aktualizacja dokumentu zgodnie z komentarzami do rozporządzenia CSM przekazanymi przez służby prawno-lingwistyczne Komisji Europejskiej.

European Railway Agency ● Marc LEFRANCQ, 120 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

Spis treści

European Railway Agency ● Marc LEFRANCQ, 120 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

Spis schematów

European Railway Agency ● Marc LEFRANCQ, 120 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

Spis tabel

European Railway Agency ● Marc LEFRANCQ, 120 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

0. WPROWADZENIE

0.1. Zakres

0.1.1. Niniejszy dokument ma na celu udzielenie dodatkowych wyjaśnień do „rozporządzenia Komisji 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" {Ref. 3}. Rozporządzenie to będzie zwane w niniejszym dokumencie „rozporządzeniem CSM".

0.1.2. Niniejszy dokument nie jest wiążący prawnie i jego treść nie powinna być interpretowana jako jedyny sposób spełnienia wymogów CSM. Niniejszy dokument ma na celu uzupełnienie przewodnika dotyczącego stosowania rozporządzenia CSM {Ref. 4} pod względem sposobu wykorzystania i zastosowania procesu określonego w tym rozporządzeniu. Dokument zawiera dodatkowe praktyczne informacje, które w żadnym stopniu na zobowiązują do przestrzegania procedur i nie ustanawiają prawnie wiążącej praktyki. Informacje te mogą być przydatne dla wszystkich podmiotów[(1)], których działalność może mieć wpływ na bezpieczeństwo systemów kolejowych, i które bezpośrednio lub pośrednio muszą stosować wspólne metody oceny bezpieczeństwa. Niniejszy dokument zawiera przykłady ocen ryzyka oraz narzędzia, które mogą być pomocniczo wykorzystane dla potrzeb wspólnych metod oceny bezpieczeństwa. Podane przykłady mają wyłącznie charakter informacyjno-pomocniczy. Podmioty mogą korzystać z alternatywnych metod lub mogą nadal stosować swoje własne aktualne metody i narzędzia, aby dostosować się do wspólnych metod oceny bezpieczeństwa, jeśli ich zdaniem własne metody i narzędzia są bardziej odpowiednie.
Ponadto przykłady i dodatkowe informacje zamieszczone w niniejszym dokumencie nie są wyczerpujące i nie obejmują wszystkich ewentualnych sytuacji, w stosunku do których proponowane są znaczące zmiany, dlatego też niniejszy dokument ma charakter wyłącznie informacyjny.

0.1.3. Niniejszy dokument informacyjny należy traktować wyłącznie jako dodatkową pomoc przy stosowaniu rozporządzenia CSM. Niniejszy dokument nie zastępuje rozporządzenia CSM, jedynie ma ułatwić stosowanie wspólnych metod oceny bezpieczeństwa i w związku z tym należy odczytywać go w powiązaniu z rozporządzeniem CSM {Ref. 3} i przewodnikiem {Ref. 4}.

0.1.4. Niniejszy dokument został sporządzony przez Europejską Agencję Kolejową (ERA) przy wsparciu ekspertów stowarzyszenia przedsiębiorstw kolejowych i krajowego organu ds. bezpieczeństwa z grupy roboczej CSM. Stanowi on zbiór rozwiniętych pomysłów i informacji zebranych przez Agencję podczas spotkań wewnętrznych oraz spotkań z grupą roboczą i grupami zadaniowymi ds. CSM. W razie potrzeby Agencja dokona przeglądu i aktualizacji dokumentu, aby uwzględnić postęp w zakresie standardów europejskich, a także zmiany rozporządzenia CSM w zakresie oceny ryzyka i ewentualne informacje zwrotne dotyczące doświadczenia w stosowaniu rozporządzenia CSM. Ponieważ podczas opracowywania dokumentu nie jest możliwe podanie harmonogramu jego korekt, pytania o informacje na temat najnowszego wydania należy kierować do Europejskiej Agencji Kolejowej.

---

(1) *Zainteresowanymi podmiotami są podmioty zamawiające, o których mowa w art. 2 lit. r} dyrektywy 2008/57/WE w sprawie interoperacyjności systemu kolei we Wspólnocie lub producenci, wszyscy zbiorczo określeni w rozporządzeniu jako „wnioskodawca" bądź ich dostawcy i usługodawcy.*

European Railway Agency ● Marc LEFRANCQ, 120 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

0.2. Zagadnienia nieobjęte zakresem dokumentu

0.2.1. Niniejszy dokument nie zawiera wskazówek na temat sposobów organizacji, eksploatacji lub projektowania (i produkcji) systemu kolejowego lub jego części. Nie definiuje on również umownych porozumień i ustaleń, które mogą istnieć między niektórymi podmiotami w zakresie stosowania procesu zarządzania ryzykiem. Porozumienia umowne właściwe dla danego projektu wychodzą poza zakres rozporządzenia CSM, jak również dotyczącego go przewodnika i niniejszego dokumentu.

0.2.2. Porozumienia zawarte pomiędzy stosownymi podmiotami, mimo że nie wchodzą w zakres niniejszego dokumentu, mogą być zapisane w stosownych umowach na samym początku projektu, jednak bez naruszania przepisów rozporządzenia CSM. Mogą one obejmować na przykład:

(a) koszty nieodłącznie związane z zarządzaniem ryzykiem w zakresie bezpieczeństwa na interfejsach pomiędzy podmiotami;

(b) koszty, które nie były znane w chwili rozpoczęcia projektu, a które są nieodłącznie związane z przenoszeniem odpowiedzialności za zagrożenia między podmiotami i powiązanych środków bezpieczeństwa

(c) sposoby rozwiązywania konfliktów, które mogą wyniknąć w trakcie projektu;

(d) itp.

W przypadku zaistnienia nieporozumień lub konfliktu pomiędzy wnioskodawcą a podwykonawcami w trakcie realizacji projektu, można powoływać się na stosowne umowy w celu rozstrzygnięcia wszelkich konfliktów.

0.3. Układ dokumentu

0.3.1. Mimo że niniejszy dokument może wydawać się samodzielnym dokumentem, nie zastępuje on rozporządzenia CSM {Ref. 3}. Aby ułatwić wyszukiwanie informacji w niniejszym dokumencie, przytoczony został każdy artykuł rozporządzenia CSM. Jeżeli zachodzi taka potrzeba, dany artykuł jest objaśniany wcześniej w przewodniku stosowania rozporządzenia CSM {Ref. 4}. W kolejnych akapitach zamieszczone zostały natomiast, jeżeli jest to konieczne, dodatkowe informacje ułatwiające lepsze zrozumienie rozporządzenia CSM.

0.3.2. Wybrane fragmenty rozporządzenia Komisji Nr 352/2009 zostały zapisane kursywą i umieszczone w tabelce, tak jak ten tekst. Taki kształt umożliwi łatwe rozróżnienie tekstu rozporządzenia {dokument Ref. 3} od dodatkowych wyjaśnień zawartych w tym dokumencie. Fragmenty Przewodnika w zakresie stosowania rozporządzenia Komisji Nr 352/2009 {dokument Ref. 4} nie zostały umieszczone w tym dokumencie.

0.3.3. Dla zapewnienia czytelności układ niniejszego dokumentu odwzorowuje układ rozporządzenia CSM i powiązanego przewodnika.

0.4. Opis dokumentu

0.4.1. Dokument składa się z następujących części:

(a) rozdział 0. definiuje zakres dokumentu i zawiera listę dokumentów referencyjnych;

European Railway Agency ● Marc LEFRANCQ, 120 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

(b) załącznik I i załącznik II zapewniają dodatkowe informacje odnoszące się do odpowiadających im części rozporządzenia CSM {Ref. 3} i powiązanego przewodnika {Ref. 4};

(c) nowe załączniki zawierają szersze omówienie niektórych szczegółowych zagadnień wraz z przykładami.

0.5. Dokumenty referencyjne

Tabela 2: Zestawienie dokumentów referencyjnych.

{Dokument ref. nr}	Tytuł	Źródło	Wersja
{Ref. 1}	Dyrektywa 2004/49/WE Parlamentu Europejskiego i Rady z dnia 29 kwietnia 2004 r. w sprawie bezpieczeństwa kolei wspólnotowych oraz zmieniająca dyrektywę Rady 95/18/WE w sprawie przyznawania licencji przedsiębiorstwom kolejowym, oraz dyrektywę 2001/14/WE w sprawie alokacji zdolności przepustowej infrastruktury kolejowej i pobierania opłat za użytkowanie infrastruktury kolejowej oraz certyfikację w zakresie bezpieczeństwa (dyrektywa w sprawie bezpieczeństwa kolei)	2004/49/WE Dz.U. L 164 z 30.4.2004, s. 44, sprostowanie w Dz.U. L 220 z 21.6.2004, s. 16.	-
{Ref. 2}	Dyrektywa Parlamentu Europejskiego i Rady 2008/57/WE z dnia 17 czerwca 2008 r. w sprawie interoperacyjności systemu kolei we Wspólnocie	2008/57/WE Dz.U. L 191 z 18.7.2008, s. 1.	-
{Ref. 3}	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	352/2009/WE	dnia 24 kwietnia 2009 r.
{Ref. 4}	Przewodnik stosowania rozporządzenia Komisji w sprawie przyjęcia wspólnej metody oceny bezpieczeństwa w zakresie wyceny i oceny ryzyka, o której mowa w art. 6 ust. 3 lit. a) dyrektywy w sprawie bezpieczeństwa kolei	ERA/GUI/01-2008/SAF	1.0
{Ref. 5}	Dyrektywa Parlamentu Europejskiego i Rady 2008/57/WE z dnia 17 czerwca 2008 r. w sprawie interoperacyjności systemu kolei we Wspólnocie	2008/57/WE Dz.U. L 191 z 18.7.2008, s. 1.	-
{Ref. 6}	System zarządzania bezpieczeństwem – Kryteria oceny przedsiębiorstw kolejowych i zarządców infrastruktury	Kryteria oceny systemu zarządzania bezpieczeństwem Część A. Certyfikaty bezpieczeństwa i zezwolenia	31/05/2007
{Ref. 7}	Zastosowania kolejowe – Łączność, sygnalizacja i systemy sterowania – Programy dla kolejowych systemów sterowania i zabezpieczenia	EN 50129	luty 2003 r.
{Ref. 8}	Zastosowania kolejowe – Specyfikacja nieuszkadzalności, gotowości, obsługiwalności i bezpieczeństwa (RAMS) – Część 1: Norma	EN 50126-1	wrzesień 2006 r.
{Ref. 9}	Zastosowania kolejowe – Specyfikacja niezawodności, dostępności, podatności utrzymaniowej i bezpieczeństwa (RAMS) – Część 2: Wytyczne stosowania normy bezpieczeństwa EN 50126-1	EN 50126-2 (Wytyczne)	wersja ostateczna (sierpień 2006 r.)
{Ref. 10}	Wytyczne ogólne dotyczące oszacowania ryzyka związanego z przewozem kolejami towarów niebezpiecznych	wytyczne OTIF zatwierdzone przez komitet ekspertów ds. przewozu kolejami towarów niebezpiecznych	24 listopada 2005 r.
{Ref. 11}	Kryterium akceptacji ryzyka w odniesieniu do systemów technicznych	Nota 01/08	1.1 (25/01/2008)

European Railway Agency ● Marc LEFRANCQ, 120 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

Tabela 2: Zestawienie dokumentów referencyjnych.

{Dokument ref. nr}	Tytuł	Źródło	Wersja
{Ref. 12}	Jednostka ds. Bezpieczeństwa ERA: System wykonalności – „Podział wymagań bezpieczeństwa (dla podsystemów TSI) i konsolidacja TSI z punktu widzenia bezpieczeństwa” WP1.1 – Ocena wykonalności w zakresie podziału wspólnych wymagań bezpieczeństwa	WP1.1	1.0
{Ref. 13}	„Kolejnictwo – System oznaczania pojazdów szynowych – Część 4: EN 0015380 Część 4: Grupy funkcji”.	EN 0015380 Część 4	

0.6. Standardowe definicje, terminy i skróty

0.6.1. Ogólne definicje, terminy i skróty używane w niniejszym dokumencie można znaleźć w standardowym słowniku.

0.6.2. Nowe definicje, terminy i skróty użyte w niniejszym przewodniku zostały zdefiniowane poniżej.

0.7. Definicje

0.7.1. Zobacz Artykuł 3.

0.8. Terminy i skróty

0.8.1. W części tej zostały zdefiniowane nowe terminy i skróty, które często występują w niniejszym dokumencie.

Tabela 3: Wykaz terminów.

Termin	Definicja
Agencja	Europejska Agencja Kolejowa (ERA)
przewodnik	„przewodnik stosowania rozporządzenia 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”
rozporządzenie CSM	„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” {Ref. 3}

Tabela 4: Wykaz skrótów

Skrót	Znaczenie
CCS	sterowanie
CSM	wspólne metody oceny bezpieczeństwa
CST	wspólne wymagania bezpieczeństwa
KE	Komisja Europejska
ERA	Europejska Agencja Kolejowa

European Railway Agency ● Marc LEFRANCQ, 120 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

Tabela 4: Wykaz skrótów

Skrót	Znaczenie
IM	zarządcy infrastruktury
ISA	niezależny organ ds. oceny bezpieczeństwa
OTIF	Międzyrządowa Organizacja Międzynarodowych Przewozów Kolejami
PCz	państwo członkowskie
NOBO	jednostka notyfikowana
NSA	krajowy organ ds. bezpieczeństwa
QMP	proces zarządzania jakością
QMS	system zarządzania jakością
RISC	Komitet ds. Interoperacyjności i Bezpieczeństwa Kolei
RU	przedsiębiorstwa kolejowe
SMP	proces zarządzania bezpieczeństwem
SMS	system zarządzania bezpieczeństwem
SRT	bezpieczeństwo w tunelach kolejowych
TBC	należy uzupełnić
TSI	techniczne specyfikacje interoperacyjności

European Railway Agency ● Marc LEFRANCQ, 120 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

WYJAŚNIENIE ARTYKUŁÓW ROZPORZĄDZENIA CSM

Artykuł 1. Cel

Artykuł 1 ust 1

Niniejsze rozporządzenie ustanawia wspólną metodę oceny bezpieczeństwa w zakresie wyceny i oceny ryzyka (CSM), o której mowa w art. 6 ust. 3 lit. a) dyrektywy 2004/49/WE.

[G 1] Uznano, że dodatkowe wyjaśnienia nie są konieczne.

Artykuł 1 ust 2

Celem CSM w zakresie wyceny i oceny ryzyka jest zachowanie poziomu bezpieczeństwa kolei wspólnotowych lub jego poprawa, gdy jest to konieczne i praktycznie możliwe. CSM poprawia dostęp do rynku usług przewozów kolejowych dzięki harmonizacji:

(a) procesów zarządzania ryzykiem stosowanych do oceny poziomów bezpieczeństwa i zgodności z wymogami bezpieczeństwa;
(b) wymiany informacji mających znaczenie dla bezpieczeństwa pomiędzy różnymi podmiotami sektora kolejowego w celu zarządzania bezpieczeństwem w ramach różnych interfejsów istniejących w tym sektorze;
(c) dowodów uzyskanych dzięki stosowaniu procesu zarządzania ryzykiem.

[G 1] Uznano, że dodatkowe wyjaśnienia nie są konieczne.

Artykuł 2. Zakres

Artykuł 2 ust 1

CSM w zakresie wyceny i oceny ryzyka ma zastosowanie do wszelkich zmian systemu kolejowego w państwie członkowskim, o których mowa w pkt 2 lit. d) załącznika III do dyrektywy 2004/49/WE, które są uznawane za znaczące w rozumieniu art. 4 niniejszego rozporządzenia. Zmiany takie mogą mieć charakter techniczny, eksploatacyjny lub organizacyjny. W przypadku zmian organizacyjnych, brane są pod uwagę pod uwagę wyłącznie zmiany, które mogą mieć wpływ na warunki eksploatacji.

[G 1] CSM ma zastosowanie do całego systemu kolejowego i obejmuje ocenę następujących zmian w systemach kolejowych, jeżeli w świetle Artykuł 4 ich wycena spowoduje, że będą znaczące:

(a) budowa nowych linii lub zmiany istniejących linii,
(b) wprowadzenie nowych lub zmodyfikowanych systemów technicznych;
(c) zmiany eksploatacyjne (takie jak nowe lub zmienione zasady eksploatacji i procedury utrzymania ruchu);

European Railway Agency ● Marc LEFRANCQ, 120 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

(d) zmiany w obrębie organizacji przedsiębiorstw kolejowych/zarządców infrastruktury.

We wspólnej metodzie oceny bezpieczeństwa termin „system" odnosi się do wszystkich aspektów systemu i obejmuje, między innymi, jego rozbudowę, eksploatację, utrzymanie ruchu itp., aż do momentu wycofania z eksploatacji lub likwidacji.

[G 2] CSM obejmuje znaczące zmiany

(a) „małych i prostych" systemów, które mogą się składać z niewielu technicznych podsystemów lub elementów,
(b) „dużych i bardziej skomplikowanych" systemów (np. takich, w skład których mogą wchodzić stacje i tunele).

Artykuł 2 ust 2

W przypadku gdy znaczące zmiany dotyczą podsystemów strukturalnych, do których ma zastosowanie dyrektywa 2008/57/WE, CSM w zakresie wyceny i oceny ryzyka znajduje zastosowanie:

(a) jeżeli ocena ryzyka jest wymagana w odpowiednich technicznych specyfikacjach interoperacyjności (TSI). W takim przypadku TSI określają, w razie potrzeby, które elementy CSM mają zastosowanie;

(b) aby zapewnić bezpieczną integrację podsystemów strukturalnych, do których mają zastosowanie TSI, z istniejącym systemem, zgodnie z art. 15 ust. 1 dyrektywy 2008/57/WE.

Jednakże, stosowanie CSM w przypadku, o którym mowa w akapicie pierwszym lit. b) nie może prowadzić do wymogów sprzecznych z wymogami, które są określone w odpowiednich TSI i mają charakter obligatoryjny.

Jeżeli jednak stosowanie CSM prowadzi do wymogu sprzecznego z określonym we właściwym TSI, wnioskodawca informuje o tym zainteresowane państwo członkowskie, które może wówczas wystąpić o przegląd TSI zgodnie z art. 6 ust. 2 lub art. 7 dyrektywy 2008/57/WE lub o przyznanie odstępstwa zgodnie z art. 9 tej dyrektywy.

[G 1] Na przykład zgodnie z dyrektywą w sprawie bezpieczeństwa kolei {Ref. 1} i dyrektywą w sprawie interoperacyjności kolei {Ref. 2} nowy rodzaj taboru dla kolei dużych prędkości musi być zgodny z TSI taboru dla kolei dużych prędkości. Mimo że TSI obejmują większość systemu podlegającego ocenie, nie uwzględniają tak istotnego zagadnienia w odniesieniu do kabiny maszynisty jak czynnik ludzki. Dlatego też stosowany jest CSM, aby zagwarantować, że wszystkie możliwe do przewidzenia zagrożenia związane z kwestiami czynnika ludzkiego (czyli interfejsami między maszynistą, taborem a pozostałą częścią systemu kolejowego) są ustalone i w należyty sposób kontrolowane.

European Railway Agency ● Marc LEFRANCQ, 120 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

Artykuł 2 ust 3

Niniejsze rozporządzenie nie ma zastosowania do:

(a) metra, tramwajów i innych systemów kolei lekkiej;

(b) sieci, które są funkcjonalnie wyodrębnione z systemu kolejowego i przeznaczone są tylko na potrzeby pasażerskich przewozów lokalnych, miejskich lub podmiejskich, a także przedsiębiorstw kolejowych prowadzących działalność wyłącznie w obrębie tych sieci;

(c) infrastruktury kolejowej należącej do właścicieli prywatnych, która jest użytkowana wyłącznie w ramach ich własnej działalności w zakresie transportu towarów;

(d) pojazdów zabytkowych działających w sieciach krajowych, pod warunkiem że spełniają one krajowe przepisy i regulacje dotyczące bezpieczeństwa, aby zapewnić bezpieczne działanie tego rodzaju pojazdów;

(e) kolei zabytkowych, muzealnych i turystycznych działających w ramach własnej sieci, łącznie z warsztatami, pojazdami i personelem.

[G 1] Uznano, że dodatkowe wyjaśnienia nie są konieczne.

Artykuł 2 ust 4

Niniejsze rozporządzenie nie ma zastosowania do systemów i zmian, które z dniem wejścia w życie niniejszego rozporządzenia znajdują się na zaawansowanym etapie realizacji w rozumieniu art. 2 lit. t) dyrektywy 2008/57/WE.

[G 2] Uznano, że dodatkowe wyjaśnienia nie są konieczne.

Artykuł 3. Definicje

Do celów niniejszego rozporządzenia, stosuje się definicje zawarte w art. 3 dyrektywy 2004/49/WE.

Stosuje się również następujące definicje:

(1) „ryzyko" oznacza częstotliwość wypadków i incydentów prowadzących do szkody (spowodowanej zagrożeniem) oraz stopień powagi tej szkody (EN 50126-2);

(2) „analiza ryzyka" oznacza systematyczne wykorzystywanie wszystkich dostępnych informacji do identyfikowania zagrożeń i szacowania ryzyka (ISO/IEC 73);

(3) „wycena ryzyka" oznacza procedurę opierającą się na analizie ryzyka, która ma na celu ustalenie, czy osiągnięto poziom dopuszczalnego ryzyka (ISO/IEC 73);

(4) „ocena ryzyka" oznacza całościowy proces obejmujący analizę ryzyka i wycenę ryzyka (ISO/IEC 73);

(5) „bezpieczeństwo" oznacza brak niedopuszczalnego ryzyka szkody (EN 50126-1);

(6) „zarządzanie ryzykiem" oznacza planowe stosowanie polityki, procedur i praktyk zarządczych w ramach zadań dotyczących analizy, wyceny i nadzoru ryzyka (ISO/IEC 73);

(7) „interfejsy" oznacza wszystkie punkty interakcji podczas cyklu życia systemu lub podsystemu, w tym utrzymanie i eksploatację, w których ramach różne podmioty branży kolejowej współpracują ze sobą, aby zarządzać ryzykiem;

(8) „podmioty" oznacza wszystkie strony, które są zaangażowane, bezpośrednio lub na mocy porozumień umownych, w stosowanie niniejszego rozporządzenia zgodnie z 0;

(9) „wymogi bezpieczeństwa" oznacza właściwości bezpieczeństwa (jakościowe lub ilościowe)

European Railway Agency ● Marc LEFRANCQ, 120 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

odnoszące się do systemu i jego eksploatacji (w tym zasady eksploatacji), które są konieczne do spełnienia prawnych lub wewnętrznych celów w zakresie bezpieczeństwa;

(10) „środki bezpieczeństwa" oznacza pakiet działań zmniejszających częstotliwość zagrożeń albo łagodzących ich skutki, który ma na celu osiągnięcie lub utrzymanie dopuszczalnego poziomu ryzyka;

(11) „wnioskodawca" oznacza przedsiębiorstwa kolejowe lub zarządców infrastruktury w ramach środków nadzoru ryzyka, do których wdrażania są oni zobowiązani zgodnie z art. 4 dyrektywy 2004/49/WE; podmioty zamawiające lub producentów, gdy wzywają jednostkę notyfikowaną do zastosowania procedury weryfikacji WE zgodnie z art. 18 ust. 1 dyrektywy 2008/57/WE; lub podmioty składające wnioski o zezwolenie na dopuszczenie pojazdów do eksploatacji;

(12) „raport w sprawie oceny bezpieczeństwa" oznacza dokument zawierający wnioski z oceny przeprowadzonej przez jednostkę oceniającą w odniesieniu do ocenianego systemu;

(13) „zagrożenie" oznacza stan, który może prowadzić do wypadku (EN 50126-2);

(14) „jednostka oceniająca" oznacza niezależną kompetentną osobę, organizację lub podmiot, które przeprowadzają badanie w celu ocenienia, na podstawie dowodów, zdolności systemu do spełnienia wymogów bezpieczeństwa, które się do niego stosują;

(15) „kryteria akceptacji ryzyka" oznacza kryteria, na podstawie których oceniana jest 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;

(16) „rejestr zagrożeń" oznacza dokument, w którym rejestruje się i opatruje odniesieniami zidentyfikowane zagrożenia, związane z nimi środki i źródło zagrożeń oraz wskazuje organizację, która ma nimi zarządzać;

(17) „identyfikacja zagrożeń" oznacza proces wykrywania zagrożeń oraz sporządzanie ich wykazu i opisu (ISO/IEC Guide 73);

(18) „zasada akceptacji ryzyka" oznacza zasady, które są stosowane w celu wyciągnięcia wniosku o dopuszczalności lub niedopuszczalności ryzyka związanego z określonym zagrożeniem lub określonymi zagrożeniami;

(19) „kodeks postępowania" oznacza spisany zbiór zasad, które mogą być wykorzystywane do nadzorowania określonego zagrożenia lub określonych zagrożeń, pod warunkiem ich prawidłowego stosowania;

(20) „system odniesienia" oznacza system, który sprawdził się w praktyce jako system o dopuszczalnym poziomie bezpieczeństwa i z którym można porównywać system oceniany pod kątem dopuszczalności ryzyka;

(21) „szacowanie ryzyka" oznacza proces prowadzący do uzyskania pomiaru poziomu analizowanego ryzyka, na który składają się następujące etapy: analiza częstotliwości, analiza skutków i połączenie tych dwóch typów analiz (ISO/IEC 73);

(22) „system techniczny" oznacza produkt lub zespół produktów, w tym projekt oraz dokumentację wykonawczą i pomocniczą; proces opracowywania systemu technicznego rozpoczyna się od opracowania specyfikacji wymogów, a kończy odbiorem tego systemu; system techniczny nie obejmuje użytkowników ani ich działań, chociaż uwzględnia się projekt odpowiednich interfejsów z zachowaniami ludzi. Proces utrzymania jest opisany w instrukcjach utrzymania, ale sam nie stanowi części systemu technicznego;

(23) „katastroficzne konsekwencje" oznacza ofiary śmiertelne lub osoby poważnie ranne lub poważne szkody wyrządzone środowisku w wyniku wypadku (Table 3 from EN 50126);

(24) „odbiór w zakresie bezpieczeństwa" oznacza status nadany zmianie przez wnioskodawcę w oparciu o raport w sprawie oceny bezpieczeństwa przedstawiony przez jednostkę oceniającą;

(25) „system" oznacza każdy element systemu kolejowego, który jest zmieniany;

European Railway Agency ● Marc LEFRANCQ, 120 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

(26) „zgłoszony przepis krajowy" oznacza przepis krajowy, który został zgłoszony przez państwa członkowskie zgodnie z dyrektywą Rady 96/48/WE[4], dyrektywą 2001/16/WE Parlamentu Europejskiego i Rady[5] oraz dyrektywami 2004/49/WE i 2008/57/WE.

[G 1] Uznano, że dodatkowe wyjaśnienia nie są konieczne.

Artykuł 4. Znaczące zmiany

Artykuł 4 ust. 1

Jeżeli nie zgłoszono przepisu krajowego, na podstawie którego określa się, czy zmiana jest w danym państwie członkowskim znacząca, czy też nie, wnioskodawca dokonuje oceny potencjalnego wpływu danej zmiany na bezpieczeństwo systemu kolejowego.

W przypadku, gdy proponowana zmiana nie ma wpływu na bezpieczeństwo, nie istnieje konieczność stosowania procesu zarządzania ryzykiem opisanego w art. 5.

[G 1] Jeżeli nie istnieje żaden zgłoszony przepis krajowy, podjęcie decyzji leży w gestii wnioskodawcy. Ocena znaczenia zmiany jest oparta na opinii eksperta. Jeżeli przykładowo planowana zmiana w istniejącym systemie ma kompleksowy charakter, można ją wycenić jako znaczącą w przypadku, gdy istnieje wysokie ryzyko, że będzie ona miała wpływ na istniejące funkcje systemu[6], mimo że zmiana sama w sobie niekoniecznie jest związana w dużym stopniu z bezpieczeństwem.

Artykuł 4 ust. 2

W przypadku gdy proponowana zmiana ma wpływ na bezpieczeństwo, wnioskodawca, kierując się fachowym osądem, decyduje o znaczeniu zmiany na podstawie następujących kryteriów:

(a) skutki awarii systemu: wiarygodny najgorszy scenariusz w przypadku awarii ocenianego systemu, uwzględniający istnienie barier zabezpieczających poza tym systemem;
(b) innowacja wykorzystana przy wprowadzaniu zmiany; kryterium to obejmuje innowacje dotyczące zarówno całej branży kolejowej, jak i tylko organizacji wprowadzającej zmianę;
(c) złożoność zmiany;
(d) monitoring: niezdolność monitorowania wprowadzonej zmiany podczas całego cyklu życia systemu i dokonywania odpowiednich interwencji;
(e) odwracalność zmiany: niezdolność powrotu do systemu sprzed zmiany;
(f) dodatkowość: ocena znaczenia zmiany z uwzględnieniem wszystkich przeprowadzonych niedawno zmian ocenianego systemu, które były związane z bezpieczeństwem i nie zostały ocenione jako znaczące.

Wnioskodawca przechowuje odpowiednią dokumentację, która uzasadnia jego decyzję.

---

(4) *Dz.U. L 235, 17.9.1996, s. 6.*

(5) *Dz.U. L 110 , 20.4.2001, s. 1.*

(6) *Ponieważ funkcje w systemie nie zawsze są niezależne, zmiany niektórych funkcji mogą mieć również wpływ na inne funkcje systemu, mimo że może się wydawać, że zmiany nie dotyczyły bezpośrednio tych funkcji.*

European Railway Agency ● Marc LEFRANCQ, 120 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

[G 1] **Przykład małych zmian:** po oddaniu systemu do eksploatacji jednorazowe zwiększenie maksymalnej prędkości linii o 5 km/h może być mało znaczącą zmianą. Jeżeli jednak maksymalna prędkość linii będzie nadal stopniowo zwiększana o 5 km/h, wówczas suma kolejnych zmian (które oddzielnie zostały ocenione jako nieistotne) może stanowić znaczącą zmianę w stosunku do wymogów bezpieczeństwa systemu wyjściowego.

[G 2] Aby móc wycenić, czy szereg kilku kolejnych (nieistotnych) zmian ma znaczenie, jeśli potraktuje się je jako całość, należy ocenić wszystkie zagrożenia i rodzaje ryzyka związane z wszystkimi zmianami. Komplet takich zmian można uznać za nieistotny, jeśli powodowane przez nie ryzyko jest generalnie dopuszczalne.

[G 3] Jak wynika z prac Agencji nad znaczącymi zmianami:

(a) niemożliwe jest ustalenie zharmonizowanych progów lub przepisów, na podstawie których, w odniesieniu do danej zmiany, można podjąć decyzję o znaczeniu takiej zmiany; a także
(b) niemożliwe jest sporządzenie wyczerpującej listy znaczących zmian;
(c) decyzja nie może być ważna w odniesieniu do wszystkich wnioskodawców oraz wszystkich warunków technicznych, eksploatacyjnych, organizacyjnych i środowiskowych.

Należy zatem pozostawić podjęcie decyzji w gestii wnioskodawców, na których spoczywa odpowiedzialność, zgodnie z art. 4 ust. 3 dyrektywy w sprawie bezpieczeństwa kolei {Ref. 1}, za bezpieczne funkcjonowanie ich części systemu kolejowego i nadzór nad ryzykiem z tym związanym.

[G 4] W części C.2. załącznika C zamieszczono jeden przykład „oceny i zastosowania kryteriów", który ma służyć jako pomoc dla wnioskodawców.

[G 5] Nie wolno stosować CSM, jeśli zmiana związana z bezpieczeństwem nie jest uważana za znaczącą. Nie oznacza to jednak, że nie podejmuje się żadnych działań. Wnioskodawca przeprowadza pewnego rodzaju (wstępne) analizy ryzyka, aby ocenić, czy zmiana jest znacząca. Takie analizy ryzyka, podobnie jak wszelkie uzasadnienia i argumentacje, muszą być udokumentowane, aby umożliwić krajowemu organowi ds. bezpieczeństwa przeprowadzenie kontroli. Organowi oceniającemu nie wolno niezależnie dokonywać oceny znaczenia zmiany i podejmować decyzji stwierdzającej, że zmiana jest nieistotna.

Artykuł 5. Proces zarządzania ryzykiem

Artykuł 5 ust 1

Opisany w załączniku I proces zarządzania ryzykiem stosuje się:

(a) w przypadku znaczącej zmiany, o której mowa w art. 4, w tym dopuszczenia do eksploatacji podsystemów strukturalnych, o którym mowa w art. 2 ust. 2 lit. b);

(b) *gdy TSI, o której mowa w art. 2 ust. 2 lit. a) odsyła do niniejszego rozporządzenia, aby nakazać* proces zarządzania ryzykiem opisany w załączniku I, jak określono w art. 2 ust. 2 lit. a).

[G 1] Uznano, że dodatkowe wyjaśnienia nie są konieczne.

European Railway Agency ● Marc LEFRANCQ, 120 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

Artykuł 5 ust 2

Proces zarządzania ryzykiem opisany w załączniku I jest stosowany przez wnioskodawcę.

[G 1] Uznano, że dodatkowe wyjaśnienia nie są konieczne.

Artykuł 5 ust 3

Wnioskodawca gwarantuje zarządzanie ryzykiem powodowanym przez dostawców i usługodawców, w tym ich podwykonawców. W tym celu wnioskodawca może poprosić dostawców i usługodawców, w tym ich podwykonawców, o uczestniczenie w procesie zarządzania ryzykiem opisanym w załączniku I.

[G 2] Uznano, że dodatkowe wyjaśnienia nie są konieczne.

Artykuł 6. Niezależna ocena

Artykuł 6 ust 1

Niezależnej oceny prawidłowości stosowania procesu zarządzania ryzykiem, który jest opisany w załączniku I, oraz jego wyników dokonuje jednostka spełniająca kryteria wymienione w załączniku II. W przypadku gdy jednostka oceniająca nie została wcześniej wskazana w prawie wspólnotowym lub w ustawodawstwie krajowym, wnioskodawca wyznacza swoją własną jednostkę oceniającą, którą może być inna organizacja lub dział wewnętrzny.

[G 1] Wymagany poziom niezależności w odniesieniu do jednostki oceniającej zależy od poziomu bezpieczeństwa, który jest wymagany w odniesieniu do systemu objętego oceną. W oczekiwaniu na harmonizację wymagań w tym zakresie, najlepsze zasady można znaleźć w klauzuli 8 IEC61508-1:2001 lub w części § 5.3.9. normy EN 50 129 {Ref. 7}. Stopień niezależności jest uzależniony zarówno od powagi skutków zagrożenia związanych ze sprzętem, jak i od jego nowoczesności. Część § 9.7.2 w normach EN 50 126-2 i EN 50129 określa poziom niezależności w odniesieniu do systemów sygnalizacji. W zasadzie tę część można również zastosować w odniesieniu do innych systemów.

[G 2] Agencja nadal pracuje nad zdefiniowaniem zadań i obowiązków różnych organów oceniających (krajowego organu ds. bezpieczeństwa, jednostki notyfikowanej oraz niezależnego organu ds. oceny bezpieczeństwa), jak również niezbędnych interfejsów pomiędzy nimi. Pozwoli to określić, który z tych organów (w miarę możliwości) wykonuje jakie zadania i w jaki sposób. Dzięki temu będzie można ostatecznie określić, w jaki sposób:

(a) sprawdzić, na podstawie dowodów, że procesy zarządzania ryzykiem i oceny ryzyka w ramach CSM są właściwie stosowane, a także
(b) udzielić wsparcia wnioskodawcy w podjęciu decyzji odnośnie do zaakceptowania znaczącej zmiany w ramach systemu objętego oceną.

European Railway Agency ● Marc LEFRANCQ, 120 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

Artykuł 6 ust 2

Należy unikać dublowania prac pomiędzy oceną zgodności systemu zarządzania bezpieczeństwem wymaganą zgodnie z dyrektywą 2004/49/WE, oceną zgodności dokonywaną przez jednostkę notyfikowaną lub organ krajowy, która jest wymagana zgodnie z dyrektywą 2008/57/WE, oraz niezależną oceną bezpieczeństwa dokonywaną przez jednostkę oceniającą zgodnie z niniejszym rozporządzeniem.

[G 1] Prace Agencji nad zadaniami i obowiązkami organów oceniających dostarczą dodatkowych informacji.

Artykuł 6 ust 3

Organ ds. bezpieczeństwa może działać w charakterze jednostki oceniającej, jeżeli znaczące zmiany dotyczą następujących przypadków:

(a) pojazd wymaga zezwolenia na dopuszczenie do eksploatacji, zgodnie z art. 22 ust. 2 i art. 24 ust. 2 dyrektywy 2008/57/WE;

(b) pojazd wymaga dodatkowego zezwolenia na dopuszczenie do eksploatacji, zgodnie z art. 23 ust. 5 i art. 25 ust. 4 dyrektywy 2008/57/WE;

(c) certyfikat bezpieczeństwa musi zostać zaktualizowany w związku ze zmianą typu lub zakresu działalności, zgodnie z art. 10 ust. 5 dyrektywy 2004/49/WE;

(d) certyfikat bezpieczeństwa musi zostać zmieniony w związku z istotną zmianą w przepisach dotyczących bezpieczeństwa, zgodnie z art. 10 ust. 5 dyrektywy 2004/49/WE;

(e) autoryzacja bezpieczeństwa musi zostać zaktualizowana w związku z istotną zmianą w infrastrukturze, sygnalizacji, w zasilaniu energią lub w zasadach eksploatacji i utrzymania infrastruktury, zgodnie z art. 11 ust. 2 dyrektywy 2004/49/WE;

(f) autoryzacja bezpieczeństwa musi zostać zmieniona w związku z istotną zmianą w przepisach dotyczących bezpieczeństwa, zgodnie z art. 11 ust. 2 dyrektywy 2004/49/WE.

[G 1] Uznano, że dodatkowe wyjaśnienia nie są konieczne.

Artykuł 6 ust 4

Jeżeli znaczące zmiany dotyczą podsystemu strukturalnego, który wymaga zezwolenia na dopuszczenie do eksploatacji, zgodnie z art. 15 ust. 1 lub art. 20 dyrektywy 2008/57/WE, organ ds. bezpieczeństwa może działać w charakterze jednostki oceniającej, chyba że wnioskodawca przydzielił już to zadanie jednostce notyfikowanej zgodnie z art. 18 ust. 2 tej dyrektywy.

[G 1] Uznano, że dodatkowe wyjaśnienia nie są konieczne.

Artykuł 7. Raporty w sprawie oceny bezpieczeństwa

Artykuł 7 ust 1

Jednostka oceniająca przedstawia wnioskodawcy raport w sprawie oceny bezpieczeństwa.

[G 1] Uznano, że dodatkowe wyjaśnienia nie są konieczne.

European Railway Agency ● Marc LEFRANCQ, 120 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

Artykuł 7 ust 2

W przypadku, o którym mowa w art. 5 ust. 1 lit. a), raport w sprawie oceny bezpieczeństwa jest brany pod uwagę przez krajowy organ ds. bezpieczeństwa przy podejmowaniu decyzji o zezwoleniu na dopuszczenie do eksploatacji podsystemów i pojazdów.

[G 1] Uznano, że dodatkowe wyjaśnienia nie są konieczne.

Artykuł 7 ust 3

W przypadku, o którym mowa w art. 5 ust. 1 lit. b), niezależna ocena należy do zadań jednostki notyfikowanej, o ile TSI nie nakazuje inaczej.
Jeżeli niezależna ocena nie stanowi części zadania notyfikowanej jednostki, raport w sprawie oceny bezpieczeństwa jest brany pod uwagę przez jednostkę notyfikowaną, która odpowiada za wydawanie certyfikatu zgodności, lub przez podmiot zamawiający, który sporządza deklarację weryfikacji WE.

[G 1] Uznano, że dodatkowe wyjaśnienia nie są konieczne.

Artykuł 7 ust 4

Jeżeli dokonano już odbioru systemu lub jego części po przeprowadzeniu procesu zarządzania ryzykiem określonego w niniejszym rozporządzeniu, raport w sprawie oceny bezpieczeństwa dotyczący takiego wcześniejszego procesu nie powinien być kwestionowany przez inną jednostkę oceniającą, która dokonuje nowej oceny tego samego systemu. Warunkiem uznania jest wykazanie, że system będzie użytkowany w takich samych warunkach funkcjonalnych, eksploatacyjnych i środowiskowych jak już zaakceptowany system oraz że zastosowano równoważne kryteria akceptacji ryzyka.

[G 1] Ta zasada wzajemnego uznawania została już zaakceptowana przez normy CENELEC: zob. część § 5.5.2 w EN 50 129 i część § 5.9 w EN 50 126-2. W normach CENELEC zasada wspólnej akceptacji lub wzajemnego uznawania jest stosowana przez wnioskodawców i niezależne organy ds. oceny bezpieczeństwa w odniesieniu do produktów ogólnego przeznaczenia oraz zastosowań ogólnych[7], pod warunkiem że ocena bezpieczeństwa i wykazanie bezpieczeństwa są przeprowadzane zgodnie z wymogami bezpieczeństwa CENELEC.

[G 2] Zasada wzajemnego uznawania musi być również stosowana w odniesieniu do akceptowania nowych lub zmodyfikowanych systemów, jeśli ocena ryzyka związanego z tymi systemami i wykazanie zgodności systemu z wymogami bezpieczeństwa są przeprowadzane zgodnie z przepisami rozporządzenia CSM {Ref. 3}.

(7) *Zob. część 1.1.5 pkt [G 5] oraz przypisy (9) i (10) na str. 31, jak również schemat 3 niniejszego dokumentu, aby uzyskać dodatkowe wyjaśnienie terminów „produkt ogólnego przeznaczenia i zastosowanie ogólne" oraz ich podstawowych zasad.*

European Railway Agency ● Marc LEFRANCQ, 120 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

Artykuł 8. Zarządzanie nadzorem ryzyka oraz audyty wewnętrzne i zewnętrzne

Artykuł 8 ust 1

Przedsiębiorstwa kolejowe i zarządcy infrastruktury włączają audyty stosowania CSM w zakresie wyceny i oceny ryzyka do swoich regularnych audytów systemu zarządzania ryzykiem, o których mowa w art. 9 dyrektywy 2004/49/WE.

[G 1] Uznano, że dodatkowe wyjaśnienia nie są konieczne.

Artykuł 8 ust 2

W ramach zadań określonych w art. 16 ust. 2 lit. e) dyrektywy 2004/49/WE krajowy organ ds. bezpieczeństwa monitoruje stosowanie CSM w zakresie wyceny i oceny ryzyka.

[G 1] Uznano, że dodatkowe wyjaśnienia nie są konieczne.

Artykuł 9. Informacje zwrotne a postęp techniczny

Artykuł 9 ust 1

W rocznym raporcie dotyczącym bezpieczeństwa, o którym mowa w art. 9 ust. 4 dyrektywy 2004/49/WE, każde przedsiębiorstwo kolejowe i każdy zarządca infrastruktury zdaje krótkie sprawozdanie ze swoich doświadczeń dotyczących stosowania CSM w zakresie wyceny i oceny ryzyka. Raport zawiera ponadto streszczenie decyzji dotyczących stopnia znaczenia zmian.

[G 1] Uznano, że dodatkowe wyjaśnienia nie są konieczne.

Artykuł 9 ust 2

W rocznym raporcie dotyczącym bezpieczeństwa, o którym mowa w art. 18 dyrektywy 2004/49/WE, każdy krajowy organ ds. bezpieczeństwa zdaje sprawozdanie z doświadczeń wnioskodawców dotyczących stosowania CSM w zakresie wyceny i oceny ryzyka, a w stosownych przypadkach również ze swoich własnych doświadczeń.

[G 1] Uznano, że dodatkowe wyjaśnienia nie są konieczne.

Artykuł 9 ust 3

Europejska Agencja Kolejowa monitoruje stosowanie CSM w zakresie wyceny i oceny ryzyka, zbiera informacje zwrotne na ten temat, i w stosownych przypadkach przekazuje Komisji zalecenia dotyczące ulepszeń.

[G 1] Uznano, że dodatkowe wyjaśnienia nie są konieczne.

European Railway Agency ● Marc LEFRANCQ, 120 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

Artykuł 9 ust 4

Najpóźniej w dniu 31 grudnia 2011 r. Europejska Agencja Kolejowa przedstawia Komisji raport obejmujący:

(a) analizę doświadczeń dotyczących stosowania CSM w zakresie wyceny i oceny ryzyka, w tym przypadków, w których wnioskodawcy dobrowolnie stosowali CSM przed właściwymi datami zastosowania, o których mowa w art. 10;

(b) analizę doświadczeń wnioskodawców dotyczących decyzji w sprawie stopnia znaczenia zmian;

(c) analizę przypadków stosowania kodeksu postępowania w sposób opisany w sekcji 2.3.8 załącznika I;

(d) analizę ogólnej skuteczności CSM w zakresie wyceny i oceny ryzyka.

Organy ds. bezpieczeństwa pomagają Agencji, wskazując przypadki, w których stosowano niniejszą CSM w zakresie wyceny i oceny ryzyka.

[G 1] Uznano, że dodatkowe wyjaśnienia nie są konieczne.

Artykuł 10. Wejście w życie

Artykuł 10 ust 1

Niniejsze rozporządzenie wchodzi w życie dwudziestego dnia po jego opublikowaniu w Dzienniku Urzędowym Unii Europejskiej.

[G 1] Uznano, że dodatkowe wyjaśnienia nie są konieczne.

Artykuł 10 ust 2

Niniejsze rozporządzenie stosuje się od dnia 1 lipca 2012 r.

Jednakże niniejsze rozporządzenie stosuje się od dnia 19 lipca 2010 r.:

(a) do wszystkich znaczących zmian technicznych dotyczących pojazdów, które są zdefiniowane w art. 2 lit. c) dyrektywy 2008/57/WE;

(b) do wszystkich znaczących zmian dotyczących podsystemów strukturalnych, gdy wymagają tego przepisy art. 15 ust. 1 dyrektywy 2008/57/WE lub TSI.

[G 1] Uznano, że dodatkowe wyjaśnienia nie są konieczne.

European Railway Agency ● Marc LEFRANCQ, 120 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

ZAŁĄCZNIK I - WYJAŚNIENIE PROCESU OKREŚLONEGO W ROZPORZĄDZENIU CSM

1. GŁÓWNE ZASADY STOSUJĄCE SIĘ DO PROCESU ZARZĄDZANIA RYZYKIEM

1.1. Główne zasady i obowiązki

1.1.1. Proces zarządzania ryzykiem, którego dotyczy niniejsze rozporządzenie, rozpoczyna się od zdefiniowania systemu podlegającego ocenie i obejmuje następujące działania:

(a) proces oceny ryzyka, w ramach którego identyfikuje się zagrożenia, ryzyko, związane z nimi środki bezpieczeństwa oraz wymogi bezpieczeństwa, które powinien spełniać oceniany system;
(b) wykazanie zgodności systemu ze zidentyfikowanymi wymogami bezpieczeństwa; oraz
(c) zarządzenie wszystkimi zidentyfikowanymi zagrożeniami oraz związanymi z nimi środkami bezpieczeństwa.

Proces zarządzania ryzykiem ma charakter wieloetapowy. Jego przebieg przedstawiono na schemacie w dodatku. Proces ten kończy się z chwilą wykazania zgodności systemu ze wszystkimi wymogami bezpieczeństwa koniecznymi do zaakceptowania ryzyka związanego ze zidentyfikowanymi zagrożeniami.

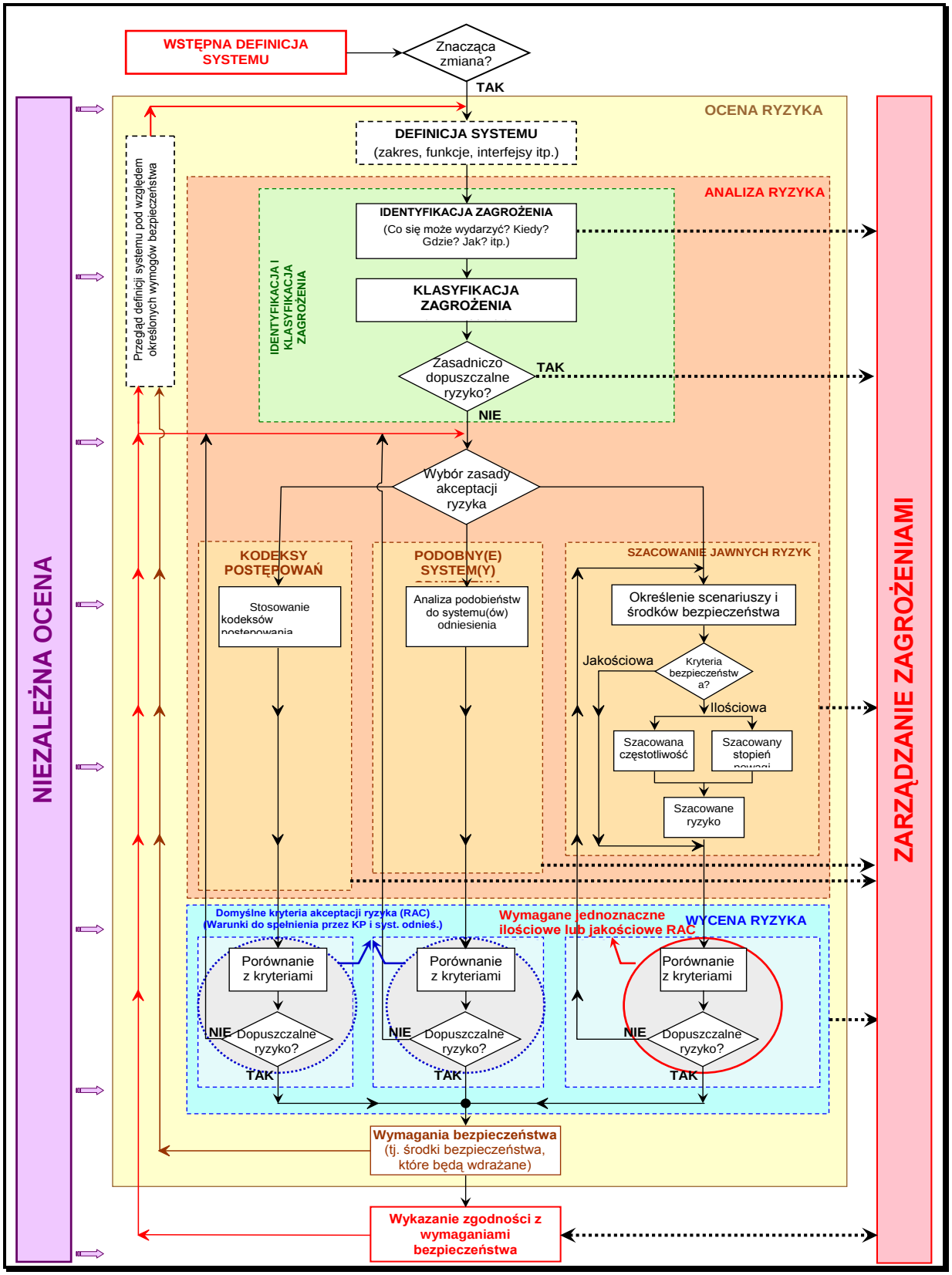
[G 1] Schemat 1 przedstawia ramy zarządzania ryzykiem w odniesieniu do CSM i powiązany proces oceny ryzyka. Tam, gdzie uznano to za konieczne, każda ramka/działanie z tego schematu opisane jest w określonej części niniejszego dokumentu.

[G 2] Zgodnie z radami CENELEC, procesy zarządzania ryzykiem i oceny ryzyka opisuje się w planie bezpieczeństwa. Jeśli jednak nie jest to praktyczne z punktu widzenia projektu, opis taki można umieścić w jakimkolwiek innym stosownym dokumencie. Zob. część 1.1.6.

[G 3] Proces oceny ryzyka rozpoczyna się od wstępnej definicji systemu. W trakcie rozbudowy projektu wstępna definicja systemu jest stopniowo aktualizowana i zastępuje ją definicja systemu. W przypadku gdy nie istnieje wstępna definicja systemu, do przeprowadzenia oceny ryzyka stosowana jest formalna definicja systemu. Wówczas jednak warto, aby wszystkie podmioty, których dotyczy znacząca zmiana, spotkały się w momencie rozpoczęcia projektu, aby:

(a) uzgodnić ogólne zasady systemu, funkcje systemu itp. W zasadzie można je opisać we wstępnej definicji systemu;
(b) ustalić organizację projektu;
(c) w stosownych przypadkach - uzgodnić podział zadań i obowiązków pomiędzy różnymi podmiotami już zaangażowanymi w projekt, w tym krajowym organem ds. bezpieczeństwa, jednostką notyfikowaną i niezależnym organem ds. ochrony bezpieczeństwa.

European Railway Agency ● Marc LEFRANCQ, 120 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu



Schemat 1: Struktura zarządzania ryzykiem zgodnie z rozporządzeniem CSM {Ref. 3}.

European Railway Agency ● Marc LEFRANCQ, 120 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

Taka koordynacja, na przykład podczas ustalania wstępnej definicji systemu, daje wnioskodawcy, podwykonawcom, krajowemu organowi ds. bezpieczeństwa, jednostce notyfikowanej i niezależnemu organowi ds. ochrony bezpieczeństwa - w stosownych przypadkach - możliwość uzgodnienia na początkowym etapie takich kodeksów postępowania i systemów odniesienia, których użycie w ramach projektu jest możliwe do zaakceptowania.

1.1.2. Wieloetapowy proces zarządzania ryzykiem:

(a) obejmuje odpowiednie działania w zakresie zapewnienia jakości i przeprowadza go kompetentny personel;

(b) jest niezależnie oceniany przez jednostkę oceniającą lub jednostki oceniające.

[G 1] System zarządzania bezpieczeństwem przedsiębiorstwa kolejowego i zarządcy infrastruktury określa proces i procedury, które:

(a) pozwalają monitorować bezpieczeństwo systemu w całym cyklu życia systemu (tj. podczas jego eksploatacji i utrzymania);
(b) zapewniają bezpieczny demontaż lub bezpieczną wymianę powiązanego systemu.

Ten proces nie jest częścią CSM w zakresie oceny ryzyka.

[G 2] W celu wdrożenia CSM, wszystkie zaangażowane strony muszą być kompetentne (tj. posiadać właściwe umiejętności, wiedzę i doświadczenie). Istnieje ciągłe zapotrzebowanie na zarządzanie kompetencjami w ramach organizacji podmiotów sektora kolejowego:

(a) w przypadku zarządców infrastruktury i przedsiębiorstw kolejowych funkcję tę spełniają ich systemy zarządzania bezpieczeństwem na mocy załącznika III pkt 2 lit. e) dyrektywy w sprawie bezpieczeństwa kolei {Ref. 1};
(b) inne podmioty, których działania mogą mieć wpływ na bezpieczeństwo systemu kolejowego, mimo że w zasadzie system zarządzania bezpieczeństwem nie jest obowiązkowy, przynajmniej na poziomie projektu (zob. pkt [G 1] w sekcji 5.1), dysponują procesem zarządzania jakością lub procesem zarządzania bezpieczeństwem, który spełnia ten wymóg.

[G 3] Poniższe fragmenty normy CENELEC EN 50 126-1 {Ref. 8} określają wytyczne w zakresie kompetencji:

(a) zgodnie z § 5.3.5.b): *„wszyscy pracownicy odpowiedzialni za proces zarządzania”* ryzykiem muszą posiadać *„odpowiednie kompetencje, aby wywiązywać się ze swoich obowiązków”;*
(b) § 5.3.5.d): wymogi zarządzania ryzykiem i oceny ryzyka powinny być *„wprowadzone w ramach procesów biznesowych przy wsparciu systemu zarządzania jakością (QMS) zgodnie z wymogami normy EN ISO 9001, EN ISO 9002 lub EN ISO 9003 właściwej dla systemu objętego”* oceną. Przykłady aspektów kontrolowanych przez system zarządzania jakością są podane w części § 5.2. normy EN 50 129 {Ref. 7}.

Obejmują one działania w zakresie zapewnienia jakości, jak również doskonalenie umiejętności i szkolenia personelu/osób, które są wymagane w celu wsparcia procesu objętego CSM.

[G 4] Bardzo często w procesie oceny ryzyka od samego początku projektu uczestniczy jednostka oceniająca, jednak - o ile prawo krajowe w państwie członkowskim nie stanowi inaczej - takie zaangażowanie jednostki oceniającej na tak wczesnym etapie nie jest obowiązkowe, choć wskazane. Opinia niezależnej jednostki oceniającej mogłaby być przydatna przed przejściem

European Railway Agency ● Marc LEFRANCQ, 120 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

z jednego etapu oceny ryzyka do kolejnego. Więcej szczegółowych informacji na temat niezależnej oceny znajduje się w Artykuł 6.

1.1.3. Wnioskodawca odpowiedzialny za proces zarządzania ryzykiem, który jest wymagany zgodnie z niniejszym rozporządzeniem, prowadzi rejestr zagrożeń zgodnie z sekcją 4.

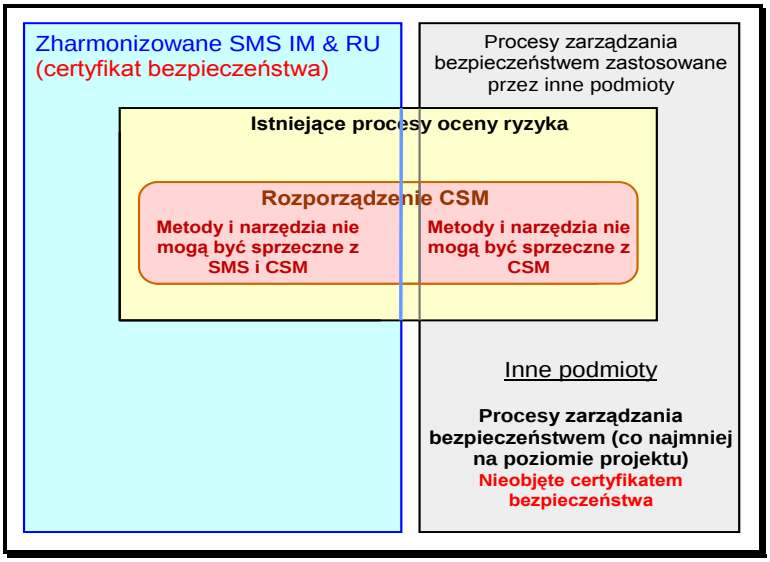
[G 1] Uznano, że dodatkowe wyjaśnienia nie są konieczne.

1.1.4. Podmioty, które stosują już metody lub narzędzia oceny ryzyka, mogą je dalej stosować, o ile są one zgodne z przepisami niniejszego rozporządzenia i spełniają następujące warunki:

(a) metody lub narzędzia oceny ryzyka są opisane w systemie zarządzania bezpieczeństwem, który został zaakceptowany przez krajowy organ ds. bezpieczeństwa zgodnie z art. 10 ust. 2 lit. a) lub art. 11 ust. 1 lit. a) dyrektywy 2004/49/WE; lub

(b) metody lub narzędzia oceny ryzyka są wymagane zgodnie z TSI lub są zgodne z publicznie dostępnymi uznanymi normami określonymi w zgłoszonych przepisach krajowych.

[G 1] Schemat 2 przedstawia zależność pomiędzy CSM i „systemami zarządzania bezpieczeństwem oraz procesami oceny ryzyka".



Schemat 2: Zharmonizowane SMS i CSM.

European Railway Agency ● Marc LEFRANCQ, 120 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

1.1.5. Bez uszczerbku dla odpowiedzialności cywilnej zgodnej z prawnymi wymogami państw członkowskich, za proces oceny ryzyka jest odpowiedzialny wnioskodawca. Wnioskodawca, za zgodą zainteresowanych podmiotów, decyduje w szczególności o tym, kto będzie odpowiadał za spełnienie wymogów bezpieczeństwa wynikających z oceny ryzyka. Decyzja ta jest uzależniona od charakteru środków bezpieczeństwa, które zostały wybrane, aby nadzorować ryzyko, utrzymując je na dopuszczalnym poziomie. Zgodność z wymogami bezpieczeństwa wykazuje się zgodnie z sekcją 3.

[G 1] Jeżeli wnioskodawcą jest zarządca infrastruktury lub przedsiębiorstwo kolejowe, konieczne może być niekiedy włączenie innych podmiotów w ten proces [8] (zob. część 1.2.1). W niektórych przypadkach zarządca infrastruktury lub przedsiębiorstwo kolejowe może zlecić podwykonanie, częściowe lub całkowite, działań związanych z oceną ryzyka. Zadania i obowiązki każdego z podmiotów są zazwyczaj ustalane pomiędzy zainteresowanymi podmiotami na wczesnym etapie projektu.

[G 2] Należy zauważyć, że wnioskodawca zawsze ponosi odpowiedzialność za zastosowanie CSM, akceptację ryzyka i tym samym za bezpieczeństwo systemu, w tym również za dbałość o to, aby:

(a) zaangażowane podmioty w pełni ze sobą współpracowały, aby zapewnić wszystkie niezbędne informacje, a także

(b) było oczywiste, kto odpowiada za spełnienie danego wymogu CSM (np. przeprowadzenie analizy ryzyka lub zarządzanie wykazem zagrożeń).

W przypadku różnicy zdań pomiędzy podmiotami na temat wymogów bezpieczeństwa, które mają spełnić, należy zasięgnąć opinii krajowego organu ds. bezpieczeństwa. Niemniej jednak obowiązek znalezienia rozwiązania nadal spoczywa na wnioskodawcy i nie może być przerzucony na krajowy organ ds. bezpieczeństwa: zob. także część 0.2.2.

[G 3] W przypadku gdy zadanie zostało zlecone podwykonawcom, podwykonawca nie ma obowiązku posiadania własnej organizacji bezpieczeństwa, jeśli nie jest zarządcą infrastruktury lub przedsiębiorstwem kolejowym, lub zwłaszcza jeśli podwykonawca jest niewielką firmą lub jeśli jego wkład w ogólny system jest ograniczony. Odpowiedzialność za zarządzanie ryzykiem, w tym ocenę ryzyka i zarządzanie zagrożeniem, może ponosić organizacja wyższego szczebla (tj. klient podwykonawcy). Niemniej jednak podwykonawca ma zawsze obowiązek dostarczyć właściwe informacje na temat swoich działań, które są potrzebne organizacji wyższego szczebla w celu kompilowania dokumentacji zarządzania ryzykiem.
Organizacje współpracujące ze sobą mogą również uzgodnić założenie wspólnej organizacji ds. bezpieczeństwa, na przykład w celu zoptymalizowania kosztów. W takim przypadku tylko jedna organizacja będzie zarządzać działaniami dotyczącymi bezpieczeństwa wszystkich zaangażowanych organizacji. Odpowiedzialność za poprawność informacji (tj. zagrożenia, ryzyko i środki bezpieczeństwa) oraz za zarządzanie wdrażaniem środków bezpieczeństwa nadal ponosi organizacja odpowiedzialna za kontrolę zagrożeń, których dotyczą te środki bezpieczeństwa.

[G 4] Wnioskodawca zazwyczaj ustala „poziomy bezpieczeństwa” i „wymogi bezpieczeństwa” przypisane podmiotom zaangażowanym w projekt oraz różnym podsystemom i sprzętowi, które należą do tych podmiotów:

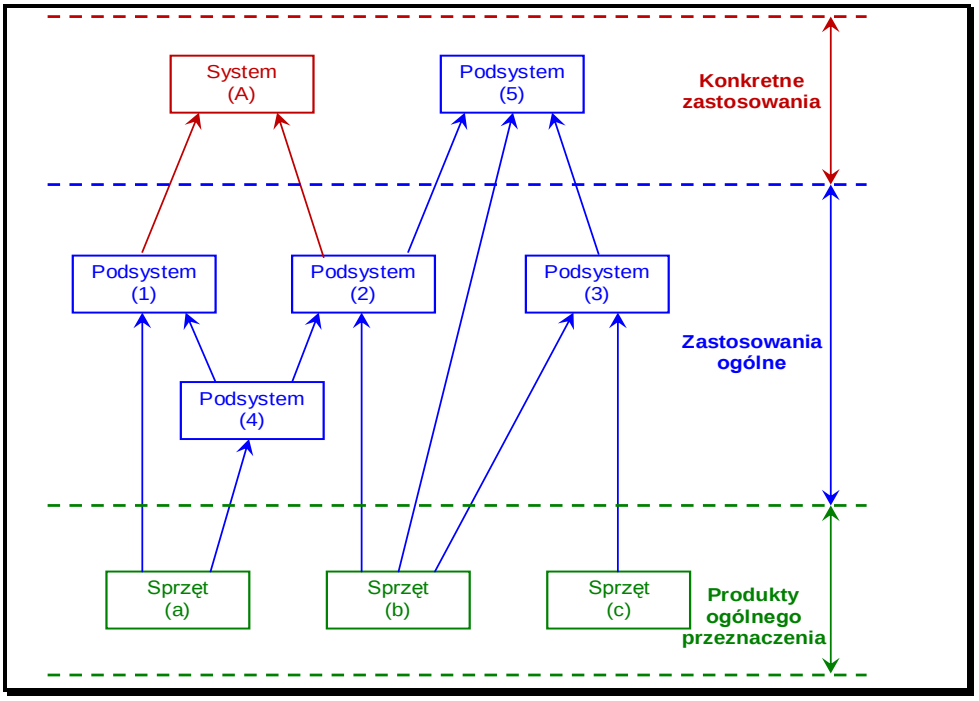
(8) *Jest to zgodne z załącznikiem A.4 do normy CENELEC 50 129 {Ref. 7}.*

European Railway Agency ● Marc LEFRANCQ, 120 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

(a) w umowach pomiędzy wnioskodawcą i odpowiednimi podmiotami (podwykonawcami);
(b) w planie bezpieczeństwa, lub jakimkolwiek innym stosownym dokumencie sporządzonym w takim samym celu, wraz z opisem ogólnej organizacji projektu i obowiązków każdego podmiotu, w tym obowiązków wnioskodawcy: zob. część 1.1.6;
(c) w wykazie/wykazach zagrożeń wnioskodawcy: zob. część 4.1.1.

Przydział „poziomów bezpieczeństwa" i „wymogów bezpieczeństwa" systemu podsystemom i sprzętowi, a tym samym poszczególnym podmiotom, w tym samemu wnioskodawcy, można udoskonalić/rozszerzyć na „etapie wykazania zgodności systemu z wymogami bezpieczeństwa": zob. Schemat 1. W porównaniu z modelem V według CENELEC (zob. część 2.1.1 i Schemat 5 na str. 35), działanie to odnosi się do fazy 5, która dotyczy „rozdzielenia wymogów systemowych" na różne podsystemy i elementy.

[G 5] Artykuł 5 ust. 2 dopuszcza, aby podmioty inne niż przedsiębiorstwa kolejowe i zarządcy infrastruktury ponosiły pełną odpowiedzialność za zgodność z CSM w zależności od potrzeb. Przykładowo, w odniesieniu do produktów ogólnego przeznaczenia i zastosowań ogólnych[9] producent może przeprowadzić ocenę ryzyka na podstawie „ogólnej definicji systemu" w celu określenia poziomów bezpieczeństwa i wymogów bezpieczeństwa, które mają zostać spełnione przez produkty ogólnego przeznaczenia i zastosowania.



Schemat 3: Przykłady zależności pomiędzy dowodami bezpieczeństwa (zaczerpnięte ze schematu 9 normy EN 50 129).

[G 6] Zgodnie z zaleceniami CENELEC producent powinien dostarczać udokumentowane dane z oceny ryzyka w dziennikach zagrożeń i zasadach bezpieczeństwa produktu ogólnego

European Railway Agency ● Marc LEFRANCQ, 120 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

przeznaczenia (lub zastosowania ogólnego[9]). Te zasady bezpieczeństwa i dzienniki zagrożeń obejmują wszystkie założenia[10] i ustalone „ograniczenia stosowania" (tj. warunki stosowania związane z bezpieczeństwem), które stosuje się w odniesieniu do powiązanych produktów ogólnego przeznaczenia (lub zastosowania ogólnego). Dlatego też, ilekroć produkt ogólnego przeznaczenia i zastosowanie ogólne są wykorzystywane w eksploatacji w konkretnym zastosowaniu, należy wykazać zgodność ze wszystkimi tymi założeniami[10] i „ograniczeniami stosowania" (lub warunkami stosowania związanymi z bezpieczeństwem) w odniesieniu do każdego takiego konkretnego zastosowania.

---

(9) *Takie terminy jak „zastosowanie ogólne" i „dowody bezpieczeństwa dotyczące produktu ogólnego przeznaczenia" są stosowane za CENELEC, gdzie wyróżniono trzy różne kategorie dowodu bezpieczeństwa (zob. Schemat 3):*

- *(a)* ***dowód bezpieczeństwa dotyczący produktu ogólnego przeznaczenia*** *(niezależnie od zastosowania). Produkt ogólnego przeznaczenia można użyć ponownie do różnych, niezależnych od siebie zastosowań;*
- *(b)* ***dowód bezpieczeństwa dotyczący zastosowania ogólnego*** *(w odniesieniu do grupy zastosowań). Zastosowanie ogólne można ponownie użyć w odniesieniu do grupy/ rodzaju zastosowań charakteryzujących się wspólnymi funkcjami;*
- *(c)* ***dowód bezpieczeństwa dotyczący konkretnego zastosowania*** *(w odniesieniu do konkretnego zastosowania). Konkretne zastosowanie można użyć wyłącznie w odniesieniu do jednej konkretnej instalacji.*

W celu uzyskania dodatkowych informacji na temat zależności pomiędzy tymi dowodami należy odnieść się do części § 9.4. i schematu 9.1 Wytycznych do CENELEC 50 126-2 {Ref. 9}.

(10) *Te założenia i ograniczenia stosowania określają zakres i ważność „ocen bezpieczeństwa" i „analiz bezpieczeństwa" powiązanych z odpowiednimi dowodami bezpieczeństwa dotyczącymi produktu ogólnego przeznaczenia i zastosowania ogólnego. Jeżeli nie są one spełnione w rozważanym konkretnym zastosowaniu, należy zaktualizować odpowiednie „oceny bezpieczeństwa" i „analizy bezpieczeństwa" (np. typowe analizy) lub zastąpić je nowymi.*

> *Jest to zgodne z następującą ogólną zasadą bezpieczeństwa: „Ilekroć projekt konkretnego (pod)systemu jest oparty na zastosowaniach ogólnych i produktach ogólnego przeznaczenia, należy wykazać, że konkretny (pod)system jest zgodny ze wszystkimi założeniami i ograniczeniami stosowania (nazywanymi warunkami stosowania związanymi z bezpieczeństwem w CENELEC), które są włączane w odpowiednie dowody bezpieczeństwa dotyczące zastosowania ogólnego i produktu ogólnego przeznaczenia (zob. Schemat 3)"*

Jeżeli w odniesieniu do konkretnego zastosowania nie można osiągnąć zgodności z pewnymi założeniami i ograniczeniami stosowania na poziomie podsystemu (np. w przypadku eksploatacyjnych wymogów bezpieczeństwa), odpowiednie założenia i ograniczenia stosowania można przenieść na wyższy poziom (tj. zazwyczaj na poziom systemu). Te założenia i ograniczenia stosowania są następnie wyraźnie określane w „dowodzie bezpieczeństwa dotyczącym konkretnego zastosowania" odpowiedniego podsystemu. W takich przykładach zależności należy zapewnić spełnienie warunków stosowania związanych z bezpieczeństwem każdego dowodu bezpieczeństwa w dowodzie bezpieczeństwa wyższego poziomu lub też przeniesienie ich do warunków stosowania związanych z bezpieczeństwem dowodu bezpieczeństwa najwyższego poziomu (tj. dowodu bezpieczeństwa systemu).

European Railway Agency ● Marc LEFRANCQ, 120 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

1.1.6. Pierwszy etap procesu zarządzania ryzykiem polega na określeniu przez wnioskodawcę w specjalnym dokumencie zadań poszczególnych podmiotów oraz ich działań z zakresu zarządzania ryzykiem. Wnioskodawca koordynuje bliską współpracę pomiędzy poszczególnymi zaangażowanymi podmiotami, stosownie do zadań tych podmiotów, w celu zarządzania zagrożeniami i związanymi z nimi środkami bezpieczeństwa.

[G 1] Bardzo często, o ile nie ustalono inaczej w umowach zawartych na początku projektu, dla każdego projektu istnieje dokument, który opisuje działania w zakresie zarządzania ryzykiem. Dokument taki jest aktualizowany i poddawany przeglądom, ilekroć w pierwotnym systemie wprowadzane są znaczące zmiany.

[G 2] Dokument określa strukturę organizacyjną, obowiązki przydzielonych pracowników, procesy, procedury i działania, które łącznie gwarantują, że system objęty oceną osiąga wyznaczone poziomy bezpieczeństwa i spełnia wymogi bezpieczeństwa. Dokument musi być zgodny z CSM, ponieważ stanowi pomoc i zapewnia wskazówki dla organu oceniającego. Zgodnie z normami CENELEC, tego rodzaju informacje należy włączyć do planu bezpieczeństwa lub innego dokumentu, którego część jest poświęcona tym zagadnieniom.

[G 3] Ogólną organizację projektu przedstawia przede wszystkim plan bezpieczeństwa wnioskodawcy lub jakikolwiek inny stosowny dokument. Opisuje on sposób podziału zadań i obowiązków pomiędzy zaangażowanymi podmiotami. Bardziej szczegółowe informacje można uzyskać zapoznając się z planami bezpieczeństwa lub organizacjami bezpieczeństwa różnych zaangażowanych podmiotów. Zazwyczaj podział obowiązków pomiędzy różnymi podmiotami jest omawiany i ustalany na etapie wstępnej definicji systemu (tj. na początku projektu), o ile taka definicja istnieje.

[G 4] Plan bezpieczeństwa jest żywym dokumentem, który w miarę potrzeby jest aktualizowany w trakcie realizacji projektu.

[G 5] Więcej szczegółów można znaleźć w normie EN 50 126-1 {Ref. 8} oraz powiązanych wytycznych do normy 50 126-1 {Ref. 9} na temat zawartości planu bezpieczeństwa.

1.1.7. Za ocenę prawidłowości stosowania procesu zarządzania ryzykiem opisanego w niniejszym rozporządzeniu odpowiada jednostka oceny.

[G 1] Uznano, że dodatkowe wyjaśnienia nie są konieczne.

1.2. Zarządzanie interfejsami (zarządzanie ryzykiem wspólnym)

1.2.1. Zainteresowane podmioty sektora kolejowego współpracują ze sobą w odniesieniu do wszystkich interfejsów mających znaczenie dla ocenianego systemu (bez uszczerbku dla specyfikacji interfejsów określonych w odpowiednich TSI), aby identyfikować zagrożenia dotyczące tych interfejsów i środki bezpieczeństwa związane z tymi zagrożeniami oraz wspólnie nimi zarządzać. Zarządzanie wspólnym ryzykiem na interfejsach jest koordynowane przez wnioskodawcę.

[G 1] Przykładowo, jeśli ze względów eksploatacyjnych przedsiębiorstwo kolejowe potrzebuje zarządcy infrastruktury w celu przeprowadzenia określonych zmian w infrastrukturze, zgodnie z wymogami załącznika III ust. 2 lit. g) dyrektywy w sprawie bezpieczeństwa kolei

European Railway Agency ● Marc LEFRANCQ, 120 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

{Ref. 1}, przedsiębiorstwo kolejowe monitoruje również całość prac, aby oczekiwane zmiany zostały przeprowadzane we właściwy sposób. Niemniej jednak przywództwo przedsiębiorstwa kolejowego nie zwalnia powiązanego zarządcy infrastruktury z obowiązku informowania innych przedsiębiorstw kolejowych o danej zmianie w infrastrukturze, jeśli taka zmiana będzie miała wpływ także na te przedsiębiorstwa. Zarządca infrastruktury może nawet być zmuszony do przeprowadzenia oceny ryzyka zgodnie z CSM, jeśli dana zmiana okaże się znacząca z punktu widzenia CSM.

[G 2] Przenoszenie odpowiedzialności pomiędzy różnymi podmiotami jest możliwe i w niektórych przypadkach wręcz konieczne. Niemniej, w przypadku gdy kilka podmiotów jest zaangażowanych w system, bardzo często wyznacza się jeden podmiot jako odpowiedzialny za całość systemu. Zawsze istnieją zależności pomiędzy podsystemami i operacjami, których rozpoznanie wymaga szczególnych wysiłków. Konieczne jest zatem, aby ktoś wziął na siebie całą odpowiedzialność za analizy bezpieczeństwa, a także posiadał pełny dostęp do całej dokumentacji w tym zakresie. Oczywiście wnioskodawca, który zamierza wprowadzić znaczącą zmianę, ponosi zazwyczaj ogólną odpowiedzialność za systematyczne prowadzanie i kompletność oceny ryzyka.

[G 3] Do najważniejszych kryteriów, które należy ustalić w odniesieniu do zarządzania powiązaniami między zainteresowanymi podmiotami, należą:

(a) przywództwo, które zwykle zapewnia wnioskodawca, który ma zamiar wprowadzić znaczącą zmianę;
(b) wymagane dane wejściowe;
(c) metody identyfikacji zagrożenia i oceny ryzyka;
(d) wymagani uczestnicy o niezbędnych kompetencjach (tj. połączenie wiedzy, umiejętności i doświadczenia praktycznego w danym zakresie – zob. również definicję „kompetencji personelu” w pkt. [G 2] lit. b) w objaśnieniu do art. 3 w {Ref. 4});
(e) oczekiwane rezultaty.

Powyższe kryteria opisano w planach bezpieczeństwa (lub w jakichkolwiek innych stosownych dokumentach) spółek, które zajmują się tymi oddziaływaniami.

[G 4] Przykłady płaszczyzn oddziaływań znajdują się w części C.3. załącznika C, podobnie jak przykład zastosowania tych głównych kryteriów w odniesieniu do zarządzania interfejsami pomiędzy producentem pociągu a zarządcą infrastruktury lub przedsiębiorstwem kolejowym.

[G 5] Zarządzanie interfejsami to również uwzględnienie ryzyka, które może się pojawić na interfejsach z operatorami maszyn (wykorzystywanymi podczas eksploatacji i utrzymania ruchu) w celu projektowania tych interfejsów.

1.2.2. Jeżeli podmiot stwierdzi, że istnieje potrzeba zastosowania środka bezpieczeństwa, którego nie jest w stanie wdrożyć samodzielnie, podmiot ten, działając w porozumieniu z innym podmiotem, przenosi na niego zarządzanie danym zagrożeniem zgodnie z procedurą opisaną w sekcji 4.

[G 1] Proces przenoszenia odpowiedzialności za zagrożenia i powiązanych z nimi środków bezpieczeństwa jest również stosowany na niższych poziomach modelu V według CENELEC na Schemat 5 na str. 35. Można go stosować, ilekroć pojawi się konieczność wymiany tego rodzaju informacji, na przykład pomiędzy podmiotem a jego podwykonawcami. Różnica w stosunku do takiego samego procesu na poziomie systemu polega na tym, że wnioskodawca nie musi być informowany o wszystkich przypadkach przeniesienia zarządzania zagrożeniami i powiązanymi środkami bezpieczeństwa na poziomie

European Railway Agency ● Marc LEFRANCQ, 120 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

podsystemu. Wnioskodawcę informuje się tylko w przypadku, gdy przenoszona odpowiedzialność za zagrożenia i powiązane z tym środki bezpieczeństwa dotyczą interfejsów na wysokim poziomie (tj. kiedy znajdują one swoje odzwierciedlenia w interfejsie z wnioskodawcą).

1.2.3. Każdy podmiot, który stwierdzi, że środek bezpieczeństwa dotyczący ocenianego systemu jest niezgodny lub nieodpowiedni, ma obowiązek zgłosić to wnioskodawcy, który z kolei poinformuje podmiot wprowadzający ten środek bezpieczeństwa.

[G 1] System zarządzania bezpieczeństwem przedsiębiorstwa kolejowego i zarządcy infrastruktury obejmuje ustalenia i procedury, które mają na celu zapewnienie właściwego zarządzania brakiem zgodności z wymogami i nieadekwatnością środków bezpieczeństwa, dlatego też te ustalenia i procedury nie są częścią CSM.

[G 2] Podobnie ustalenia i procedury[(11)], które mają być wdrożone przez pozostałe podmioty[(12)] w celu zapewnienia właściwego zarządzania brakiem zgodności z wymogami i nieadekwatnością środków bezpieczeństwa oraz - w miarę konieczności - przekazania środków bezpieczeństwa wszystkim zainteresowanym podmiotom, są uzgadniane pomiędzy zainteresowanymi podmiotami na początku projektu oraz wyszczególniane w ich planie bezpieczeństwa: zob. część 0.2.

1.2.4. Podmiot wprowadzający środek bezpieczeństwa poinformuje następnie wszystkie podmioty, których dotyczy problem w ramach ocenianego systemu lub (zgodnie z wiedzą podmiotu) w ramach innych istniejących systemów, w których stosowany jest ten sam środek bezpieczeństwa.

[G 1] Umożliwi to zatem zarządzanie możliwym brakiem zgodności z wymogami lub nieadekwatnością środka bezpieczeństwa w ramach systemu objętego oceną lub w ramach podobnych systemów korzystających z tego samego środka.

1.2.5. W przypadku niemożności osiągnięcia porozumienia pomiędzy dwoma podmiotami lub większą ich liczbą, za znalezienie odpowiedniego rozwiązania odpowiada wnioskodawca.

[G 1] Uznano, że dodatkowe wyjaśnienia nie są konieczne.

1.2.6. Jeżeli podmiot nie jest w stanie spełnić wymogu zawartego w zgłoszonym przepisie krajowym, wnioskodawca zwraca się o radę do właściwego organu.

[G 1] Uznano, że dodatkowe wyjaśnienia nie są konieczne.

---

(11) *Z reguły te ustalenia i procedury objęte są procesami zarządzania jakością lub zarządzania bezpieczeństwem przez te podmioty, ustalonymi co najmniej na etapie projektu (zob. również Schemat 2).*

(12) *Termin „pozostałe podmioty" oznacza wszystkie zainteresowane podmioty inne niż zarządcy infrastruktury i przedsiębiorstwa kolejowe.*

European Railway Agency ● Marc LEFRANCQ, 120 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

1.2.7.	*Niezależnie od definicji ocenianego systemu wnioskodawca jest zobowiązany zagwarantować, że zakres zarządzania ryzykiem obejmuje sam system oraz jego integrację z całym systemem kolejowym.*

[G 1] Uznano, że dodatkowe wyjaśnienia nie są konieczne.

European Railway Agency ● Marc LEFRANCQ, 120 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

2. OPIS PROCESU OCENY RYZYKA

2.1. Opis ogólny – Zgodność pomiędzy procesem oceny ryzyka CSM i modelem V według CENELEC

2.1.1. Proces oceny ryzyka jest całościowym, wieloetapowym procesem obejmującym:

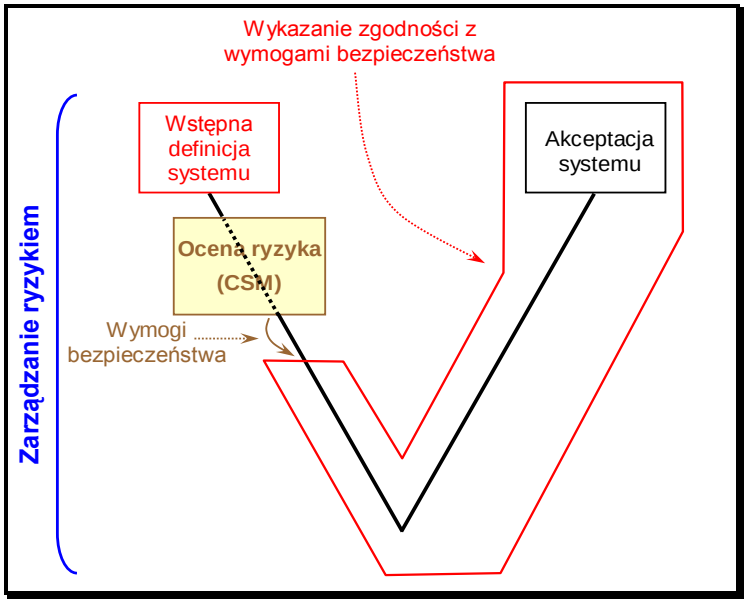
(a) zdefiniowanie systemu;
(b) analizę ryzyka, w tym identyfikację zagrożeń;
(c) wycenę ryzyka.

Proces oceny ryzyka jest powiązany z zarządzaniem zagrożeniami zgodnie z sekcją 4.1.

[G 1] Proces zarządzania ryzykiem objęty CSM można przedstawić w postaci modelu V, który rozpoczyna się od (wstępnej) definicji systemu i kończy się akceptacją systemu: zob. Schemat 4. Ten uproszczony model V można następnie nanieść na klasyczny model V na schemacie 10 normy EN 50 126-1 {Ref. 8}. W celu wykazania zgodności z procesem zarządzania ryzykiem CSM przedstawionym na Schemat 1, model V według CENELEC przedstawiony na schemacie 10 powtórzono na Schemat 5:

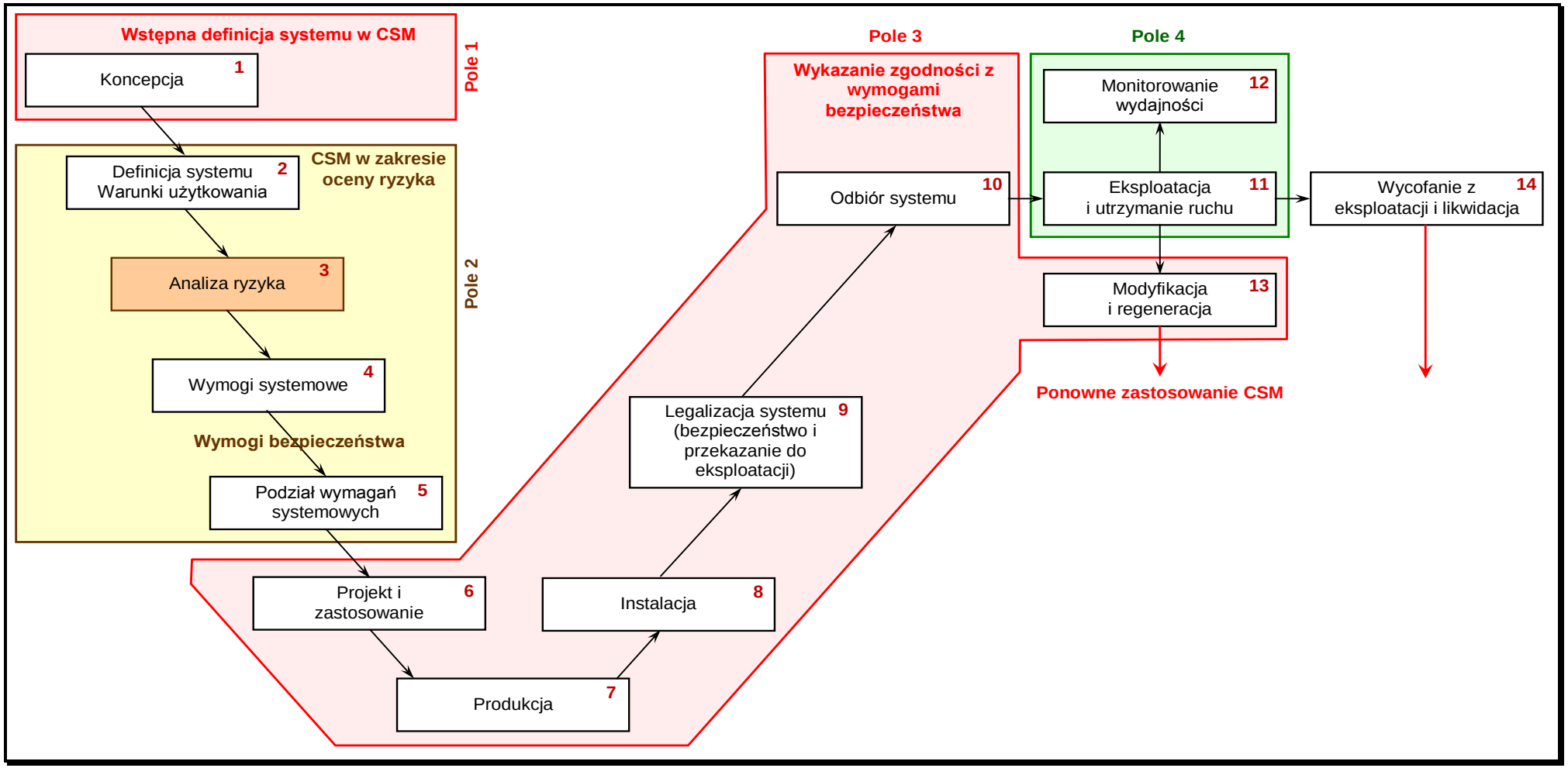
(a) „wstępna definicja systemu" CSM na Schemat 1 odpowiada fazie 1 modelu V według CENELEC, tj. definicji „koncepcji" systemu (zob. pole 1 na Schemat 5);
(b) „ocena ryzyka" CSM na Schemat 1 obejmuje następujące fazy modelu V według CENELEC (zob. pole 2 na Schemat 5):

(1) faza 2 na Schemat 5: „definicja systemu i warunki stosowania";
(2) faza 3 na Schemat 5: „analiza ryzyka";
(3) faza 4 na Schemat 5: „wymogi systemu";
(4) faza 5 na Schemat 5: „rozdział wymogów systemu" na różne podsystemy i elementy.



Schemat 4: Uproszczony model V ze schematu 10 normy EN 50 126.

European Railway Agency ● Marc LEFRANCQ, 120 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu



Schemat 5: Schemat 10 przedstawiający model V według normy EN 50 126 (cykl życia systemy CENELEC).

European Railway Agency ● Marc LEFRANCQ, 120 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

[G 2] Rezultaty procesu oceny ryzyka w CSM (po przeprowadzeniu iteracji – zob. Schemat 1 są następujące:

(a) „definicja systemu" zaktualizowana o „wymogi bezpieczeństwa" będące wynikiem działań związanych z „analizą ryzyka" i „wyceną ryzyka" (zob. część 2.1.6);
(b) „rozdział wymogów systemu" na różne podsystemy i elementy (faza 5 na Schemat 5);
(c) „rejestr zagrożeń" zawierający:

(1) wszystkie zidentyfikowane zagrożenia i powiązane środki bezpieczeństwa;
(2) wynikowe wymogi bezpieczeństwa;
(3) założenia uwzględnione w odniesieniu do systemu, które wyznaczają zakres i ważność oceny ryzyka (zob. część 2.1.2 lit. (g));

(d) i ogólnie wszelkie dowody wynikające z zastosowania CSM: zob. część 5.

Te rezultaty oceny ryzyka CSM odpowiadają rezultatom fazy 4 modelu V według CENELEC związanym z bezpieczeństwem, tj. specyfikacji wymogów systemowych na Schemat 5.

[G 3] Definicja systemu zaktualizowana o wyniki oceny ryzyka oraz rejestr zagrożeń stanowi dane wyjściowe, na podstawie których system jest projektowany i dopuszczany. „Wykazanie zgodności sytemu z wymogami bezpieczeństwa" w CSM odpowiada następującym fazom modelu V według CENELEC (zob. pole 3 na Schemat 5):

(a) faza 6 na Schemat 5: „projekt i wdrożenie";
(b) faza 7 na Schemat 5: „produkcja";
(c) faza 8 na Schemat 5: „instalacja";
(d) faza 9 na Schemat 5: „walidacja systemu (w tym akceptacja pod względem bezpieczeństwa i przekazanie do eksploatacji)";
(e) faza 10 na Schemat 5: „akceptacja systemu".

[G 4] Wykazanie zgodności systemu z wymogami bezpieczeństwa zależy od tego, czy znacząca zmiana ma charakter techniczny, eksploatacyjny czy organizacyjny. Dlatego też różne etapy modelu V według CENELEC na Schemat 5 mogą nie być odpowiednie dla wszystkich znaczących zmian danego rodzaju. Należy odpowiednio dostosować model V na Schemat 5 i ocenić, co pasuje do każdego konkretnego zastosowania (np. w przypadku zmian eksploatacyjnych i organizacyjnych nie występuje faza produkcji).

[G 5] Oznacza to, że „wykazanie zgodności systemu z wymogami bezpieczeństwa" w CSM nie obejmuje jedynie działań związanych z „weryfikacją i walidacją" poprzez testy lub symulację. W praktyce etap ten obejmuje wszystkie fazy „od 6 do 10" (zob. listę powyżej i Schemat 5) w model V według CENELEC. Obejmują one działania związane z projektem, produkcją, instalacją, weryfikacją i walidacją, jak również powiązane czynności dotyczące niezawodności, dostępności, podatności utrzymaniowej i bezpieczeństwa (RAMS) oraz akceptację systemu.

[G 6] W trakcie „wykazania zgodności systemu z wymogami bezpieczeństwa" ogólna zasada polega na tym, aby ocena ryzyka koncentrowała się jedynie na funkcjach związanych z bezpieczeństwem i interfejsach systemu. Oznacza to, że ilekroć w zakresie jednej z faz w modelu V według CENELEC przedstawionego na Schemat 5 wymagane są działania związane z oceną ryzyka i bezpieczeństwa, koncentrują się one na:

(a) funkcjach związanych z bezpieczeństwem i płaszczyznach oddziaływania;
(b) podsystemach lub składnikach zapewniających uzyskanie funkcji związanych z bezpieczeństwem lub interfejsami poddawanymi ocenie w trakcie działań w zakresie oceny ryzyka na wyższym poziomie.

European Railway Agency ● Marc LEFRANCQ, 120 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

[G 7] Z porównania CSM z klasycznym modelem V według CENELEC przedstawionym na Schemat 5 wynika zatem, że:

(a) CSM obejmują fazy „od 1 do 10" i „13" tego modelu V. Obejmują one szereg działań wymaganych w celu akceptacji systemu objętego oceną:

(b) CSM nie obejmują faz „11", „12" i „14" cyklu życia systemu:

(1) fazy „11" i „12" odpowiednio odnoszą się do „eksploatacji i utrzymania" oraz „monitorowania wydajności" systemu po jego akceptacji w oparciu o CSM. Te dwie fazy są objęte systemem zarządzania bezpieczeństwem przedsiębiorstwa kolejowego i zarządcy infrastruktury (zob. pole 4 na Schemat 5). Niemniej jednak, jeżeli w trakcie eksploatacji, utrzymania ruchu lub monitorowania wydajności systemu pojawia się konieczność zmodyfikowania i modernizacji systemu (faza 13 na Schemat 5), który już wprowadzono do eksploatacji, CSM są ponownie stosowane w odniesieniu do nowych wymaganych zmian zgodnie z Artykuł 2. W związku z tym, jeżeli zmiana jest znacząca:

(i) procesy zarządzania ryzykiem i oceny ryzyka w zakresie CSM są stosowane w odniesieniu do tych nowych zmian;
(ii) konieczna jest akceptacja tych nowych zmian zgodnie z Artykuł 6;

(2) „wycofanie z eksploatacji i likwidacja" systemu już wprowadzonego do eksploatacji (faza 14) również można uznać za znaczącą zmianę, dlatego też ponownie można zastosować CSM zgodnie z Artykuł 2 w odniesieniu do fazy 14 na Schemat 5.

Więcej informacji na temat zakresu każdej fazy lub działania w modelu V według CENELEC przytoczonym na Schemat 5 można znaleźć w części § 6 normy EN 50 126-1 {Ref. 8}.

2.1.2. Definicja systemu powinna uwzględniać co najmniej:

(a) cel systemu, np. zamierzone przeznaczenie;
(b) funkcje i elementy systemu, jeżeli ma to zastosowanie (w tym np. element ludzki, techniczny i operacyjny);
(c) granicę systemu, z uwzględnieniem innych systemów, z którymi system ten wzajemnie oddziałuje;
(d) interfejsy fizyczne (tj. systemy, z którymi system ten wzajemnie oddziałuje) i funkcjonalne (tj. nakłady i efekty dotyczące działania);
(e) otoczenie systemu (np. przepływy energii i przepływy termiczne, wstrząsy, wibracje, zakłócenia elektromagnetyczne, przeznaczenie eksploatacyjne);
(f) istniejące środki bezpieczeństwa oraz definicja wymogów bezpieczeństwa określonych w drodze procesu oceny ryzyka (na kolejnych etapach);
(g) założenia określające progi mające zastosowanie do oceny ryzyka.

[G 1] Uznano, że dodatkowe wyjaśnienia nie są konieczne.

2.1.3. Identyfikacja zagrożenia dotyczy zdefiniowanego systemu, zgodnie z sekcją 2.2.

[G 1] Uznano, że dodatkowe wyjaśnienia nie są konieczne.

European Railway Agency ● Marc LEFRANCQ, 120 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

2.1.4. Dopuszczalność ryzyka dotyczącego ocenianego systemu jest badana za pomocą jednej lub kilku z poniższych zasad akceptacji ryzyka:

(a) stosowanie kodeksów postępowania (sekcja 2.3);
(b) porównanie z podobnymi systemami (sekcja 2.4);
(c) szacowanie jawnego ryzyka (sekcja 2.5).

Zgodnie z ogólną zasadą, o której mowa w sekcji 1.1.5, jednostka oceniająca nie narzuca wnioskodawcy zasady akceptacji ryzyka, którą powinien stosować.

[G 1] Zazwyczaj wnioskodawca będzie decydować, jaka zasada akceptacji ryzyka jest najbardziej odpowiednia do nadzorowania ustalonych zagrożeń w oparciu o szczegółowe wymogi projektu, jak również w oparciu o swoje doświadczenie związane z tymi trzema zasadami.

[G 2] Nie zawsze możliwa jest ocena dopuszczalności ryzyka na poziomie systemu poprzez zastosowanie tylko jednej z trzech metod akceptacji ryzyka. Akceptacja ryzyka często wynika z zastosowania wszystkich zasad. Jeżeli w odniesieniu do znaczącego zagrożenia konieczne jest zastosowanie większej liczby zasad akceptacji ryzyka niż jedna w celu nadzorowania powiązanego ryzyka, dane zagrożenie należy podzielić na zagrożenia cząstkowe, tak aby każde poszczególne zagrożenie cząstkowe było należycie kontrolowane poprzez jedną tylko zasadę akceptacji ryzyka.

[G 3] Podejmując decyzję o nadzorowaniu zagrożenia poprzez zasadę akceptacji ryzyka, należy uwzględnić zagrożenie i przyczyny tego zagrożenia, które już zostały rozpoznane w fazie identyfikacji zagrożenia. Jeżeli zatem dwie różne i niezależne przyczyny są związane z tym samym zagrożeniem, zagrożenie takie należy podzielić na dwa różne zagrożenia cząstkowe. Każde zagrożenie cząstkowe będzie wówczas nadzorowane poprzez jedną zasadę akceptacji ryzyka. Obydwa zagrożenia cząstkowe należy wciągnąć na listę zagrożeń i kontrolować je. Na przykład, jeżeli zagrożenie jest spowodowane błędem w projekcie, można nim zarządzać poprzez zastosowanie kodeksów postępowania, zaś jeśli przyczyną zagrożenia jest błąd w utrzymaniu, same kodeksy postępowania mogą nie wystarczyć; wówczas konieczne jest zastosowanie innej zasady akceptacji ryzyka.

[G 4] Aby zmniejszyć ryzyko do dopuszczalnego poziomu, konieczne może być przeprowadzenie kilku iteracji między fazą analizy ryzyka a fazą wyceny ryzyka, aż do wskazania odpowiednich środków bezpieczeństwa.

[G 5] Istniejące ryzyko szczątkowe wynikające z praktycznego doświadczenia istniejących systemów i systemów będących efektem zastosowania kodeksów postępowania jest uznawane za dopuszczalne. Ryzyko wynikające z jednoznacznego oszacowania ryzyka jest oparte na opinii eksperta i różnych założeniach sformułowanych przez niego w trakcie analiz lub na bazach danych związanych z doświadczeniem w podobnych przypadkach i doświadczeniem eksploatacyjnym. W związku z tym nie można potwierdzić ryzyka szczątkowego wynikającego z jednoznacznego oszacowania ryzyka bezpośrednio na podstawie doświadczenia. Aby je wykazać, potrzebny jest czas na eksploatację, monitorowanie powiązanych systemów i uzyskanie miarodajnego doświadczenia. Ogólnie, zastosowanie kodeksów postępowania i porównanie z podobnymi systemami odniesienia jest bardziej korzystne, ponieważ pozwala uniknąć przesadnie szczegółowego określania zbyt surowych wymogów bezpieczeństwa, które mogą być wynikiem nadmiernie konserwatywnych założeń (dotyczących bezpieczeństwa) przyjętych przy szacowaniu jawnego ryzyka. Może się jednak zdarzyć, że w przypadku systemu objętego oceną spełnienie niektórych wymogów bezpieczeństwa z kodeksów postępowania lub podobnych systemów odniesienia nie jest konieczne. W takim wypadku zastosowanie szacowania jawnego ryzyka byłoby bardziej korzystne, aby uniknąć niepotrzebnego i nadmiernego

European Railway Agency ● Marc LEFRANCQ, 120 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

projektowania systemu objętego oceną i umożliwiłoby bardziej efektywne kosztowo projektowanie, które nie zostało wypróbowane wcześniej.

[G 6] W przypadku gdy zidentyfikowane zagrożenia i powiązane z nimi ryzyko dla systemu objętego oceną nie mogą być kontrolowane poprzez zastosowanie kodeksów postępowania lub podobnych systemów odniesienia, przeprowadzane jest szacowanie jawnego ryzyka w oparciu o ilościowe i jakościowe analizy niebezpiecznych zdarzeń. Taka sytuacja ma miejsce, gdy system objęty oceną jest całkowicie nowy (lub projekt jest innowacyjny) lub gdy system odbiega od kodeksu postępowania lub systemu odniesienia. Szacowanie jawnego ryzyka pozwoli następnie stwierdzić, czy ryzyko jest dopuszczalne (a więc dalsza analiza nie jest konieczna) lub czy konieczne jest podjęcie dodatkowych środków bezpieczeństwa w celu dalszego ograniczenia ryzyka.

[G 7] Wskazówki dotyczące ograniczania ryzyka i akceptacji ryzyka można również znaleźć w części § 8 Wytycznych do normy EN 50 126-2 {Ref. 9}.

[G 8] Jednostka oceniająca musi ocenić użytą zasadę akceptacji ryzyka i jej zastosowanie.

2.1.5. Wnioskodawca wykazuje w wycenie ryzyka, że wybrana zasada akceptacji ryzyka została odpowiednio zastosowana. Wnioskodawca sprawdza ponadto, czy wybrane zasady akceptacji ryzyka są stosowane konsekwentnie.

[G 1] Na przykład, jeżeli w odniesieniu do oprogramowania elementu jako wymóg bezpieczeństwa podano zastosowanie procesu opracowywania SIL 4 według normy EN 50 128, wówczas należy wykazać, że proces zalecany w normie jest stosowany. Na przykład, należy wykazać, że:

(a) spełnione są wymogi dotyczące niezależności w przygotowaniu projektu, weryfikacji i walidacji oprogramowania;
(b) stosowane są właściwe metody z normy EN 50 128 dotyczące poziomu integralności bezpieczeństwa (SIL 4);
(c) itp.

[G 2] Jeżeli na przykład do produkcji zaworów elektromagnetycznych hamulca awaryjnego ma być zastosowana oddzielny kodeks postępowania, należy wykazać, że wszystkie wymogi kodeksu postępowania są spełnione w trakcie procesu produkcji.

2.1.6. 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, które powinien spełniać system. Zgodność z tymi wymogami bezpieczeństwa jest wykazywana zgodnie z sekcją 3.

[G 1] Można wskazać dwa rodzaje środków bezpieczeństwa:

(a) „zapobiegawcze środki bezpieczeństwa" zapobiegające wystąpieniu zagrożeń lub ich przyczyn, oraz
(b) „łagodzące środki bezpieczeństwa" zapobiegające przekształceniu się zagrożeń w wypadki lub ograniczające konsekwencje wypadków po ich zaistnieniu (środki ochronne).

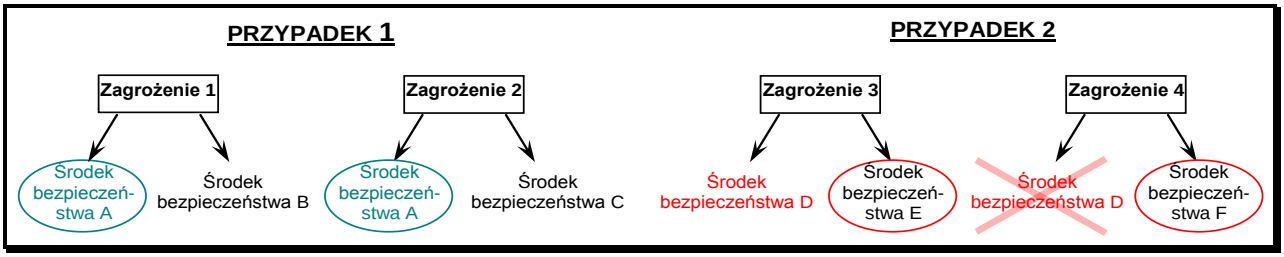
European Railway Agency ● Marc LEFRANCQ, 120 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

Zapobieganie przyczynom jest generalnie bardziej skutecznym sposobem na zapewnienie sprawnego działania.

[G 2] Wnioskodawca uzna za najbardziej odpowiednie te środki bezpieczeństwa, które zapewnią najlepszy kompromis pomiędzy kosztami obniżenia ryzyka i poziomem ryzyka szczątkowego. Wybrane środki bezpieczeństwa stają się wymogami bezpieczeństwa dla systemu objętego oceną.

[G 3] Należy się upewnić, że środki bezpieczeństwa wybrane w celu kontrolowania jednego zagrożenia nie są sprzeczne z innymi zagrożeniami. Jak przedstawiono na Schemat 6, mogą zaistnieć na przykład następujące dwie sytuacje[(13)]:

(a) PRZYPADEK 1: jeżeli ten sam środek bezpieczeństwa (środek A na Schemat 6) może kontrolować różne zagrożenia nie tworząc sprzeczności pomiędzy nimi i jest uzasadniony ze względów ekonomicznych, można wskazać ten jeden środek bezpieczeństwa jako „wymóg bezpieczeństwa" związany z tymi zagrożeniami. Ogólna liczba wymogów bezpieczeństwa, które należy spełnić, jest mniejsza niż w przypadku wdrażania zarówno środka B, jak i C;



Schemat 6: Wybór odpowiednich środków bezpieczeństwa do kontrolowania ryzyka.

(b) PRZYPADEK 2: i odwrotnie, jeżeli jeden środek bezpieczeństwa może kontrolować jedno zagrożenie, ale jest sprzeczny z innym zagrożeniem (środek D na Schemat 6), nie można go wskazać jako "wymóg bezpieczeństwa". Należy zastosować inne środki bezpieczeństwa w odniesieniu do rozpatrywanego zagrożenia (środki E i F na Schemat 6):

(1) Typowym przykładem w systemie sterowania ruchem kolejowym jest wykorzystanie lokalizacji pociągu na torach do kontrolowania uruchamiania hamulca, albo w celu zezwolenia na przyspieszenie pociągu. Wykorzystanie czoła pociągu do lokalizacji pociągu (w stosunku do końca pociągu) nie jest bezpieczne we wszystkich sytuacjach:

(i) kiedy system sterowania ruchem pociągu ETCS ma bezpiecznie uruchomić hamulce awaryjne, wykorzystuje MAKSYMALNE BEZPIECZNE POŁOŻENIE CZOŁA POCIĄGU, aby zagwarantować, że czoło pociągu rzeczywiście zatrzyma się przez niebezpiecznym punktem;

(ii) i odwrotnie: jeżeli na przykład pociąg ma przyspieszyć po okresie jazdy z ograniczoną prędkością, system sterowania ruchem pociągu ETCS wykorzystuje MINIMALNE BEZPIECZNE POŁOŻENIE KOŃCA POCIĄGU;

(2) Kolejnym przykładem jest środek bezpieczeństwa, który mógłby być odpowiedzialny za zatrzymanie pociągu niemalże w każdych okolicznościach, z

(13) *Należy zaznaczyć, że przewodnik nie wylicza wszystkich sytuacji, w których środki bezpieczeństwa mogłyby być sprzeczne z innymi zidentyfikowanymi zagrożeniami. Zapewniono jedynie kilka przykładów ilustrujących.*

European Railway Agency ● Marc LEFRANCQ, 120 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

wyjątkiem tunelu lub mostu, tak aby pociąg był bezpieczny w razie awarii. W tym drugim przypadku, nie należy uwzględniać środka D w PRZYPADKU 2 na Schemat 6.

2.1.7. Wieloetapowy proces oceny ryzyka można uznać za zakończony, gdy wykazane zostanie, że wszystkie wymogi bezpieczeństwa zostały spełnione i nie istnieje potrzeba uwzględnienia jakichkolwiek dodatkowych, racjonalnie przewidywalnych zagrożeń.

[G 1] W zależności - na przykład - od technicznych rozwiązań podczas projektowania systemu, jego podsystemów i sprzętu, nowe zagrożenia mogłyby zostać zidentyfikowane w trakcie „wykazania zgodności z wymogami bezpieczeństwa" (np. użycie niektórych farb mogłoby doprowadzić do powstania toksycznych gazów w razie pożaru). Te nowe zagrożenia i powiązane z nimi ryzyko należy uznać za nowe dane wejściowe dla kolejnego cyklu w powtarzalnym procesie zarządzania ryzykiem. Załącznik A.4.3 do normy EN 50 129 zawiera inne przykłady sytuacji, w których mogą się pojawić nowe zagrożenia, które należy nadzorować.

2.2. Identyfikacja zagrożeń

2.2.1. Wnioskodawca, korzystając z szerokiej wiedzy specjalistycznej kompetentnego zespołu, identyfikuje regularnie wszystkie racjonalnie przewidywalne zagrożenia dotyczące całego ocenianego systemu, jego funkcji (jeżeli ma to zastosowanie) i interfejsów.

Wszystkie zidentyfikowane zagrożenia są umieszczane w rejestrze zagrożeń zgodnie z sekcją 4.

[G 1] W miarę możliwości zagrożenia są opisywane na tym samym poziomie szczegółowości. Podczas wstępnych analiz zagrożeń może się zdarzyć, że zidentyfikowane zostaną zagrożenia o różnych stopniach szczegółowości (np. ponieważ w analizie metodą HAZOP uczestniczyły osoby posiadające różne doświadczenie).
Poziom szczegółowości zależy również od zasady akceptacji ryzyka, którą wybrano w celu kontrolowania zidentyfikowanych zagrożeń. Na przykład, jeżeli zagrożenie jest w całości nadzorowane dzięki kodeksowi postępowania lub podobnemu systemowi odniesienia, bardziej szczegółowa identyfikacja zagrożenia nie jest konieczna.

[G 2] Wszystkie zagrożenia zidentyfikowane w procesie oceny ryzyka (w tym zagrożenia związane z ogólnie akceptowalnym ryzykiem), w powiązanych środkach bezpieczeństwa i powiązanych rodzajach ryzyka należy zamieścić w rejestrze zagrożeń.

[G 3] W zależności od charakteru analizowanego systemu, można zastosować różne metody identyfikacji zagrożeń:

(a) empiryczną identyfikację zagrożeń można zastosować wykorzystując wcześniejsze doświadczenia (np. wykorzystanie list kontrolnych lub wykazu ogólnych zagrożeń);
(b) kreatywną identyfikację zagrożeń można zastosować w przypadku nowych obszarów zainteresowania (zapobiegawcze prognozy, np. badania skonstruowane wokół pytania „a co, jeśli" prowadzone takimi metodami, jak FMEA lub HAZOP).

[G 4] Empiryczne i kreatywne metody identyfikacji zagrożeń można stosować łącznie, aby się uzupełniały w celu zagwarantowania, że lista potencjalnych zagrożeń i środków bezpieczeństwa, w stosownych przypadkach, jest wyczerpująca.

European Railway Agency ● Marc LEFRANCQ, 120 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

[G 5] Wstępem do identyfikacji ryzyka może być przeprowadzenie narady metodą burzy mózgów przez zespół składający się z ekspertów posiadających różne kompetencje, odpowiadające wszelkim istotnym aspektom znaczącej zmiany. W stosownych przypadkach, określonych przez panel ekspertów, można stosować metody empiryczne w celu przeprowadzenia analizy konkretnego trybu funkcyjnego lub eksploatacyjnego.

[G 6] Metody wykorzystywane w celu zidentyfikowania zagrożenia zależą od definicji systemu. Kilka przykładów podano w załączniku B.

[G 7] Więcej informacji na temat technik i metod identyfikacji zagrożeń można znaleźć w załącznikach A.2 i E Wytycznych do norm EN 50 126-2 {Ref. 9}.

[G 8] Przykładową listę ogólnych zagrożeń podano w części C.17. załącznika C.

2.2.2. Aby w ocenie móc skupić się na najważniejszym ryzyku, zagrożenia należy klasyfikować według wynikającego z nich szacowanego ryzyka. Jeżeli tak wskazuje fachowy osąd, zagrożenia związane z zasadniczo dopuszczalnym ryzykiem nie muszą być głębiej analizowane, należy je jednak umieścić w rejestrze zagrożeń. Klasyfikacja zagrożeń powinna być opatrywana uzasadnieniem, aby umożliwić jednostce oceniającej jej niezależną ocenę.

[G 1] Aby ułatwić proces oceny ryzyka, znaczące zagrożenia, można dodatkowo podzielić na różne kategorie. Na przykład, znaczące zagrożenia można sklasyfikować lub uszeregować według oczekiwanego stopnia ryzyka z nimi związanego i częstotliwości występowania. Wytyczne do tego rodzaju zadania można znaleźć w normach CENELEC: zob. część A.2. załącznika A.

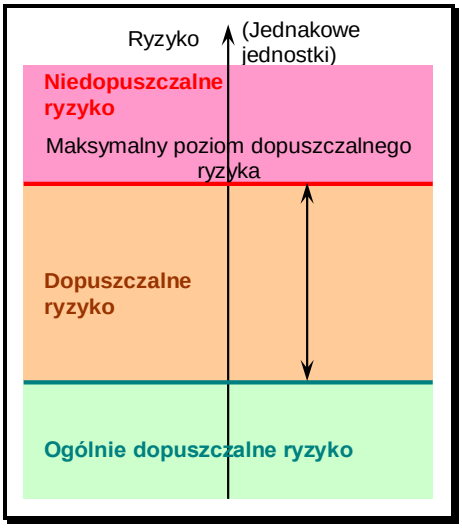
[G 2] Analizę i wycenę ryzyka, które opisano w części 2.1.4, stosuje się na zasadzie ustalania priorytetów, poczynając od najwyżej uszeregowanych zagrożeń.

2.2.3. Ryzyka wynikające z zagrożeń mogą zostać zaklasyfikowane jako zasadniczo dopuszczalne, gdy spełnione jest kryterium, zgodnie z którym ryzyko powinno być na tyle małe, że wprowadzanie jakichkolwiek dodatkowych środków bezpieczeństwa jest nieracjonalne. Podczas fachowego osądu należy zwrócić uwagę, czy suma zasadniczo dopuszczalnego ryzyka nie przekracza określonego udziału w ryzyku całkowitym.

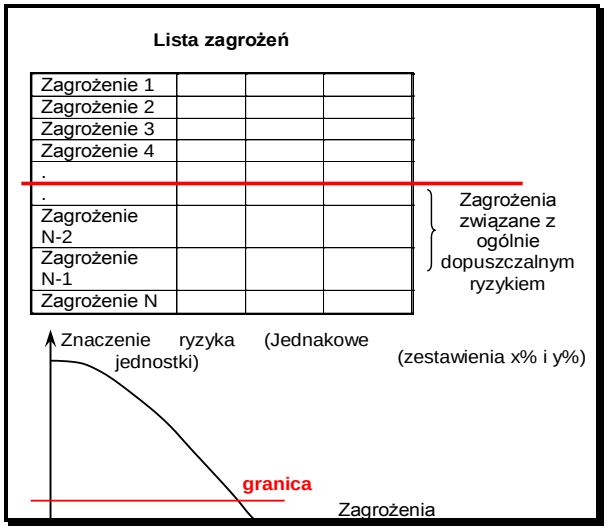
[G 1] Na przykład ryzyko związane z zagrożeniem można uznać za ogólnie dopuszczalne, jeśli:

(a) ryzyko jest niższe niż dany procent (np. x%) maksymalnego dopuszczalnego ryzyka w odniesieniu do tego rodzaju zagrożenia. Wartość x% można ustalić w oparciu o najlepszą praktykę i doświadczenie z różnymi podejściami do analizy ryzyka, np. stosunek pomiędzy ogólnie dopuszczalnym ryzykiem i klasyfikacjami niedopuszczalnego ryzyka przedstawiony w postaci krzywych F-N lub na matrycach ryzyka. Można to przedstawić w taki sposób, jak pokazano na Schemat 7;
(b) lub strata związana z ryzykiem jest tak mała, że stosowanie jakichkolwiek środków bezpieczeństwa nie jest uzasadnione.

European Railway Agency ● Marc LEFRANCQ, 120 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu



Schemat 7: Ogólnie dopuszczalne ryzyko



Schemat 8: Selekcjonowanie zagrożeń związanych z ogólnie dopuszczalnym ryzykiem.

[G 2] Jeżeli ponadto zidentyfikowane zostaną zagrożenia o różnych poziomach szczegółowości (tj. z jednej strony wysokie zagrożenia, a z drugiej szczegółowe zagrożenia cząstkowe), należy podjąć środki ostrożności, aby uniknąć nieprawidłowego sklasyfikowania takich zagrożeń jako zagrożeń związanych z ogólnie akceptowalnym ryzykiem. Udział wszystkich zagrożeń związanych z ogólnie akceptowalnym ryzykiem nie może przekroczyć danej proporcji (np. y%) całego ryzyka na poziomie systemu. Takie zestawienie jest konieczne, aby uniemożliwić wypaczenie zasadności tej metody poprzez dzielenie zagrożeń na wiele zagrożeń cząstkowych o niskim poziomie ryzyka. Niewątpliwie, jeżeli jedno zagrożenie zostanie przedstawione w postaci wielu różnych „mniejszych" zagrożeń cząstkowych, wówczas, jeśli się je oceni oddzielnie, każde z nich można łatwo sklasyfikować jako powiązane z ogólnie dopuszczalnym ryzykiem, ale jeśli się je oceni razem, będą powiązane ze znaczącym ryzykiem (tj. jako jedno wysokie zagrożenie). Wartość proporcji (np. y%) zależy od kryteriów akceptacji ryzyka stosowanych na poziomie systemu i można ją wyliczyć na podstawie doświadczeń związanych z eksploatacją podobnych systemów odniesienia.

[G 3] Te dwa sprawdziany (w porównaniu do x% i y%) umożliwiają skoncentrowanie się na najważniejszych zagrożeniach podczas oceny ryzyka, jak również zapewnienie kontrolowania każdego znaczącego ryzyka (zob. Schemat 8).
Nie naruszając przepisów prawnych państwa członkowskiego, wnioskodawca ma obowiązek określić, na podstawie opinii eksperta, wartości x% i y% oraz poddać je niezależnej ocenie przez organ oceniający. Przykładem rzędów wielkości mogą być x = 1% i y = 10%, o ile zostaną uznane za dopuszczalne w opinii eksperta.

[G 4] Zgodnie z wymogami części 2.2.2, klasyfikacja ryzyka jako „ogólnie akceptowalnego" jest niezależnie oceniana przez jednostkę oceniającą.

2.2.4. Podczas identyfikacji zagrożeń mogą zostać określone środki bezpieczeństwa. Należy je umieścić w rejestrze zagrożeń zgodnie z sekcją 4.

[G 1] Głównym celem tego działania jest identyfikacja zagrożeń, które są powiązane ze zmianą. W przypadku gdy środki bezpieczeństwa są już wskazane, należy je zamieścić w rejestrze

European Railway Agency ● Marc LEFRANCQ, 120 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

zagrożeń. Charakter środków zależy od zmiany; mogą one być proceduralne, techniczne, eksploatacyjne i organizacyjne.

2.2.5.	*Identyfikacja zagrożeń powinna być dokonywana na poziomie szczegółowości, który jest konieczny, aby określić przypadki, w których środki bezpieczeństwa powinny utrzymywać ryzyko pod kontrolą zgodnie z jedną z zasad akceptacji ryzyka, o których mowa w pkt 2.1.4. W związku z tym konieczne może być powtarzanie etapów analizy ryzyka i wyceny ryzyka do czasu osiągnięcia dostatecznego poziomu szczegółowości, aby możliwa była identyfikacja zagrożenia.*

[G 1] Nawet jeśli ryzyko jest nadzorowane i utrzymywane na dopuszczalnym poziomie, wnioskodawca nadal może podjąć decyzję, że konieczna jest bardziej szczegółowa identyfikacja zagrożenia. Jednym z powodów takiej decyzji może być prawdopodobieństwo, że w trakcie przeprowadzania bardziej szczegółowej identyfikacji zagrożeń znalezione zostaną bardziej efektywne pod względem kosztów środki bezpieczeństwa w celu nadzorowania ryzyka.

2.2.6.	*W każdym przypadku gdy ryzyko jest kontrolowane za pomocą kodeksu postępowania lub systemu odniesienia, identyfikację zagrożeń można ograniczyć do:* *(a) sprawdzenia, czy kodeks postępowania lub system odniesienia są właściwe w danym przypadku.* *(b) wskazania niezgodności z kodeksem postępowania lub systemem odniesienia.*

[G 1] Uznano, że dodatkowe wyjaśnienia nie są konieczne.

2.3. Korzystanie z kodeksów postępowania przy wycenie ryzyka

2.3.1.	*Wnioskodawca bada, z pomocą innych zaangażowanych podmiotów i kierując się wymogami wymienionymi w pkt 2.3.2, czy zagrożenie lub zagrożenia są objęte zakresem odpowiednich kodeksów postępowania.*

[G 1] Uznano, że dodatkowe wyjaśnienia nie są konieczne.

2.3.2.	*Kodeksy postępowania spełniają przynajmniej następujące wymagania:* *(a) są powszechnie uznane w branży kolejowej; w przeciwnym wypadku kodeks postępowania należy uzasadnić i powinien on być akceptowalny dla jednostki oceniającej;* *(b) są relewantne z punktu widzenia nadzoru nad rozważanymi zagrożeniami występującymi w ocenianym systemie;* *(c) są publicznie dostępne dla wszystkich podmiotów, które chcą z nich korzystać.*

[G 1] Uznano, że dodatkowe wyjaśnienia nie są konieczne.

European Railway Agency ● Marc LEFRANCQ, 120 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

2.3.3.	*W przypadku gdy dyrektywa 2008/57/WE wymaga zgodności z TSI, a odpowiednie TSI nie nakładają obowiązku stosowania procesu zarządzania ryzykiem, który jest przewidziany w niniejszym rozporządzeniu, TSI mogą być uważane za kodeksy postępowania do celów nadzoru nad zagrożeniami, pod warunkiem, że spełniony jest wymóg, o którym mowa w pkt 2.3.2 lit. c).*

[G 1] Uznano, że dodatkowe wyjaśnienia nie są konieczne.

2.3.4.	*Krajowe przepisy zgłoszone zgodnie z art. 8 dyrektywy 2004/49/WE i art. 17 ust. 3 dyrektywy 2008/57/WE mogą być uważane za kodeksy postępowania, pod warunkiem że spełnione są wymogi, o których mowa w pkt 2.3.2.*

[G 1] Uznano, że dodatkowe wyjaśnienia nie są konieczne.

2.3.5.	*Jeżeli zagrożenie lub zagrożenia są kontrolowane za pomocą kodeksów postępowania spełniających wymogi, o których mowa w pkt 2.3.2, ryzyko związane z tymi zagrożeniami uważa się za dopuszczalne. Oznacza to, że:* *(a) nie istnieje potrzeba głębszego analizowania tego ryzyka;* *(b) stosowanie kodeksów postępowania zostaje odnotowane w rejestrze zagrożeń jako wymóg bezpieczeństwa w odniesieniu do odpowiednich zagrożeń.*

[G 1] Uznano, że dodatkowe wyjaśnienia nie są konieczne.

2.3.6.	*W przypadku gdy podejście alternatywne nie jest w pełni zgodne z kodeksem postępowania, wnioskodawca musi wykazać, że zastosowanie alternatywnego podejścia zapewnia co najmniej taki sam poziom bezpieczeństwa.*

[G 1] Uznano, że dodatkowe wyjaśnienia nie są konieczne.

2.3.7.	*Jeżeli ryzyko dotyczące określonego zagrożenia nie może zostać zredukowane do dopuszczalnego poziomu przez zastosowanie kodeksu postępowania, należy określić dodatkowe środki bezpieczeństwa za pomocą jednej z dwóch pozostałych zasad akceptacji ryzyka.*

[G 1] Uznano, że dodatkowe wyjaśnienia nie są konieczne.

European Railway Agency ● Marc LEFRANCQ, 120 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

2.3.8. Jeżeli wszystkie zagrożenia są kontrolowane za pomocą kodeksów postępowania, proces zarządzania ryzykiem można ograniczyć do:

(a) identyfikacji zagrożeń zgodnie z sekcją 2.2.6;
(b) odnotowania faktu stosowania kodeksu postępowania w rejestrze zagrożeń zgodnie z sekcją 2.3.5;
(c) udokumentowania stosowania procesu zarządzania ryzykiem zgodnie z sekcją 5;
(d) niezależnej oceny zgodnie z art. 6.

[G 1] Uznano, że dodatkowe wyjaśnienia nie są konieczne.

2.4. Korzystanie z systemu odniesienia przy wycenie ryzyka

2.4.1. Wnioskodawca bada, z pomocą innych zaangażowanych podmiotów, czy zagrożenie lub zagrożenia są uwzględnione w podobnym systemie, który można wykorzystać jako system odniesienia.

[G 1] Więcej informacji na temat tych zasad można znaleźć w części § 8 wytycznych do normy EN 50 126-2 {Ref. 9}

2.4.2. System odniesienia spełnia przynajmniej następujące wymagania:

(a) sprawdził się już w praktyce jako system o dopuszczalnym poziomie bezpieczeństwa i również obecnie spełniłby warunki wymagane do jego zatwierdzenia w państwie członkowskim, w którym ma być wprowadzona zmiana;
(b) ma podobne funkcje i interfejsy jak oceniany system;
(c) jest eksploatowany w podobnych warunkach eksploatacji jak oceniany system;
(d) jest eksploatowany w podobnych warunkach środowiskowych jak oceniany system.

[G 1] Na przykład stary system sterowania ruchem kolejowym, posiadający dopuszczalny poziom bezpieczeństwa, co udowodniono w trakcie eksploatacji, mógłby być zastąpiony przez inny system, oparty na bardziej nowoczesnej technologii i dający lepsze wyniki pod względem bezpieczeństwa. Ważne jest zatem, aby przy każdym zastosowaniu systemu odniesienia sprawdzić, czy nadal kwalifikuje się on jako dopuszczalny.

[G 2] Na przykład w związku z tym, że niektóre aspekty bezpieczeństwa w tunelach lub bezpieczeństwa transportu niebezpiecznych towarów mogą mieć szczególny charakter i mogą być uzależnione od warunków eksploatacyjnych i środowiskowych, w przypadku każdego projektu należy sprawdzić, czy system będzie stosowany w takich samych warunkach.

European Railway Agency ● Marc LEFRANCQ, 120 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

2.4.3. Jeżeli system odniesienia spełnia wymogi wymienione w pkt 2.4.2, oznacza to, że w przypadku ocenianego systemu:

(a) ryzyko związane z zagrożeniami uwzględnionymi w systemie odniesienia uważa się za dopuszczalne;
(b) wymogi bezpieczeństwa dotyczące zagrożeń uwzględnionych w systemie odniesienia można wywieść z analiz dotyczących bezpieczeństwa lub z oceny zapisów dotyczących bezpieczeństwa systemu odniesienia;
(c) określone w ten sposób wymogi bezpieczeństwa odnotowuje się w rejestrze zagrożeń jako wymogi bezpieczeństwa dotyczące odpowiednich zagrożeń.

[G 1] Uznano, że dodatkowe wyjaśnienia nie są konieczne.

2.4.4. 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. W takim przypadku ryzyko związane z zagrożeniami uwzględnionymi w systemie odniesienia uważa się za dopuszczalne.

[G 1] Więcej informacji na temat analiz podobieństw można znaleźć w części § 8.1.3 wytycznych do normy EN 50 126-2 {Ref. 9}.

2.4.5. Jeżeli niemożliwie jest wykazanie takiego samego poziomu bezpieczeństwa jak w przypadku systemu odniesienia, należy określić, za pomocą jednej z dwóch pozostałych zasad akceptacji ryzyka, dodatkowe środki bezpieczeństwa w odniesieniu do różnic między systemami.

[G 1] Uznano, że dodatkowe wyjaśnienia nie są konieczne.

2.5. Szacowanie i wycena jawnego ryzyka

2.5.1. W przypadku gdy zagrożenia nie są objęte jedną z dwóch zasad akceptacji ryzyka opisanych w sekcjach 2.3 i 2.4, dopuszczalność ryzyka jest udowadniana za pomocą szacowania i wyceny jawnego ryzyka. Ryzyka wynikające z tych zagrożeń powinny być szacowane jakościowo lub ilościowo, z uwzględnieniem istniejących środków bezpieczeństwa.

[G 1] Uznano, że dodatkowe wyjaśnienia nie są konieczne.

European Railway Agency ● Marc LEFRANCQ, 120 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

2.5.2. Dopuszczalność szacowanego ryzyka jest badana za pomocą kryteriów akceptacji ryzyka, które są wywodzone z wymogów prawnych określonych w prawodawstwie wspólnotowym lub w zgłoszonych przepisach krajowych albo bazują na tych wymogach. W zależności od kryteriów akceptacji ryzyka dopuszczalność ryzyka może być badana pojedynczo, w odniesieniu do każdego powiązanego zagrożenia, lub zbiorczo, w odniesieniu do kombi-nacji wszystkich zagrożeń rozważanych w wycenie jawnego ryzyka.

Jeżeli szacowane ryzyko nie jest dopuszczalne, należy określić i wdrożyć dodatkowe środki bezpieczeństwa, aby zredukować ryzyko do dopuszczalnego poziomu.

[G 1] W celu stwierdzenia, czy ryzyko związane z systemem objętym oceną jest dopuszczalne, konieczne są kryteria akceptacji ryzyka (zob. pola „wycena ryzyka" na Schemat 1). Kryteria te mogą być domniemane lub jawne:

(a) domniemane kryteria akceptacji ryzyka: zgodnie z treścią części 2.3.5 i 2.4.3, rodzaje ryzyka objęte zakresem stosowania kodeksów postępowania oraz porównania z systemami odniesienia uznaje się w domniemaniu za dopuszczalne pod warunkiem (zob. okrąg zaznaczony linią kropkowaną na Schemat 1):

(1) spełnienia warunków stosowania kodeksów postępowania określonych w części 2.3.2;
(2) spełnienia warunków stosowania systemu odniesienia, o którym mowa w części 2.4.2;

(b) jawne kryteria akceptacji ryzyka: aby ocenić, czy dany rodzaj ryzyka nadzorowany w drodze szacowania jawnego ryzyka jest dopuszczalny, konieczne są jednoznaczne kryteria akceptacji ryzyka (zob. okrąg zaznaczony linią ciągłą na Schemat 1 w przypadku zasady trzeciej). Kryteria te mogą zostać zdefiniowane na różnych poziomach systemu kolejowego. Można przedstawić je w postaci „piramidy kryteriów" (zob. Schemat 9), zaczynając od kryteriów akceptacji wysokiego ryzyka (wyrażonych na przykład jako ryzyko społeczne lub indywidualne), przechodząc w dół do podsystemów i elementów (obejmujących systemy techniczne), z uwzględnieniem operatorów wykonujących działania z zakresu eksploatacji i utrzymania ruchu systemu i podsystemów. Mimo że kryteria akceptacji ryzyka przyczyniają się do zapewnienia bezpieczeństwa działania systemu, a zatem są powiązane z CST i NRV, bardzo trudno jest stworzyć łączący je model matematyczny: aby uzyskać więcej informacji na ten temat zob. {Ref. 12}
Poziom, na którym definiowane są jawne kryteria akceptacji ryzyka, musi być dostosowany do znaczenia i złożoności znaczącej zmiany. Przykładowo, ocena ogólnego ryzyka systemu kolejowego nie jest konieczna w przypadku zmiany rodzaju osi taboru kolejowego. Definicja kryteriów akceptacji ryzyka może koncentrować się na bezpieczeństwie taboru kolejowego. Z kolei ocena poważnych zmian lub uzupełnień w istniejącym systemie kolejowym nie powinna opierać się wyłącznie na wynikach w zakresie bezpieczeństwa poszczególnych funkcji lub zmian, które są wprowadzane. Na poziomie systemu kolejowego należy również sprawdzić, czy dana zmiana jest dopuszczalna jako całość.

European Railway Agency ● Marc LEFRANCQ, 120 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

Schemat 9: Piramida kryteriów akceptacji ryzyka (ang. risk acceptance criteria - RAC).

[G 2] Jawne kryteria akceptacji ryzyka, niezbędne dla potrzeb wzajemnego uznawania, zostaną zharmonizowane między państwami członkowskimi w ramach trwających prac Agencji nad kryteriami akceptacji ryzyka. Jeśli udostępnione zostaną dodatkowe informacje, zostaną one włączone do niniejszego dokumentu.

[G 3] Tymczasem ryzyko może być oceniane z zastosowaniem, na przykład, matrycy ryzyka, o której mowa w części § 4.6 normy EN 50 126-1 {Ref. 8}. Można stosować również inne odpowiednie kryteria, o ile uznane zostanie, że w danym przypadku zapewniają one dopuszczalny poziom bezpieczeństwa.

2.5.3. Jeżeli ryzyko związane z zagrożeniem lub kombinacją kilku zagrożeń jest uważane za dopuszczalne, zidentyfikowane środki bezpieczeństwa zostają odnotowane w rejestrze zagrożeń.

[G 1] Uznano, że dodatkowe wyjaśnienia nie są konieczne.

2.5.4. Jeżeli zagrożenia wynikają z awarii systemów technicznych, które nie są objęte kodeksami postępowania ani nie można wykorzystać w ich przypadku systemu odniesienia, wówczas w odniesieniu do projektu systemu technicznego ma zastosowanie poniższe kryterium akceptacji ryzyka:

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.

[G 1] Dodatkowe informacje na temat RAC-TS, a także informacje na temat aspektów i funkcji systemu technicznego, do których odnosi się to kryterium, można znaleźć w dołączonej do niniejszego dokumentu nocie Agencji: zob. załącznik A część A.3. oraz dokument referencyjny {Ref. 11}.

European Railway Agency ● Marc LEFRANCQ, 120 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

2.5.5.	*Bez uszczerbku dla procedury określonej w art. 8 dyrektywy 2004/49/WE w krajowych przepisach można przewidzieć bardziej rygorystyczne kryterium w celu utrzymania poziomu krajowego bezpieczeństwa. W przypadku dodatkowych zezwoleń na dopuszczenie do eksploatacji pojazdów mają jednak zastosowanie procedury określone w art. 23 i 25 dyrektywy 2008/57/WE.*

[G 1] Uznano, że dodatkowe wyjaśnienia nie są konieczne.

2.5.6.	*W przypadku systemu technicznego, który został opracowany przy użyciu określonego w pkt 2.5.4 kryterium 10^{-9} , stosuje się zasadę wzajemnej akceptacji zgodnie z art. 7 ust. 4 niniejszego rozporządzenia.* *Jeżeli jednak wnioskodawca jest w stanie wykazać, że utrzymanie poziomu krajowego bezpieczeństwa w państwie członkowskim, w którym został złożony wniosek, jest możliwe również w przypadku współczynnika awarii wyższego niż 10^{-9} , może on wówczas stosować takie kryterium.*

[G 1] Uznano, że dodatkowe wyjaśnienia nie są konieczne.

2.5.7.	*Szacowanie i wycena jawnego ryzyka spełniają co najmniej następujące wymogi:* *(a) metody stosowane do celów szacowania jawnego ryzyka są prawidłowo dobrane do ocenianego systemu i jego parametrów (w tym wszystkich trybów pracy);* *(b) wyniki są dostatecznie dokładne, aby mogły służyć jako wiarygodne uzasadnienie decyzji, tzn. niewielkie zmiany w założeniach wejściowych lub warunkach wstępnych nie powodują znacząco odmiennych wyników dotyczących wymogów.*

[G 1] Uznano, że dodatkowe wyjaśnienia nie są konieczne.

European Railway Agency ● Marc LEFRANCQ, 120 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

3. WYKAZANIE ZGODNOŚCI Z WYMOGAMI BEZPIECZEŃSTWA

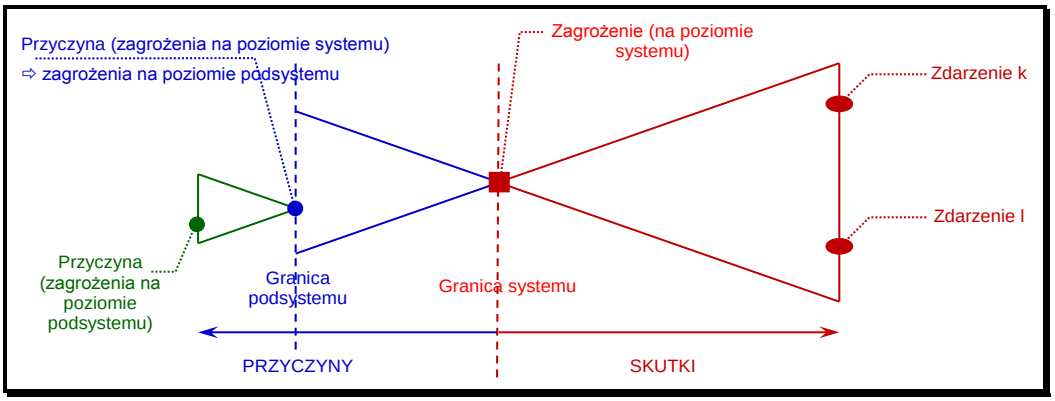
3.1. Przed odbiorem zmiany w zakresie bezpieczeństwa należy wykazać pod nadzorem wnioskodawcy, że spełnia ona wymogi bezpieczeństwa określone na etapie oceny ryzyka.

[G 1] Jak wyjaśniono w pkt. od [G 3] do [G 6] w części 2.1.1, „wykazanie zgodności systemu z wymogami bezpieczeństwa" obejmuje fazy „od 6 do 10" modelu V wg CENELEC (zob. pole 3 na Schemat 5). Zob. pkt [G 3] w części 2.1.1.

[G 2] Zob. też pkt [G 4] w części 2.1.1 niniejszego dokumentu.

3.2. Do wykazania zgodności zobowiązany jest każdy podmiot odpowiedzialny za spełnienie wymogów bezpieczeństwa, stosownie do pkt 1.1.5.

[G 1] Przykładem ocen i analiz bezpieczeństwa, które mogą być prowadzone na poziomie podsystemu, są analizy przyczynowości: zob. Schemat 10. Aby wykazać zgodność podsystemu z wymogami bezpieczeństwa dotyczącymi danych wejściowych można jednak zastosować każdą inną metodę.

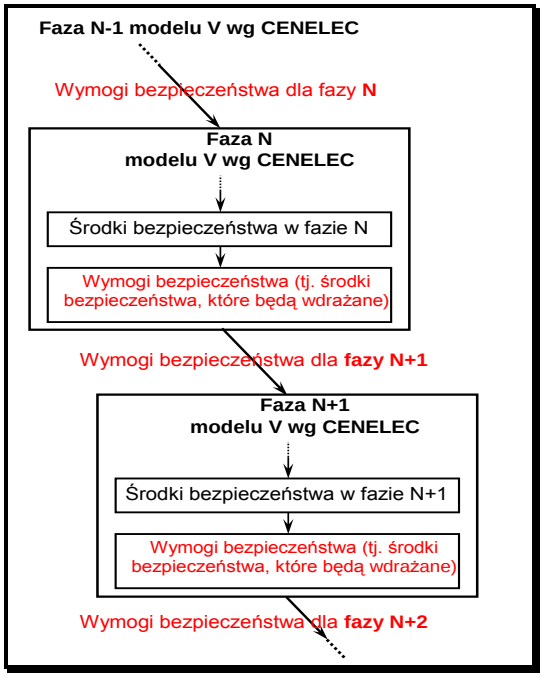


Schemat 10: Schemat A.4 normy EN 50 129: Definicja zagrożeń w kontekście granic systemu.

[G 2] Tworzenie hierarchicznej struktury zagrożeń i przyczyn w odniesieniu do systemów i podsystemów można powtarzać w przypadku wszystkich faz niższego poziomu w modelu V wg CENELEC, przedstawionego na Schemat 5. Działania z zakresu identyfikacji zagrożeń oraz analizy przyczynowości (lub dowolnej odpowiedniej metody), a także stosowania norm czynnościowych, podobnych systemów odniesienia oraz jawnych analiz i wycen mogą być powtarzane również w odniesieniu do wszystkich faz cyklu rozwoju systemu, aby otrzymać, w oparciu o środki bezpieczeństwa zidentyfikowane na poziomie podsystemu, wymogi bezpieczeństwa, które należy spełnić w kolejnej fazie. Proces ten pokazano na Schemat 11.

[G 3] Zob. też pkt [G 4] w części 2.1.1 niniejszego dokumentu.

European Railway Agency ● Marc LEFRANCQ, 120 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu



Schemat 11: Określenie wymogów bezpieczeństwa dla faz niższego poziomu.

3.3. Jednostka oceniająca dokonuje niezależnej oceny podejścia przyjętego do celów wykazania zgodności z wymogami bezpieczeństwa oraz samego wykazania.

[G 1] Niezależnej ocenie podlegają zatem również wszystkie działania przedstawione w POLU 3[(14)] modelu V wg CENELEC na Schemat 5.

[G 2] Rodzaj oraz poziom szczegółowości niezależnej oceny prowadzonej przez organy oceniające (tj. oceny szczegółowej lub makroskopowej) omówiono w ramach wyjaśnień zawartych w Artykuł 6.

3.4. Gdy środki bezpieczeństwa, dzięki którym powinny zostać spełnione wymogi bezpieczeństwa, okażą się nieodpowiednie lub gdy podczas wykazywania zgodności z wymogami bezpieczeństwa odkryte zostaną nowe zagrożenia, wnioskodawca dokonuje ponownej oceny i wyceny powiązanego ryzyka zgodnie z sekcją 2. Nowe zagrożenia są umieszczane w rejestrze zagrożeń zgodnie z sekcją 4.

[G 1] Przykładowo, sposób gaszenia pożaru może powodować pojawienie się nowego zagrożenia (uduszenie), które narzuci nowe wymogi bezpieczeństwa (np. specjalną procedurę ewakuacji pasażerów). Innym przykładem jest stosowanie hartowanego szkła, aby zapobiec rozbiciu okien podczas wypadków oraz zranieniu pasażerów odłamkami szkła, czy wręcz ich wypadnięciu z pociągu. Nowe zagrożenie polega na tym, że ewakuacja z wagonów przez

(14) *Podobieństwo działań między CSM a Schemat 5 (tj. schemat 10 metody V dla normy CENELEC 50 126) zostało opisane w części 2.1.1. W części 2.1.1 pkt [G 3] wymieniono działania CENELEC, które zostały uwzględnione w fazie CSM „wykazanie zgodności systemu z wymogami bezpieczeństwa".*

European Railway Agency ● Marc LEFRANCQ, 120 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

okna w sytuacji awaryjnej jest o wiele trudniejsza, co może wymagać wprowadzenia wymogu bezpieczeństwa, aby niektóre okna były skonstruowane w specjalny sposób umożliwiający ewakuację.

[G 2] Przykład zmiany eksploatacyjnej: konieczne jest wprowadzenie zakazu przemieszczania się wszystkich transportów towarów niebezpiecznych przez gęsto zaludnione obszary. W zamian transport ten powinien odbywać się alternatywną trasą z tunelami, co powoduje pojawienie się różnego rodzaju zagrożeń.

[G 3] Inne przykłady nowych zagrożeń, które mogą zostać rozpoznane podczas wykazywania zgodności systemu z wymogami bezpieczeństwa, przedstawiono w załączniku A.4.3 do normy EN 50 129.

European Railway Agency ● Marc LEFRANCQ, 120 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

4. ZARZĄDZANIE ZAGROŻENIAMI

4.1. Proces zarządzania zagrożeniami

4.1.1. Podczas etapu planowania i wdrażania oraz przed odbiorem zmiany albo przedłożeniem raportu w sprawie oceny bezpieczeństwa wnioskodawca tworzy rejestr lub rejestry zagrożeń, a jeżeli taki rejestr lub rejestry już istnieją, aktualizuje je. W rejestrze zagrożeń rejestrowane są postępy w monitorowaniu ryzyka związanego ze zidentyfikowanymi zagrożeniami. Zgodnie z pkt 2 lit. g) załącznika III do dyrektywy 2004/49/WE po odbiorze systemu i rozpoczęciu jego eksploatacji rejestr zagrożeń jest dalej prowadzony przez zarządcę infrastruktury lub przedsiębiorstwo kolejowe odpowiedzialne za eksploatację ocenianego systemu, jako integralny element systemu zarządzania bezpieczeństwem tego zarządcy lub przedsiębiorstwa..

[G 1] Stosowanie rejestru zagrożeń dla potrzeb rejestracji i kontroli informacji mających znaczenie dla bezpieczeństwa, a także zarządzania tymi informacjami, zalecają również normy CENELEC 50 126-1 {Ref. 8} i 50 129 {Ref. 7}.

[G 2] Przykładowo, jeden podmiot może posiadać jeden rejestr zagrożeń lub większą ich liczbę, w zależności od stopnia złożoności systemu. W obu przypadkach rejestry zagrożeń poddawane są niezależnej ocenie organów oceniających. Jednym z możliwych rozwiązań może być na przykład posiadanie:

(a) jednego „wewnętrznego rejestru zagrożeń" dla potrzeb zarządzania wszystkimi wewnętrznymi wymogami bezpieczeństwa mającymi zastosowanie do podsystemu, za który odpowiedzialny jest dany podmiot. Jego wielkość oraz nakład pracy z zakresu zarządzania zależą od jego struktury oraz, oczywiście, od złożoności podsystemu. Rejestr ten, w związku z tym, że jest wykorzystywany dla potrzeb wewnętrznego zarządzania, nie musi jednak być przekazywany innym podmiotom. Wewnętrzny rejestr zagrożeń zawiera wszystkie rozpoznane zagrożenia znajdujące się pod nadzorem oraz powiązane z nimi zalegalizowane środki bezpieczeństwa;
(b) jednego „zewnętrznego rejestru zagrożeń" w celu przenoszenia zagrożeń oraz powiązanych z nimi środków bezpieczeństwa (których podmiot nie jest w stanie wdrożyć w pełni w samodzielny sposób) na inne podmioty zgodnie z częścią 1.2.2. Zwykle ten drugi rodzaj rejestru zagrożeń jest krótszy i wymaga mniejszego nakładu pracy z zakresu zarządzania (zob. przykład w części C.16.4. załącznika C).

[G 3] Jeśli zarządzanie kilkoma rejestrami zagrożeń wydaje się skomplikowane, innym możliwym rozwiązaniem jest zarządzanie wszystkimi zagrożeniami wraz z powiązanymi z nimi środkami bezpieczeństwa, o których mowa w lit. a) i b) powyżej, w ramach jednego rejestru zagrożeń, zapewniając jednak możliwość przedstawiania dwóch sprawozdań dotyczących rejestru zagrożeń (zob. przykład w części C.16.3. załącznika C):

(a) jedno sprawozdanie dotyczące wewnętrznego rejestru zagrożeń, które nie musiałoby być konieczne, jeśli rejestr posiada odpowiednio usystematyzowaną strukturę umożliwiającą prowadzenie niezależnej oceny;
(b) jedno sprawozdanie dotyczące zewnętrznego rejestru zagrożeń dla potrzeb przenoszenia zagrożeń i powiązanych z nimi środków bezpieczeństwa na inne podmioty.

[G 4] Jak wyjaśniono w części 4.2., na zakończenie inwestycji, w momencie odbioru systemu:

(a) wszystkie zagrożenia przenoszone na inne podmioty są kontrolowane w ramach zewnętrznego rejestru zagrożeń podmiotu, który je przenosi. Ponieważ są one importowane do wewnętrznych rejestrów zagrożeń innych podmiotów i tam odbywa się

European Railway Agency ● Marc LEFRANCQ, 120 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

zarządzanie nimi, nie muszą być dalej zarządzane przez zainteresowany podmiot podczas cyklu życia (pod)systemu;

(b) wszystkie powiązane środki bezpieczeństwa nie powinny jednak zostać zalegalizowane w rejestrze zagrożeń ze względów, o których mowa w pkt [G 9] w części 4.2. W rzeczywistości warto, aby organizacja eksportująca ograniczenia dotyczące stosowania wyraźnie zaznaczyła w swoim rejestrze zagrożeń, że powiązane środki bezpieczeństwa nie zostały zalegalizowane.

[G 5] Z kolei wszystkie wewnętrzne rejestry zagrożeń są prowadzone przez cały cykl życia (pod) systemu. Umożliwia to śledzenie postępów w monitorowaniu ryzyka związanego z rozpoznanymi zagrożeniami podczas eksploatacji i utrzymania ruchu (pod)systemu, tj. po jego zamówieniu: zob. POLE 4 modelu V wg CENELEC na Schemat 5.

4.1.2. Rejestr zagrożeń obejmuje wszystkie zagrożenia oraz wszystkie związane z nimi środki bezpieczeństwa i założenia dotyczące systemu, które zostały określone podczas procesu oceny ryzyka. Rejestr ten powinien w szczególności wskazywać wyraźnie źródło zagrożenia i wybrane zasady akceptacji ryzyka oraz podmiot lub podmioty odpowiedzialne za nadzór nad każdym zagrożeniem.

[G 1] Informacje na temat zagrożeń i powiązanych z nimi środków bezpieczeństwa otrzymywane od innych podmiotów (zob. część 1.2.2.) obejmują również wszystkie założenia[15] i ograniczenia dotyczące stosowania[(15)] (zwane również warunkami stosowania związanymi z bezpieczeństwem), mające w stosownych przypadkach zastosowanie do różnych podsystemów przypadki ogólnego zastosowania i ogólnego bezpieczeństwa produktów wytwarzanych przez producentów.

[G 2] Możliwy przykład struktury wykazu zagrożeń został opisany w części C.16. załącznika C.

4.2. Wymiana informacji

Wszystkie zagrożenia i związane z nimi wymogi bezpieczeństwa, których nie jest w stanie samodzielnie nadzorować jeden podmiot, są zgłaszane innemu właściwemu podmiotowi w celu wspólnego opracowania odpowiedniego rozwiązania. Zagrożenia figurujące w rejestrze zagrożeń prowadzonym przez podmiot, który dokonuje przeniesienia zagrożeń, są „nadzorowane" tylko wówczas, gdy wycena ryzyka związanego z tymi zagrożeniami została dokonana przez inny podmiot, a rozwiązanie zostało uzgodnione przez wszystkie zainteresowane strony.

[G 1] Przykładowo, w przypadku podsystemu odometrycznego urządzeń pokładowych ETCS, producent może zalegalizować algorytmy w laboratorium poprzez symulację sygnałów teoretycznych, które mogą być generowane przez wbudowane czujniki odometryczne. Pełna legalizacja podsystemu odometrycznego wymaga jednak pomocy przedsiębiorstwa kolejowego lub zarządcy infrastruktury w celu przeprowadzenia legalizacji z wykorzystaniem prawdziwego pociągu oraz prawdziwych kół pociągu, aby uzyskać rzeczywisty kontakt koło-szyna.

---

(15) Bardziej szczegółowe informacje dot. terminu "produkt ogólny i zastosowanie ogólne", "przypadki bezpieczeństwa i "założenia i ograniczenia stosowania" - zob. pkt. [G 5] w części ***Error! Reference source not found.*** *i przypisy [9] and [10] na stronie 31 niniejszego dokumentu.*

European Railway Agency ● Marc LEFRANCQ, 120 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

[G 2] Wśród innych przykładów wymienić można przenoszenie przez producentów na przedsiębiorstwa kolejowe środków bezpieczeństwa związanych z eksploatacją i utrzymaniem ruchu urządzeń technicznych. Środki te będą musiały zostać wdrożone przez przedsiębiorstwo kolejowe.

[G 3] Aby zainteresowane organizacje mogły wspólnie ocenić te zagrożenia, powiązane z nimi środki bezpieczeństwa oraz ryzyko, warto, aby dana organizacja, po ich zidentyfikowaniu, przedstawiła wszystkie wyjaśnienia niezbędne do pełnego zrozumienia problemu. Może zdarzyć się, że pierwotny opis zagrożeń, środków bezpieczeństwa i ryzyka będzie wymagał zmiany, aby stały się one zrozumiałe bez konieczności ponownego wspólnego omawiania. Przeprowadzona wspólnie ponowna ocena zagrożeń może prowadzić do zidentyfikowania nowych środków bezpieczeństwa.

[G 4] Podmiot odbierający, odpowiedzialny za wdrożenie, weryfikację i zatwierdzenie odebranych lub nowych środków bezpieczeństwa, rejestruje w swoim rejestrze zagrożeń wszystkie zagrożenia wraz z powiązanymi z nimi środkami bezpieczeństwa (zarówno te przejęte, jak i wspólnie zidentyfikowane).

[G 5] Jeśli środek bezpieczeństwa nie został w pełni zatwierdzony, należy opracować i umieścić w rejestrze zagrożeń jednoznaczne ograniczenie stosowania (np. operacyjne środki łagodzące). W rzeczywistości istnieje możliwość, że środki bezpieczeństwa dotyczące rozwiązań technicznych/projektowych:

(a) nie zostaną poprawnie wdrożone, lub;
(b) nie zostaną w pełni wdrożone, lub;
(c) celowo nie zostaną wdrożone, na przykład z powodu wdrożenia innych środków bezpieczeństwa niż te umieszczone w wykazie zagrożeń (np. ze względu na koszt). W związku z tym, że środki te nie zostały zalegalizowane, muszą zostać wyraźnie oznaczone w wykazie zagrożeń. Należy również przedstawić dowody/uzasadnienie wyjaśniające, dlaczego wdrożone w zamian środki zastępcze są odpowiednie[(16)], a także wykazać, że po zastąpieniu środków bezpieczeństwa system nadal spełnia wymogi bezpieczeństwa;
(d) itp.

W takich przypadkach powiązane środki bezpieczeństwa dotyczące rozwiązań technicznych/projektowych nie mogą być sprawdzane ani zalegalizowane w ramach procesu zarządzania zagrożeniami. Powiązane zagrożenia i środki bezpieczeństwa muszą pozostać otwarte w wykazie zagrożeń, aby zapobiec nieprawidłowemu wykorzystaniu środków bezpieczeństwa w odniesieniu do innych systemów poprzez zastosowanie zasady akceptacji ryzyka mówiącej o „podobnym systemie odniesienia".

[G 6] Zwykle środki bezpieczeństwa, które „nie zostały poprawnie wdrożone" lub „nie zostały w pełni wdrożone", są wcześnie wykrywane w cyklu życia systemu i korygowane przed jego odbiorem. Jeśli jednak zostaną wykryte zbyt późno, aby możliwe było poprawne i pełne wdrożenie technicznych środków bezpieczeństwa, organizacja odpowiedzialna za wdrażanie i zarządzanie musi zidentyfikować i umieścić w rejestrze zagrożeń jednoznaczne ograniczenie stosowania systemu objętego oceną. Restrykcje dotyczą często ograniczeń zastosowań operacyjnych systemu objętego oceną.

[G 7] Korzystne byłoby również zaznaczenie w rejestrze zagrożeń, czy powiązane środki bezpieczeństwa zostaną poprawnie wdrożone w późniejszym etapie cyklu życia systemu,

(16) *W przypadku wdrożenia innych środków bezpieczeństwa niż te, które zostały pierwotnie określone, muszą one zostać również zapisane w wykazie zagrożeń.*

European Railway Agency ● Marc LEFRANCQ, 120 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

czy system będzie nadal wykorzystywany w oparciu o zidentyfikowane ograniczenia stosowania. Warto także umieścić w rejestrze zagrożeń uzasadnienie powodu, dla którego powiązane techniczne środki bezpieczeństwa nie zostały wdrożone w sposób poprawny/pełny.

[G 8] Podmiot, który odbiera restrykcje stosowania:

(a) włącza je wszystkie do swojego wykazu zagrożeń;
(b) dopilnowuje, aby warunki stosowania systemu objętego oceną były zgodne ze wszystkimi przyjętymi ograniczeniami stosowania;
(c) sprawdza, czy system objęty oceną jest zgodny z ograniczeniami stosowania i dopilnowuje jego zatwierdzenia.

[G 9] W zależności od decyzji zainteresowanych organizacji:

(a) techniczne środki bezpieczeństwa zostaną poprawnie włączone do projektu w późniejszym etapie.
Organizacja przekazująca ograniczenia stosowania nadal śledzi poprawne wdrażanie powiązanych środków bezpieczeństwa z technicznego punktu widzenia. W rezultacie środki bezpieczeństwa nie mogą zastać zalegalizowane, a powiązane z nimi zagrożenia nie mogą być objęte kontrolą w rejestrze zagrożeń tej organizacji do czasu pełnego wdrożenia odpowiednich technicznych środków bezpieczeństwa. Należy tego dopilnować, nawet jeśli w tym czasie zostały wprowadzone przekazane ograniczenia stosowania.

(b) albo techniczne środki bezpieczeństwa nie zostaną uwzględnione w projekcie w późniejszym etapie. W związku z tym system, przez cały cykl życia, będzie wykorzystywany z zastosowaniem powiązanych ograniczeń stosowania. W takim przypadku można podjąć następujące działania:

(1) organizacja przekazująca ograniczenia stosowania nie umieszcza powiązanych środków bezpieczeństwa w rejestrze zagrożeń jako „zalegalizowanych”. Dzięki temu, w przypadku wykorzystania powiązanego systemu w innych inwestycjach, odpowiednie zagadnienia związane z bezpieczeństwem nie zostaną pominięte. A zatem, nawet jeśli inny podmiot zgodzi się na inny sposób zarządzania powiązanym ryzykiem, warto, aby organizacja przekazująca ograniczenia stosowania wyraźnie zaznaczyła w swoim rejestrze zagrożeń, że powiązane środki bezpieczeństwa nie zostały zalegalizowane, lub

(2) opis systemu może zostać zmieniony, by uwzględnić ograniczenia w zakresie zastosowania systemu (tj., w założeniach dla systemu) oraz w wymogach bezpieczeństwa. Umożliwi to nadzór zagrożeń. W związku z tym, w przypadku stosowania systemu jako systemu odniesienia w innym zastosowaniu:

(i) nowy system będzie musiał być wykorzystywany na takich samych warunkach (tj. z zachowaniem ograniczeń stosowania powiązanych z tymi założeniami), lub;
(ii) wnioskodawca powinien przeprowadzić dodatkową ocenę ryzyka dotyczącą odstępstw od tych założeń.

European Railway Agency ● Marc LEFRANCQ, 120 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

5. DOWODY WYNIKAJĄCE Z ZASTOSOWANIA PROCESU ZARZĄDZANIA RYZYKIEM

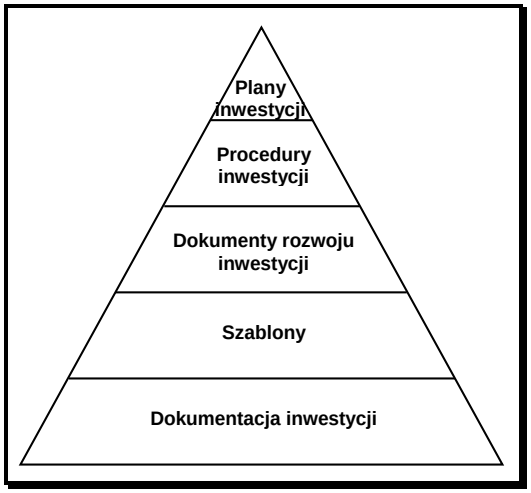
5.1. Proces zarządzania ryzykiem stosowany do celów oceny poziomów bezpieczeństwa i zgodności z wymogami bezpieczeństwa jest dokumentowany przez wnioskodawcę w taki sposób, że wszystkie niezbędne dowody świadczące o prawidłowym stosowaniu procesu zarządzania ryzykiem są dostępne dla jednostki oceniającej. Jednostka oceniająca przedstawia swoje wnioski w raporcie w sprawie oceny bezpieczeństwa.

[G 1] System zarządzania bezpieczeństwem zarządcy infrastruktury i przedsiębiorstwa kolejowego spełnia już te wymogi. W przypadku innych podmiotów sektora kolejowego, które są zaangażowane w znaczącą zmianę, nawet jeśli zasadniczo system zarządzania bezpieczeństwem nie jest obowiązkowy, przynajmniej na poziomie inwestycji, podmioty te dysponują procesem zarządzania jakością lub procesem zarządzania bezpieczeństwem. Oba procesy opierają się na usystematyzowanej hierarchii dokumentacji w ramach przedsiębiorstwa lub przynajmniej w ramach danej inwestycji. Spełniają one również wymogi z zakresu zarządzania dokumentacją specyfikacji niezawodności, dostępności, podatności utrzymaniowej i bezpieczeństwa (RAMS). Tego rodzaju usystematyzowana dokumentacja może obejmować zasadniczo następujące elementy (zob. też Schemat 12):

(a) **Plany inwestycji** opracowane dla potrzeb opisu organizacji, którą należy zastosować w celu zarządzania działaniami w ramach inwestycji.

(b) **Procedury inwestycji** opracowane dla potrzeb szczegółowego opisu sposobu realizacji specjalistycznego zadania. Zwykle przedsiębiorstwo posiada procedury i instrukcje, w oparciu o które działa i są one wykorzystywane jako takie. Nowe procedury inwestycji opracowywane są tylko w przypadku konieczności opisania konkretnego zadania w ramach danej inwestycji.

(c) **Dokumenty dotyczące rozwoju inwestycji,** opracowywane przez cały cykl życia systemu, przedstawione na Schemat 5.



Schemat 12 : Usystematyzowana hierarchia dokumentów.

(d) Dla różnych typów dokumentów, które należy sporządzić istnieją **szablony dla przedsiębiorstwa lub co najmniej inwestycji**.

(e) **Dokumentacja inwestycji** opracowywana przez cały okres realizacji inwestycji, niezbędna do wykazania zgodności z obowiązującymi w danym przedsiębiorstwie procesami zarządzania jakością i bezpieczeństwem.

Jest to jeden ze sposobów wywiązania się z wymogu dostarczenia udokumentowanych danych. Można to zrobić również na inne sposoby, pod warunkiem zachowania zgodności z kryteriami CSM.

[G 2] Normy CENELEC zalecają wykazanie zgodności systemu z wymogami funkcjonalnymi oraz wymogami bezpieczeństwa w dowodzie bezpieczeństwa (ang. „*safety case document*") (inaczej raport w sprawie oceny bezpieczeństwa). Nawet jeśli nie ma takiego obowiązku,

European Railway Agency ● Marc LEFRANCQ, 120 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

stosowanie dowodu bezpieczeństwa stanowi, w ramach usystematyzowanego dokumentu uzasadniającego stan bezpieczeństwa:

(a) dowód zarządzania jakością;
(b) dowód zarządzania bezpieczeństwem;
(c) dowód bezpieczeństwa funkcjonalnego i technicznego;

Inną zaletą dowodu bezpieczeństwa jest to, że może zapewnić wsparcie i wytyczne dla organów oceniających w prowadzonej przez nie niezależnej ocenie prawidłowego stosowania CSM.

[G 3] Dowód bezpieczeństwa zawiera opis i streszczenie sposobu, w jaki dokumenty inwestycji, będące wynikiem realizacji procesów zarządzania jakością lub bezpieczeństwem na poziomie przedsiębiorstwa lub inwestycji, są powiązane w ramach procesu rozbudowy systemu, aby wykazać jego bezpieczeństwo. Zazwyczaj dowód bezpieczeństwa nie obejmuje wielu szczegółowych danych ani dokumentacji uzupełniającej, lecz zawiera dokładne odniesienia do takich dokumentów.

[G 4] **Dowód bezpieczeństwa dla systemów technicznych:** normy CENELEC można potraktować jako wytyczne w zakresie opracowywania lub struktury dowodu bezpieczeństwa:

(a) zob. norma EN 50 129 {Ref. 7} „Zastosowania kolejowe – Łączność, sygnalizacja i systemy sterowania – Elektroniczne systemy sygnalizacji związane z bezpieczeństwem”; strukturę dowodu bezpieczeństwa systemów sygnalizacji zaproponowano również w załączniku H.2 Wytycznych stosowania normy EN 50 126-2; {Ref. 9}
(b) zob. załącznik H.1 Wytycznych stosowania normy EN 50 126-2 {Ref. 9}, aby uzyskać informacje na temat struktury dowodu uzasadniającego bezpieczeństwa dla taboru kolejowego;
(c) zob. załącznik H.3 Wytycznych stosowania normy EN 50 126-2 {Ref. 9}, aby uzyskać informacje na temat dowodu bezpieczeństwa infrastruktury.

Jak wynika z dokumentów, do których odsyłają powyższe odniesienia, struktura *dowodu* bezpieczeństwa dla systemów technicznych, a także jego treść, zależą od systemu, którego zgodność z wymogami bezpieczeństwa należy wykazać.

Dowód bezpieczeństwa przedstawiony w załączniku H Wytycznych stosowania normy EN 50 126-2 {Ref. 9} zawiera tylko przykłady i może nie być odpowiednie dla wszystkich systemów danego rodzaju. Z tego względu konieczne jest wykorzystanie szkicu z odpowiednim uzasadnieniem rozwiązań, które pasują do poszczególnych zastosowań.

[G 5] **Dowód bezpieczeństwa dla aspektów organizacyjnych i operacyjnych systemów kolejowych:**

Obecnie nie istnieje żadna specjalna norma określająca strukturę, treść oraz wytyczne opracowywania dowodu bezpieczeństwa dla aspektów organizacyjnych i eksploatacyjnych systemu kolejowego. Ponieważ jednak celem dowodu jest wykazanie w sposób usystematyzowany zgodności systemu z jego wymogami bezpieczeństwa, można zastosować taką samą strukturę dokumentu, jak w przypadku systemów technicznych. W rzeczywistości odniesienia w pkt [G 4] części 5.1 zawierają porady oraz listę kontrolną pozycji, które należy uwzględnić niezależnie od rodzaju systemu objętego oceną. Zarządzanie zmianami organizacyjnymi i operacyjnymi wymaga zastosowania tego samego typu procesów zarządzania jakością i bezpieczeństwem, jak w przypadku zmian technicznych, przy czym należy wykazać zgodność systemu z określonymi wymogami bezpieczeństwa. Spośród norm CENELEC, aspektów organizacyjnym i eksloatacyjnych nie dotyczą normy odnoszące się do rozwiązań projektowych systemów technicznych, takich jak

European Railway Agency ● Marc LEFRANCQ, 120 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

na przykład zasady „wewnętrznego bezpieczeństwa strukturalnego sprzętu komputerowego", kompatybilność elektromagnetyczna (EMC) itp.

5.2. Dokument przedstawiony przez wnioskodawcę zgodnie z pkt 5.1 obejmuje co najmniej:

(a) opis organizacji i specjalistów wyznaczonych do przeprowadzenia procesu oceny ryzyka,

(b) wyniki poszczególnych etapów oceny ryzyka oraz wykaz wszystkich wymogów bezpieczeństwa, których dopełnienie jest konieczne, aby nadzorować ryzyko, utrzymując je na dopuszczalnym poziomie.

[G 1] W zależności od poziomu złożoności systemu dowody te można zgromadzić w ramach jednego lub kilku dowodów bezpieczeństwa. Aby uzyskać informacje na temat dowodu bezpieczeństwa dla systemów technicznych oraz aspektów operacyjnych i eksploatacyjnych, zob. odpowiednio pkt. [G 4] i [G 5] w części 5.1.

[G 2] Możliwe przykłady dowodów można znaleźć również w części A.4. załącznika A.

[G 3] Na ogół przyjmuje się, że okres użytkowania systemów i podsystemów technicznych w sektorze kolejowym wynosi około 30 lat. W tak długim okresie można również spodziewać się wielu znaczących zmian w tych systemach. W związku z tym istnieje możliwość przeprowadzenia dalszej oceny ryzyka tych systemów i interfejsów z dokumentacją towarzyszącą, która będzie musiała zostać poddana przeglądowi, uzupełniona i przekazana różnym podmiotom i organizacjom korzystającym z wykazów zagrożeń. Wymaga to raczej surowych wymogów dotyczących kontroli dokumentacji i zarządzania konfiguracjami.

[G 4] Przedsiębiorstwo archiwizujące wszystkie informacje na temat oceny ryzyka i zarządzania ryzykiem powinno zatem zagwarantować możliwość odczytania/dostępność wyników/informacji przechowywanych na nośnikach fizycznych przez cały okres użytkowania systemu (np. 30 lat).

[G 5] Główne powody wprowadzenia takiego wymogu to między innymi:

(a) zapewnienie dostępności wszystkich analiz oraz wyników w zakresie bezpieczeństwa systemu objętego oceną przez cały okres jego użytkowania. W związku z tym:

(1) w przypadku kolejnych istotnych zmian w tym samym systemie dostępna jest najnowsza dokumentacja systemu;

(2) w przypadku jakichkolwiek problemów podczas okresu użytkowania systemu warto posiadać możliwość wglądu do powiązanych analiz bezpieczeństwa oraz wyników w zakresie bezpieczeństwa;

(b) zapewnienie dostępności wszystkich analiz oraz wyników w zakresie bezpieczeństwa systemu objętego oceną, jeśli system ten jest wykorzystywany w innym zastosowaniu jako podobny system odniesienia.

European Railway Agency ● Marc LEFRANCQ, 120 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

ZAŁĄCZNIK II DO ROZPORZĄDZENIA CSM

Kryteria, które muszą spełniać jednostki oceniające

1.	*Jednostka oceniająca nie może być zaangażowana, bezpośrednio ani jako upoważniony przedstawiciel, w projektowanie, wytwarzanie, budowę, wprowadzanie do obrotu, eksploatację lub utrzymanie ocenianego systemu. Powyższe kryterium nie wyklucza możliwości wymiany informacji technicznych między tą jednostką a wszystkimi zaangażowanymi podmiotami.*
2.	*Jednostka oceniająca ma obowiązek przeprowadzić ocenę z zachowaniem najwyższego stopnia uczciwości zawodowej i kompetencji technicznych oraz nie może podlegać żadnym naciskom ani wpływom, zwłaszcza natury finansowej, które mogłyby mieć wpływ na jej osąd lub wyniki ocen, w szczególności ze strony osób lub grup osób, których dotyczą te oceny.*
3.	*Jednostka oceniająca musi posiadać środki niezbędne do rzetelnej realizacji zadań technicznych i administracyjnych związanych z ocenami. Jednostka powinna mieć także dostęp do sprzętu potrzebnego do dokonywania ocen nadzwyczajnych.*
4.	*Personel odpowiedzialny za oceny:* - *musi być odpowiednio przeszkolony technicznie i zawodowo,* - *musi posiadać wystarczającą znajomość wymogów dotyczących przeprowadzanych przez niego ocen oraz wystarczające doświadczenie praktyczne w ich przeprowadzaniu,* - *musi posiadać umiejętność sporządzania raportów w sprawie oceny bezpieczeństwa, które stanowią formalne wnioski z przeprowadzonych ocen.*
5.	*Niezbędne jest zagwarantowanie niezależności pracowników odpowiedzialnych za przeprowadzanie niezależnych ocen. Urzędnik nie może być wynagradzany w oparciu o liczbę przeprowadzonych ocen ani o ich wyniki.*
6.	*Jeżeli jednostka oceniająca nie należy do struktury organizacyjnej wnioskodawcy, jednostka ta ma obowiązek posiadać ubezpieczenie od odpowiedzialności cywilnej, chyba że zgodnie z prawem krajowym odpowiedzialność cywilna spoczywa na państwie członkowskim lub oceny są przeprowadzane bezpośrednio przez państwo członkowskie.*
7.	*Jeżeli jednostka oceniająca nie należy do struktury organizacyjnej wnioskodawcy, personel tej jednostki jest zobowiązany do przestrzegania tajemnicy zawodowej w odniesieniu do wszystkich informacji pozyskanych podczas wykonywania obowiązków (z wyjątkiem właściwych organów administracyjnych w państwie, w którym wykonuje te zadania) zgodnie z niniejszym rozporządzeniem.*

[G 1] Uznano, że dodatkowe wyjaśnienia nie są konieczne.

European Railway Agency ● Marc LEFRANCQ, 120 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

ZAŁĄCZNIK A: DODATKOWE WYJAŚNIENIA

A.1. Wstęp

A.1.1. Celem tego załącznika jest ułatwienie lektury niniejszego dokumentu. Zamiast wprowadzać duże ilości informacji do treści samego dokumentu, w niniejszym załączniku przedstawiono szczegółowe wyjaśnienia bardziej złożonych zagadnień.

A.2. Klasyfikacja zagrożeń

A.2.1. W części § 4.6.3. normy EN 50 126-1 {Ref. 8} oraz w załączniku B.2 do Wytycznych dotyczących stosowania normy EN 50 126-2 {Ref. 9} zawarto wskazówki dotyczące klasyfikacji/uszeregowania zagrożeń.

A.3. Kryterium akceptacji ryzyka w odniesieniu do systemów technicznych (RAC-TS)

A.3.1. Górna granica dopuszczalności ryzyka w odniesieniu do systemów technicznych

A.3.1.1. Kryterium RAC-TS zostało opisane w części 2.5.4. {Ref. 4}.

A.3.1.2. Celem RAC-TS jest wyznaczenie górnej granicy dopuszczalności ryzyka w odniesieniu do systemów technicznych, w przypadku których wymogi bezpieczeństwa nie mogą być określone ani poprzez zastosowanie norm czynnościowych ani w drodze porównania z podobnymi systemami odniesienia. W rezultacie wyznacza ono punkt odniesienia, na podstawie którego można przeprowadzić kalibrację metody analizy ryzyka w odniesieniu do systemów technicznych. Jak opisano w części A.3.6. załącznika A do niniejszego dokumentu, punkt ten, lub inaczej górną granicę dopuszczalności ryzyka, można również wykorzystać dla potrzeb określenia kryteriów akceptacji ryzyka w odniesieniu do innych błędów funkcjonalnych systemów technicznych, z którymi nie wiąże się wiarygodna i bezpośrednia możliwość wystąpienia katastroficznych konsekwencji (tj. innych poważnych awarii). RAC-TS nie jest jednak metodą analizy ryzyka.

A.3.1.3. RAC-TS to kryterium półilościowe. Ma ono zastosowanie zarówno do przypadkowych uszkodzeń sprzętu, jak i uszkodzeń/błędów systematycznych systemu technicznego. Zaliczają się do nich również uszkodzenia/błędy systematyczne systemu technicznego będące skutkiem błędów ludzkich podczas procesu opracowywania systemu technicznego (tj. specyfikacji, projektowania, wdrażania i legalizacji). RAC-TS nie obejmuje jednak błędów ludzkich podczas eksploatacji i utrzymania ruchu systemów technicznych.

A.3.1.4. Zgodnie z treścią załączników A.3 i A.4 do normy CENELEC 50 129, uszkodzenia/błędy systematyczne nie są wymierne, a zatem cele ilościowe należy określić tylko w odniesieniu do przypadkowych awarii sprzętu, natomiast w przypadku awarii/błędów systematycznych

European Railway Agency ● Marc LEFRANCQ, 120 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

stosowane są metody jakościowe[17]. *„Ponieważ spójność uszkodzenia systematycznego nie może zostać oceniona za pomocą metod ilościowych, stosuje się poziomy nienaruszalności bezpieczeństwa w celu grupowania metod, narzędzi oraz technik, które, jeśli stosowane w skuteczny sposób, mogą zapewnić odpowiedni poziom ufności podczas realizacji systemu z zachowaniem określonego poziomu nienaruszalności."*

A.3.1.5. Podobnie, zgodnie z wymogami norm CENELEC, nie jest również wymierna nienaruszalność oprogramowania systemów technicznych. Norma CENELEC 50 128 zawiera wytyczne dotyczące procesu opracowywania oprogramowania związanego z bezpieczeństwem w zależności od wymaganego poziomu nienaruszalności bezpieczeństwa. Dotyczy to procesów projektowania, weryfikacji, legalizacji oraz procesów zapewnienia jakości oprogramowania.
Zgodnie z wymogami normy CENELEC 50 128, w przypadku programowalnego, elektronicznego systemu kontroli wdrażającego funkcje bezpieczeństwa, najwyższy możliwy poziom nienaruszalności bezpieczeństwa dla procesu opracowywania oprogramowania wynosi SIL 4, co odpowiada ilościowemu współczynnikowi tolerowanego ryzyka na poziomie 10^{-9}/godzinę.

A.3.1.6. W związku tym, skoro uszkodzenia/błędy systematyczne nie mogą zostać poddane ocenie ilościowej, muszą być zarządzane w sposób jakościowy poprzez wprowadzenie procesu jakości i bezpieczeństwa, odpowiadającego poziomowi nienaruszalności bezpieczeństwa, jaki jest wymagany w przypadku systemu objętego oceną.

(a) proces zarządzania jakością ma na celu „*ograniczenie do minimum częstotliwości występowania błędów ludzkich na każdym etapie cyklu życia, a tym samym zmniejszenie ryzyka awarii systematycznych w systemie*",

(b) proces zarządzania bezpieczeństwem ma na celu „*dalsze ograniczenie częstotliwości występowania błędów ludzkich związanych z bezpieczeństwem na przestrzeni całego cyklu życia, a tym samym ograniczenie do minimum pozostałego ryzyka awarii systematycznych związanych z bezpieczeństwem*".

A.3.1.7. Wytyczne dotyczące zarządzania częstotliwością występowania uszkodzeń/błędów systematycznych, a także wytyczne dotyczące możliwych środków projektowych mających zabezpieczyć przed uszkodzeniami mającymi wspólną przyczynę/tryb (ang. *Common Cause/Mode Failure – CCF/CMF)* oraz zapewnić wejście systemu technicznego w stan bezpieczeństwa strukturalnego w przypadku takich awarii/błędów, zostały zawarte w:

(a) normie CENELEC 50 126-1 {Ref. 8}, natomiast w odnoszących się do niej wytycznej 50 126-2 {Ref. 9} wymienione zostały klauzule normy 50 129 oraz możliwość ich stosowania w odniesieniu do udokumentowanych danych w przypadku systemów innych niż sygnalizacja: zob. tabela 9.1 w wytycznej 50 126-2 {Ref. 9}. Wykaz ten zawiera odniesienia do wytycznych dotyczących sposobu postępowania zarówno w przypadku awarii wywoływanych przez sam system, jak i będących skutkiem oddziaływania środowiska na system objęty oceną;

---

(17) *Zgodnie z wymogami norm CENELEC 50 126, 50 128 i 50 129, dane ilościowe opisujące przypadkowe uszkodzenia sprzętu muszą być zawsze powiązane z poziomem nienaruszalności bezpieczeństwa, aby możliwe było zarządzanie uszkodzeniami/błędami systematycznymi. W związku z tym określona w CSM wartość liczbowa 10^{-9}/godzinę wymaga również wprowadzenia odpowiedniego procesu umożliwiającego prawidłowe zarządzanie również uszkodzeniami/błędami systematycznymi. Jednak w celu ułatwienia odczytania uwagi, często odnosi się ona tylko do przypadkowych uszkodzeń sprzętu w systemie technicznym.*

European Railway Agency ● Marc LEFRANCQ, 120 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

Przykładowo techniki/środki odnoszące się do cech projektowych zostały podane w *„Tabeli E.5: Cechy projektowe (o których mowa w 5.4)”* normy CENELEC 50 129 {Ref. 7}, *„w celu uniknięcia i kontroli awarii spowodowanych:*

(1) *„wszelkimi usterkami w projektowaniu”;*
(2) *„warunkami środowiskowymi”;*
(3) *„nieprawidłowym użytkowaniem lub błędami w eksploatacji”,*
(4) *„wszelkimi usterkami w oprogramowaniu”;*
(5) *„czynnikami ludzkimi”.*

W załącznikach D i E do normy CENELEC 50 129 {Ref. 7} podano techniki oraz środki pozwalające uniknąć awarii systematycznych oraz umożliwiające kontrolę przypadkowych awarii/błędów sprzętu oraz uszkodzeń/błędów systematycznych w przypadku elektronicznych systemów sygnalizacji związanych z bezpieczeństwem. Wiele z nich można zastosować również w przypadku innych systemów niż sygnalizacja, poprzez odniesienie do tych wytycznych w tabeli 9.1 wytycznej 50 126-2 {Ref. 9}.

(b) norma CENELEC 50 128 zawiera wytyczne dotyczące procesu opracowywania oprogramowania związanego z bezpieczeństwem w zależności od poziomu nienaruszalności bezpieczeństwa wymaganego od oprogramowania systemu objętego oceną (od SIL 0 do SIL 4).

A.3.1.8. RAC-TS odpowiada również najwyższemu poziomi nienaruszalności, który może być wymagany zarówno przez normy CENELEC, jak i IEC. W celu ułatwienia wyszukiwania informacji, wymogi norm IEC 61508-1 oraz CENELEC 50 129 zostały przytoczone poniżej:

(a) IEC 61508-1: „Norma ta ustala dolną granicę docelowej miary uszkodzeń, w przypadku uszkodzeń niebezpiecznych, która może być zapewniona. Zostały one określone jako dolna granica dla 4 poziomu nienaruszalności bezpieczeństwa. Istnieje możliwość zaprojektowania systemów wiążących się z bezpieczeństwem przy niższych wartościach docelowych miar uszkodzeń w przypadku systemów o niskim poziomie złożoności, uznaje się jednak, że podane w tabeli dane liczbowe stanowią granicę możliwych do uzyskania parametrów w przypadku systemów o relatywnie wysokim poziomie złożoności (na przykład systemów programowalnych elektronicznych wiążących się z bezpieczeństwem.”

(b) EN 50129: *„Do funkcji posiadającej większe wymogi ilościowe niż 10^{-9}/godzinę podchodzi się w jeden z następujących sposobów:*

(1) jeżeli istnieje możliwość podziału funkcji na funkcjonalnie niezależne podfunkcje, THR może zostać rozdzielone między te podfunkcje i do każdej z nich może zostać przypisany SIL;

(2) w przypadku braku możliwości podziału funkcji konieczne jest zapewnienie co najmniej środków i metod wymaganych w przypadku SIL 4, a funkcja wykorzystywana jest w połączeniu z innymi środkami technicznymi lub eksploatacyjnych w celu osiągnięcia niezbędnego THR.”

A.3.1.9. Wszystkie systemy techniczne powinny zatem ograniczyć ilościowy wymóg bezpieczeństwa do tej wartości liczbowej. Jeśli konieczny jest wyższy poziom ochrony, nie można go osiągnąć za pomocą tylko jednego systemu. Należy dokonać zmiany struktury systemu, na przykład stosując równolegle dwa niezależne systemy, które prowadzą względem siebie kontrolę krzyżową w celu zapewnienia bezpiecznych wyników. Z pewnością powoduje to jednak zwiększenie kosztów opracowania systemu technicznego.

Uwaga: jeśli istnieją funkcje, np. systemy czysto mechaniczne, które - opierając się na doświadczeniu eksploatacyjnym - mogły osiągnąć wyższy poziom nienaruszalności, w takim

European Railway Agency ● Marc LEFRANCQ, 120 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

przypadku poziom bezpieczeństwa może zostać opisany w specjalnych normach czynnościowych lub wymogi bezpieczeństwa mogą zostać określone w drodze analizy podobieństwa z istniejącym systemem. W ramach zakresu CSM, jeżeli nie istnieją żadne normy czynnościowe ani system odniesienia, należy zastosować tylko RAC-TS.

A.3.1.10. Można streścić to w następujący sposób:

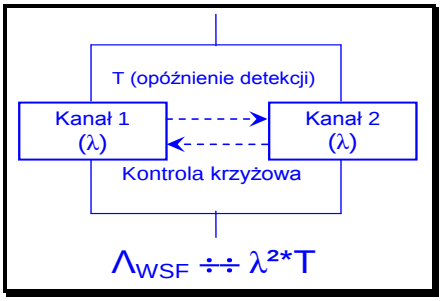
(e) zgodnie z wymogami norm CENELEC 50 126, 50 128 i 50 129, uszkodzenia/błędy systematyczne podczas opracowywania nie są wymierne;

(f) częstotliwość występowania uszkodzeń/błędów systematycznych oraz ich ryzyko szczątkowe powinny być kontrolowane i zarządzane poprzez zastosowanie odpowiednich procesów zarządzania jakością i bezpieczeństwem, które są zgodne z poziomem nienaruszalności bezpieczeństwa, jaki jest wymagany w przypadku systemu objętego oceną;

(g) najwyższy osiągalny poziom nienaruszalności bezpieczeństwa wynosi SIL 4, zarówno jeśli chodzi o przypadkowe uszkodzenia sprzętu, jak i o uszkodzenia/błędy systematyczne systemów technicznych;

(h) poziom nienaruszalności bezpieczeństwa SIL 4 oznacza, że maksymalny współczynnik tolerowanego zagrożenia (THR) (tj. maksymalny współczynnik awaryjności) w przypadku systemów technicznych musi zostać również ograniczony do 10^{-9}/godzinę.

A.3.1.11. System techniczny może osiągnąć współczynnik tolerowanego zagrożenia na poziomie 10^{-9}/godzinę albo dzięki strukturze zapewniającej bezpieczeństwo strukturalne (która z definicji osiąga takie wyniki w zakresie bezpieczeństwa) lub „strukturze rezerwowej" (np. dwóch niezależnych kanałów przetwarzania realizujących względem siebie kontrolę krzyżową).



Schemat 13: Struktura rezerwowa w przypadku systemu technicznego.

W przypadku struktury rezerwowej można wykazać, że ogólne poważne uszkodzenie (Λ_{WSF}) systemu technicznego jest proporcjonalne do λ^2*T, gdzie:

(a) λ^2 oznacza podniesioną do kwadratu wartość współczynnika krytycznego uszkodzenia jednego kanału;

(b) T oznacza czas, jaki jeden kanał potrzebuje na wykrycie poważnego uszkodzenia drugiego kanału. Zwykle jest to wielokrotność czasu/cyklu przetwarzania kanału. Zazwyczaj T przyjmuje wartość znacznie poniżej 1 sekundy.

A.3.1.12. Teoretycznie, opierając się tym wzorze (λ^2*T), można wykazać (uwzględniając tylko przypadkowe uszkodzenia urządzeń w systemie technicznym – zob. też pkt A.3.1.13. w załączniku A), że wymóg ilościowy 10^{-9}/godzinę dla RAC-TS jest możliwy do osiągnięcia. Uszkodzenia/błędy systematyczne muszą być zarządzane za pomocą procesu: zob. pkt A.3.1.6. w załączniku A. Na przykład:

(a) przy MTBF rzędu 10 000 godzin, oznaczającym niezawodność przypadającą na jeden kanał, oraz przy ostrożnym założeniu, że każde uszkodzenie kanału jest niebezpieczne, poważna awaria kanału wynosi 10^{-4}/godzinę;

European Railway Agency ● Marc LEFRANCQ, 120 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

(b) nawet jeśli czas wykrycia poważnych uszkodzeń w innym kanale wynosi 10 minut (tj. $\approx 2*10^{-3}$ godzin), co również stanowi ostrożne założenie;

Ogólne poważne uszkodzenie $\Lambda_{WSF} \approx 2 * 10^{-10}$/godzinę.

A.3.1.13. W praktyce, w przypadku tego rodzaju struktury rezerwowowej, wycena ilościowego ogólnego, poważnego uszkodzenia sprzętu musi uwzględniać środki, które zostały zastosowane w projekcie w celu zabezpieczenia przed uszkodzeniami o wspólnej przyczynie (ang. Common Causa/Mode Failure – CCF/CMF) oraz zapewnienia wejścia systemu technicznego w stan bezpieczeństwa strukturalnego w przypadku uszkodzenia mającego wspólną przyczynę. Wycena ogólnego poważnego uszkodzenia (Λ_{WSF}) musi zatem uwzględniać również:

(a) komponenty wspólne dla wszystkich kanałów, np. pojedyncze lub wspólne dane wejściowe dla wszystkich kanałów, wspólne zasilanie energią, komparatory, wybieraki itp.;
(b) czas potrzebny do wykrycia ukrytych uszkodzeń. W przypadku złożonych systemów technicznych czas te może być dłuższy o kilka rzędów wielkości od 1 sekundy;
(c) wpływ uszkodzeń o wspólnej przyczynie (CCF/CMF).

Wytyczne dotyczące tych tematów można znaleźć w normach cytowanych w pkt A.3.1.7. załącznika A do niniejszego dokumentu.

A.3.2. Schemat badania możliwości stosowania RAC-TS

A.3.2.1. Zastosowanie RAC-TS do zagrożeń wynikających z uszkodzeń systemów technicznych może zostać przedstawione w sposób pokazany na Schemat 14.

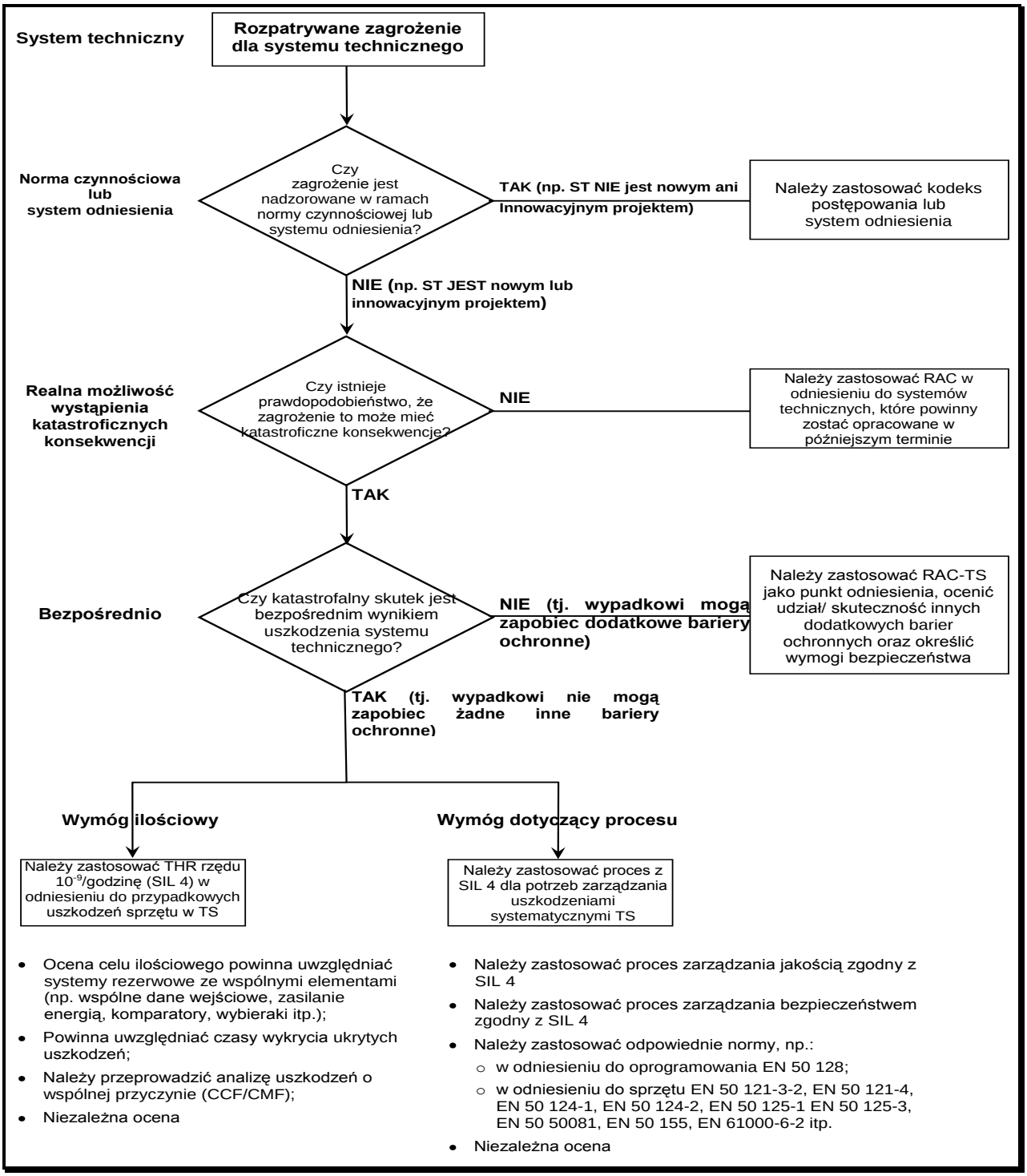
A.3.2.2. Przykładowe zastosowanie schematu badania przedstawiono w części C.15. załącznika C.

A.3.3. Definicja systemu technicznego w rozporządzeniu CSM

A.3.3.1. RAC-TS ma zastosowanie tylko do systemów technicznych. Przedstawiona poniżej definicja „systemu technicznego" została zawarta w rozporządzenia CSM.

„system techniczny" oznacza produkt lub zespół produktów, w tym projekt oraz dokumentację wykonawczą i pomocniczą; proces opracowywania systemu technicznego rozpoczyna się od opracowania specyfikacji wymogów, a kończy odbiorem tego systemu; system techniczny nie obejmuje użytkowników ani ich działań, chociaż uwzględnia się projekt odpowiednich interfejsów z zachowaniami ludzi. Proces utrzymania jest opisany w instrukcjach utrzymania, ale sam nie stanowi części systemu technicznego.

European Railway Agency ● Marc LEFRANCQ, 120 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu



Schemat 14: Schemat badania możliwości stosowania RAC-TS.

European Railway Agency ● Marc LEFRANCQ, 120 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

A.3.4. Wyjaśnienie definicji „systemu technicznego”

A.3.4.1. Przedstawiona definicja systemu technicznego opisuje jego zakres: *„system techniczny” oznacza produkt lub zespół produktów, w tym projekt oraz dokumentację wykonawczą i pomocniczą.”* W związku z tym obejmuje ona następujące elementy:

(a) elementy fizyczne tworzące system techniczny;
(b) (ewentualne) powiązane z nim oprogramowanie;
(c) projekt i wdrażanie systemu technicznego, z uwzględnieniem, w stosownych przypadkach, konfiguracji lub parametryzacji produktu ogólnego przeznaczenia w celu dostosowania go do konkretnych wymogów konkretnego zastosowania;
(d) dokumentację pomocniczą niezbędną do:

(1) opracowania systemu technicznego;
(2) obsługi i utrzymania ruchu systemu technicznego;

A.3.4.2. Uwagi do tej definicji bardziej szczegółowo określają zakres systemu technicznego:

(a) *„proces opracowywania systemu technicznego rozpoczyna się od opracowania specyfikacji wymogów, a kończy odbiorem tego systemu.”* Proces ten obejmuje fazy od 1 do 10 modelu V przedstawionego na schemacie 10 normy CENELEC 50 126-1 {Ref. 8};

(b) *„Projekt uwzględnia zachowania człowieka. System techniczny nie obejmuje jednak użytkowników ani ich działań.*” Mimo że błędy spowodowane czynnikiem ludzkim, występujące podczas obsługi i utrzymania ruchu systemu technicznego, nie stanowią jego elementu, projekt musi uwzględniać zachowania człowieka. Ma to na celu ograniczenie do minimum prawdopodobieństwa błędów ludzkich wynikających z nieodpowiedniego uwzględnienia zachowania operatorów maszyn;

(c) *„Proces utrzymania jest opisany w instrukcjach utrzymania, ale sam nie stanowi części systemu technicznego.”* Oznacza to brak konieczności stosowania RAC-TS w odniesieniu do obsługi i utrzymania ruchu systemu technicznego; działania te opierają się głównie na procesach i czynnościach personelu. Aby wesprzeć utrzymanie ruchu systemów technicznych, definicja systemu technicznego musi uwzględniać wszelkie istotne wymogi (np. okresowe prewencyjne lub korekcyjne utrzymanie ruchu w przypadku uszkodzeń) z zapewnieniem wystarczającego poziomu szczegółowości. Wymagany sposób organizacji i osiągnięcia utrzymania ruchu w odniesieniu do powiązanego z nim systemu technicznego nie jest jednak objęty definicją systemu technicznego, lecz został opisany w odpowiednich instrukcjach.

A.3.4.3. Zob. też część A.3.1. załącznika A.

A.3.5. Funkcje systemów technicznych, w przypadku których stosuje się RAC-TS.

A.3.5.1. Zgodnie z definicją RAC-TS, ma ono zastosowanie do poważnych uszkodzeń funkcji, które powinien spełniać system techniczny, jeżeli „*istnieje realna, **bezpośrednia** możliwość, że będą miały one katastroficzne konsekwencje*”. zob. część 2.5.4. w {Ref. 4}.

A.3.5.2. RAC-TS może być stosowane również w odniesieniu do funkcji angażujących systemy techniczne, ale których uszkodzenie **nie wiąże się z „*bezpośrednią* możliwością** *katastroficznych konsekwencji* ". W takim przypadku RAC-TS musi zostać zastosowany jako ogólny cel dla katastrofalnej w skutkach serii zdarzeń. Na podstawie tego ogólnego celu należy określić rzeczywisty udział każdego zdarzenia, a zatem błędów funkcjonalnych

European Railway Agency ● Marc LEFRANCQ, 120 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

systemu technicznego występującego w analizowanym scenariuszu zgodnie z częścią A.3.6. załącznika A.
Takie wykorzystanie RAC-TS wymaga dalszej dyskusji i uzgodnienia w ramach grupy roboczej ds. CSM.

A.3.5.3. W odniesieniu to jakich funkcji systemu technicznego stosuje się RAC-TS? Zgodnie z normą IEC 61226:2005:

(a) w tym kontekście funkcja definiowana jest jako *„konkretne założenia lub cele do realizacji, które mogą zostać określone lub opisane bez odniesienia do środków fizycznych umożliwiających ich osiągnięcie”;*

(b) funkcja (traktowana jako czarna skrzynka) przenosi parametry wejściowe (np. materiał, energia, informacje) na parametry wyjściowe powiązane z celami (np. materiał, energia, informacje);

(c) analiza funkcji jest niezależna od jej realizacji technicznej.

A.3.5.4. RAC-TS ma zastosowanie do następujących typów funkcji:

(a) przykłady odnoszące się do pokładowego podsystemu ETCS:

(1) „dostarcza maszyniście informacje umożliwiające mu bezpieczne prowadzenie pociągu i uruchamia funkcję hamowania w przypadku przekroczenia dopuszczalnej prędkości.” Na podstawie informacji uzyskanych na trasie pociągu (dozwolona prędkość) i w oparciu o prędkość obliczoną przez podsystem pokładowy ETCS, maszynista oraz podsystem pokładowy ETCS mogą pilnować, aby pociąg nie przekroczył dozwolonej prędkości. RAC-TS ma zastosowanie w przypadku oceny prędkości pociągu przez urządzenia pokładowe, ponieważ:

(i) nie ma żadnych dodatkowych barier (bezpośrednich), gdyż ocena informacji przekazywanych maszyniście jest również zaniżona;

(ii) nadmierna prędkość pociągu mogłaby doprowadzić do jego wykolejenia, będącego wypadkiem, który może mieć katastroficzne konsekwencje;

(2) „dostarcza maszyniście informacje umożliwiające mu bezpieczne prowadzenie pociągu i uruchamia funkcję hamowania w przypadku naruszenia pozwolenia przejazdu”,

(b) przykład dotyczący obwodu torowego: „wykrywanie zajętości danego odcinka toru”. RAC-TS będzie mogło zostać zastosowane w odniesieniu do tej funkcji tylko jeśli system blokad nie zostały wyposażony w funkcję „monitorowania sekwencji”;

(c) przykład dotyczący punktu: „kontrola położenia punktu”;

A.3.5.5. Niektóre normy definiują również funkcje, w przypadku których można zastosować RAC-TS. Na przykład:

(a) norma prEN 0015380-4 {Ref. 13} (ModTrain Work) w swojej części normatywnej definiuje trzy hierarchiczne poziomy funkcji (których liczba została zwiększona do pięciu w załącznikach informacyjnych). Norma prEN 0015380-4 definiuje ogółem kilkaset funkcji dotyczących pociągów;

(b) na ogół zaleca się wybór funkcji z trzech pierwszych poziomów prEN 0015380-4 (jednak nie poniżej), z uwzględnieniem również struktury produktowej;

(c) w przypadku funkcji nieobjętych zakresem normy prEN 0015380-4, odpowiedni poziom funkcjonalny należy określić w drodze porównania, wykorzystując w tym celu opinię eksperta.

European Railway Agency ● Marc LEFRANCQ, 120 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

Podane przykłady funkcji zawartych w normie prEN 0015380-4 nadal wymagają zaangażowania Agencji w ramach prac nad ogólnie dopuszczalnym ryzykiem oraz kryteriami akceptacji ryzyka.

A.3.5.6. RAC-TS ma również na przykład do funkcji prEN 0015380-4 „*kontrola przechyłu*" (kod = CLB). Funkcja ta może być wykorzystywana na poziomie systemu w następujący sposób:

(a) przypadek pierwszy: pociąg musi przechylać się na zakrętach, aby zapewnić wygodę pasażerów, należy także monitorować zgodność rozstawu kół pociągu z urządzeniami przytorowymi;

(b) przypadek drugi: pociąg musi przechylać się na zakrętach tylko ze względu na wygodę pasażerów, ale nie ma konieczności monitorowania zgodności rozstawu kół pociągu z urządzeniami przytorowymi.

RAC-TS zostanie zastosowane tylko w pierwszym przypadku, ponieważ w przypadku drugim uszkodzenie funkcji przechyłu nie będzie miało katastroficznych konsekwencji.

A.3.5.7. Przykład b) w pkt. A.3.5.4. oraz przykłady w pkt. A.3.5.6. załącznika A wyraźnie wskazują na brak możliwości stworzenia wykazu funkcji, w odniesieniu do których RAC-TS ma zastosowanie we wszystkich przypadkach. Zawsze będzie to zależeć od sposobu korzystania przez system z tych podfunkcji.

A.3.5.8. Przykładowe zastosowanie RAC-TS przedstawiono w części C.15. załącznika C.

A.3.6. Przykłady zastosowania RAC-TS

A.3.6.1. Wstęp

(a) W niniejszym rozdziale przedstawiono przykładowe sposoby określania wskaźnika awaryjności w przypadku innych niebezpiecznych awarii oraz obliczania wymogów bezpieczeństwa niższych niż 10^{-9}/godzinę. Niniejszy dokument nie zaleca żadnej konkretnej metody ani nie upoważnia do jej zastosowania. Ukazano w nim, wyłącznie w celach informacyjnych, sposób wykorzystania RAC-TS dla potrzeb kalibracji niektórych powszechnie stosowanych metod. Zagadnienie to nadal wymaga rozwinięcia w ramach prowadzonych przez Agencję prac nad ogólnie dopuszczalnymi rodzajami ryzyka oraz zasadami akceptacji ryzyka.

(b) W rzeczywistości RAC-TS może być stosowane bezpośrednio tylko w kilku przypadkach, ponieważ w praktyce niewiele błędów funkcjonalnych systemów technicznych jest bezpośrednią przyczyną wypadków, które mają katastroficzne konsekwencje. W związku z tym, aby zastosować to kryterium do zagrożeń, których konsekwencje nie są katastroficzne, oraz określić docelowy współczynnik awaryjności można wypracować kompromis (np. w drodze kalibracji matrycy ryzyka przez to kryterium) między różnymi parametrami, np. stopniem nasilenia w stosunku do częstotliwości.

A.3.6.2. Przykład 1: Bezpośredni kompromis dotyczący ryzyka

(a) RAC-TS może być w łatwy sposób stosowane w przypadku scenariuszy, które różnią się tylko kilkoma niezależnymi parametrami od warunków odniesienia zdefiniowanych w RAC-TS w części 2.5.4 rozporządzenia CSM {Ref. 3};

(b) przyjmijmy, że w przypadku konkretnego parametru p stosunek do ryzyka jest multiplikatywny. przyjmijmy, że p* jest obecne w warunku odniesienia, natomiast w scenariuszu alternatywnym zastosowanie ma p'. W takim przypadku istotny jest tylko

European Railway Agency ● Marc LEFRANCQ, 120 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

stosunek parametrów p* do p' i istnieje możliwość ograniczenia częstotliwości występowania. Procedurę tę można powtarzać, jeśli parametry są niezależne.

(c) Przykłady:

(1) przyjmijmy, że w opinii eksperta rzeczywista możliwość wystąpienia katastrofalnych skutków została oceniona jako dziesięciokrotnie mniejsza niż możliwość przewidziana w warunkach odniesienia w części 2.5.4 rozporządzenia CSM {Ref. 3}. W takim przypadku wymogiem byłoby 10^{-8}/na godzinę a nie 10^{-9}/na godzinę.

(2) przyjmijmy, że zidentyfikowano dodatkową barierę ochroną z innego systemu technicznego (niezależnie od skutków), której skuteczność wynosi 50% przypadków;

(3) wówczas wymóg bezpieczeństwa wynosiłby $5*10^{-7}$/godzinę (tj. $0,5*10^{-8}$/godzinę) zamiast 10^{-9}/godzinę.

A.3.6.3. Przykład 2: Kalibracja matrycy ryzyka

Tabela 5: Typowy przykład skalibrowanej matrycy ryzyka

Częstotliwość występowania wypadku (spowodowanego zagrożeniem)	**Poziomy ryzyka**			
Częste (10^{-4} na godzinę)	**Niedopuszczalne**	**Niedopuszczalne**	**Niedopuszczalne**	**Niedopuszczalne**
Prawdopodobne (10^{-5} na godzinę)	**Niedopuszczalne**	**Niedopuszczalne**	**Niedopuszczalne**	**Niedopuszczalne**
Sporadyczne (10^{-6} na godzinę)	**Dopuszczalne**	**Niedopuszczalne**	**Niedopuszczalne**	**Niedopuszczalne**
Rzadkie (10^{-7} na godzinę)	**Dopuszczalne**	**Dopuszczalne**	**Niedopuszczalne**	**Niedopuszczalne**
Mało prawdopodobne (10^{-8} na godzinę)	**Dopuszczalne**	**Dopuszczalne**	**Dopuszczalne**	**Niedopuszczalne**
Prawie niemożliwe (10^{-9} per hour)	**Dopuszczalne**	**Dopuszczalne**	**Dopuszczalne**	**Dopuszczalne**
	Nieznaczące	Marginalne	Krytyczne	Katastroficzne
	Poziomy konsekwencji zagrożenia (w przypadku wypadku)			

Ocena ryzyka	**Zmniejszenie/ nadzór ryzyka**
Nie do przyjęcia	Ryzyko należy wyeliminować.
Do przyjęcia	Ryzyko można zaakceptować. Wymagana jest niezależna ocena..

(a) Aby właściwie zastosować RAC-TS do matrycy ryzyka, musi być ona powiązana z odpowiednim poziomem systemu (porównywalnym do tego, o którym mowa w części A.3.5. załącznika A).

(b) RAC-TS definiuje jedno pole w matrycy ryzyka jako tolerowane, co odpowiada współrzędnej (stopień nasilenia katastrofalnych skutków; częstotliwość występowania 10^{-9}/godzinę): zob. czerwone pole w Tabela 5. Wszystkie pola, które odnoszą się do wyższej częstotliwości, muszą zostać oznaczone jako „niedopuszczalne". Należy zauważyć, że w przypadku realnej, bezpośredniej możliwości wystąpienia

European Railway Agency ● Marc LEFRANCQ, 120 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

katastroficznych konsekwencji, częstotliwość wypadków jest taka sama jak częstotliwość błędów funkcjonalnych.

(c) Następnie można uzupełnić pozostałą część matrycy, należy jednak uwzględnić takie skutki, jak na przykład unikanie ryzyka czy skalowanie kategorii. W najprostszym przypadku liniowego skalowania dekadowego (w Tabela 5 zaznaczonego strzałką) pole oznaczone w ten sposób jako „dopuszczalne" przez RAC-TS jest liniowo ekstrapolowane do pozostałej części matrycy. Oznacza to, że wszystkie pole leżące na tej samej przekątnej (lub poniżej) są również oznaczane jako „dopuszczalne". Również pola leżące poniżej mogą zostać oznaczone jako „dopuszczalne".

(d) wypełniona matryca może być zastosowana również w odniesieniu do zagrożeń, które nie pociągają za sobą katastrofalnych skutków. Jeśli na przykład inny błąd funkcjonalny charakteryzuje się stopniem nasilenia sklasyfikowanym jako „krytyczny", według skalibrowanej matrycy ryzyka dopuszczalna częstotliwość wypadków nie powinna przekraczać poziomu „mało prawdopodobne" (lub nawet niższego).

(e) należy zwrócić uwagę, że korzystanie z matrycy ryzyka może prowadzić do zbyt ostrożnych wyników, jeśli jest ona stosowana w odniesieniu do częstotliwości błędów funkcjonalnych (tj. błędów funkcjonalnych, które nie prowadzą bezpośrednio do wypadków).

A.3.6.4. Zasada kalibracji innych metod analizy ryzyka

Podobna procedura do tej, która została opisana w przypadku matrycy ryzyka, może zostać wykorzystana również w przypadku innych metod analizy ryzyka, np. proponowanego wskaźnika poziomu lub wykresu ryzyka z VDV 331 lub IEC 61508:

(a) etap pierwszy: sklasyfikowanie punktu odniesienia na podstawie RAC-TS jako tolerowanego, a punktów o wyższej częstotliwości lub większym stopniu nasilenia jako niedopuszczalne RAC-TS;

(b) etap drugi: zastosowanie mechanizmów kompromisu dla konkretnej metody w celu ekstrapolowania dopuszczalności ryzyka na zagrożenia, które nie pociągają za sobą katastroficznych konsekwencji (przyjmując za punkt wyjścia liniowe wyrównanie ryzyka);

(c) etap trzeci: w przypadku zagrożeń, które nie pociągają za sobą katastroficznych konsekwencji, RAC-TS można obliczyć za pomocą metody analizy ryzyka poprzez porównanie współrzędnej (częstotliwości, stopnia nasilenia) z otrzymaną w ten sposób krzywą F-N.

A.3.7. Wnioski dotyczące RAC-TS

A.3.7.1. W ramach proponowanej w rozporządzeniu CSM ogólnej struktury oceny ryzyka, kryteria akceptacji ryzyka są niezbędne do tego, by określić, w którym momencie szczątkowy poziom ryzyka staje się dopuszczalny, a zatem kiedy należy zakończyć szacowanie jawnego ryzyka.

A.3.7.2. RAC-TS jest celem projektowym (10^{-9}/godzinę) systemów technicznych.

A.3.7.3. Główne cele RAC-TS to:

(a) ustalenie górnej granicy dopuszczalności ryzyka, a zatem punktu odniesienia, na podstawie którego można przeprowadzić kalibrację metod analizy ryzyka w odniesieniu do systemów technicznych

European Railway Agency ● Marc LEFRANCQ, 120 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

(b) umożliwienie wzajemnego uznawania systemów technicznych, ponieważ oceny powiązanego ryzyka i bezpieczeństwa będą prowadzone według tej samej zasady akceptacji ryzyka we wszystkich państwach członkowskich;
(c) obniżenie kosztów, ponieważ nie wymaga ono zbyt wysokich ilościowych wymogów bezpieczeństwa;
(d) ułatwienie konkurencji między producentami. Stosowanie różnych zasad akceptacji ryzyka w zależności od wnioskodawcy lub państwa członkowskiego mogłoby doprowadzić do tego, że producenci musieliby zapewnić wiele różnych form przedstawienia tych samych systemów technicznych. Miałoby to negatywny wypływ na konkurencyjność producentów i doprowadziło niepotrzebnie do zbyt wysokiej ceny produktów.

A.3.7.4. W przypadku systemów technicznych nie zawsze istnieje konieczność wykazania zawartego w RAC-TS wymogu półilościowego. W rzeczywistości, w ramach zakresu CS, RAC-TS musi być stosowane tylko w odniesieniu do systemów technicznych, w przypadku których rozpoznane zagrożenia nie mogą być dostatecznie kontrolowane ani poprzez zastosowanie kodeksów postępowania, ani poprzez porównanie z podobnymi systemami odniesienia. Umożliwia to określenie niższych wymogów bezpieczeństwa, pod warunkiem możliwości utrzymania globalnego poziomu bezpieczeństwa.

A.3.7.5. Zharmonizowana półilościowa zasada akceptacji ryzyka dla systemów technicznych jest konieczna tylko w przypadku, gdy nie istnieją żadne kodeksy postępowania ani systemy odniesienia.

A.3.7.6. Ponieważ poziom nienaruszalności bezpieczeństwa w przypadku uszkodzeń/błędów systematycznych ogranicza się do SIL 4, poziom nienaruszalności bezpieczeństwa dla przypadkowego uszkodzenia sprzętu w systemie technicznym musi być również ograniczony do SIL 4. Odpowiada to maksymalnemu współczynnikowi tolerowanego zagrożenia rzędu 10^{-9}/godzinę (tj. maksymalnemu współczynnikowi awaryjności). Zgodnie z normą CENELEC 50 129, jeśli konieczne są bardziej rygorystyczne wymogi bezpieczeństwa, nie można ich osiągnąć za pomocą tylko jednego systemu; należy zmienić strukturę systemu, na przykład wykorzystując dwa systemy, co z całą pewnością spowoduje radykalny wzrost kosztów systemów technicznych. Bardziej szczegółowe informacje na ten temat można znaleźć w części A.3.1. załącznika A.

A.3.7.7. W części A.3.6. załącznika A opisano sposób wykorzystania RAC-TS jako punktu odniesienia dla kalibracji konkretnych metod analizy ryzyka, jeśli istnieje możliwość, że stopień nasilenia skutków dla systemów technicznych nie będzie katastrofalny.

A.4. Dane uzyskane z oceny bezpieczeństwa

A.4.1. Niniejsza część zawiera wytyczne dotyczące danych, które zazwyczaj są dostarczane organowi oceniającemu w celu umożliwienia niezależnej oceny i uzyskania akceptacji bezpieczeństwa bez uszczerbku dla wewnętrznych wymogów państwa członkowskiego. Można ją wykorzystać, we właściwych przypadkach, jako listę kontrolną w celu sprawdzenia, czy wszystkie stosowne aspekty zostały uwzględnione i udokumentowane w trakcie stosowania CSM.

A.4.2. Plan bezpieczeństwa: CENELEC zaleca, aby przygotowywać plan bezpieczeństwa na początku inwestycji, lub - jeśli nie jest to dogodne z punktu widzenia inwestycji - dołączyć opis planu do jakiegokolwiek innego stosownego dokumentu. Plan bezpieczeństwa można również przedłożyć do zaopiniowania jednsotkom oceniającym, jeżeli zostały wyznaczone na początku inwestycji. Z reguły plan bezpieczeństwa opisuje:

European Railway Agency ● Marc LEFRANCQ, 120 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

(a) zastosowaną organizację i kompetencje osób zaangażowanych w opracowanie inwestycji i ocenę ryzyka;
(b) wszelkie czynności związane z bezpieczeństwem, które są zaplanowane na różnych etapach inwestycji, a także oczekiwane rezultaty.

A.4.3. Wymagane dane z etapu definiowania systemu:

(a) opis systemu:

(1) definicja zakresu/granic systemu;
(2) opis funkcji;
(3) opis struktury systemu;
(4) opis warunków eksploatacyjnych i środowiskowych;

(b) opis zewnętrznych interfejsów;
(c) opis wewnętrznych interfejsów;
(d) opis etapów cyklu życia systemu;
(e) opis zasad bezpieczeństwa;
(f) opis założeń określających zakres oceny ryzyka.

A.4.4. W celu umożliwienia przeprowadzenia oceny ryzyka, w definicji systemu uwzględnia się kontekst planowanej zmiany:

(a) jeżeli planowana zmiana polega na modyfikacji istniejącego systemu, definicja systemu opisuje zarówno system przed zmianą, jak i po wprowadzeniu planowanej zmiany;
(b) jeżeli planowana zmiana polega na budowie nowego systemu, opis ogranicza się do definicji systemu, ponieważ nie ma żadnego opisu istniejącego systemu.

A.4.5. Wymagane dane z etapu identyfikacji ryzyka:

(a) opis i uzasadnienie (w tym ograniczenia) metod i narzędzi identyfikacji zagrożeń (metody odgórna, oddolna, HAZOP itp.);
(b) wyniki:

(1) wykaz zagrożeń;
(2) (graniczne) zagrożenia na poziomie systemu;
(3) zagrożenia na poziomie podsystemu;
(4) zagrożenia na interfejsach;
(5) środki bezpieczeństwa, które można wskazać na tym etapie.

A.4.6. Wymagane są również następujące dane z etapu analizy ryzyka:

(a) jeżeli w celu kontrolowania zagrożeń stosowane są normy czynnościowe – wykazanie, że w odniesieniu do systemu objętego oceną spełnione są wszystkie stosowne wymogi z kodeksów postępowania. Dotyczy to również wykazania, że stosowne kodeksy postępowania zostały prawidłowo zastosowane;

(b) jeżeli podobne systemy odniesienia są stosowane w celu kontrolowania zagrożeń:

(1) definicja wymogów bezpieczeństwa z odpowiednich systemów odniesienia dla systemu objętego oceną;
(2) wykazanie, że system objęty oceną jest stosowany w takich samych warunkach eksploatacyjnych i środowiskowych, jak odpowiedni system odniesienia. Jeżeli nie jest to możliwe – wykazanie, że odchylenia od systemu odniesienia zostały prawidłowo ocenione;
(3) dowody, że wymogi bezpieczeństwa z systemów odniesienia zostały poprawnie wdrożone w systemie objętym oceną;

(c) jeżeli w celu kontrolowania zagrożeń stosowane jest szacowanie jawnego ryzyka :

European Railway Agency ● Marc LEFRANCQ, 120 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

(1) opis i uzasadnienie (w tym ograniczenia) metod i narzędzi analizy ryzyka (analiza jakościowa, ilościowa, półilościowa, analiza braku pogorszenia, …);
(2) wskazanie istniejących środków bezpieczeństwa i czynników zmniejszających ryzyko w odniesieniu do każdego zagrożenia (w tym aspekty czynnika ludzkiego);
(3) wycena i uszeregowanie ryzyka w odniesieniu do każdego zagrożenia:
    (i) oszacowanie konsekwencji zagrożenia i uzasadnienie (wraz z przyjętymi założeniami i warunkami);
    (ii) oszacowanie częstotliwości zagrożenia i uzasadnienie (wraz z przyjętymi założeniami i warunkami);
    (iii) uszeregowanie zagrożeń według stopnia powagi i częstotliwości występowania;
(4) wskazanie dodatkowych, odpowiednich środków bezpieczeństwa skutkujących akceptowalnymi rodzajami ryzyka w odniesieniu do każdego zagrożenia (iteracyjny proces po etapie wyceny ryzyka).

A.4.7. Wymagane dane z wyceny ryzyka:

(a) w przypadku przeprowadzenia jednoznacznego oszacowania ryzyka:
    (1) definicja i uzasadnienie kryteriów wyceny ryzyka w odniesieniu do każdego zagrożenia;
    (2) wykazanie/uzasadnienie, że środki bezpieczeństwa i wymogi bezpieczeństwa uwzględniają każde zagrożenie do poziomu dopuszczalnego (zgodnie z wyżej wymienionymi kryteriami wyceny ryzyka);
(b) zgodnie z częściami 2.3.5 i 2.4.3 rozporządzenia CSM, przyjmuje się, że ryzyko objęte zastosowaniem kodeksów postępowania oraz porównaniem z systemami odniesienia jest dopuszczalne, pod warunkiem, że (zob. wykropkowane miejsce w Schemat 1):
    (1) warunki stosowania kodeksów postępowania opisane w części 2.3.2 są spełnione;
    (2) warunki wykorzystania systemów odniesienia opisane w części 2.4.2 są spełnione.

    Kryteria akceptacji ryzyka w odniesieniu do tych dwóch zasad akceptacji ryzyka są domniemane.

A.4.8. Dane z zarządzania zagrożeniami:

(a) zamieszczenie wszystkich zagrożeń w wykazie zagrożeń, zawierającym następujące informacje:
    (1) zidentyfikowane zagrożenie;
    (2) środki bezpieczeństwa zapobiegające wystąpieniu zagrożenia lub łagodzące jego skutki;
    (3) wymogi bezpieczeństwa dotyczące środków;
    (4) właściwa część systemu;
    (5) podmiot odpowiedzialny za środki bezpieczeństwa;
    (6) status zagrożenia (np. otwarte, zażegnane, usunięte, przekazane, kontrolowane itp.);
    (7) data zamieszczenia, przeglądu i kontroli każdego zagrożenia.
(b) opis sposobu skutecznego zarządzania zagrożeniami w całym cyklu życia systemu;
(c) opis sposobu wymiany informacji pomiędzy stronami na temat zagrożeń na interfejsach i podział obowiązków.

A.4.9. Dowody dotyczące jakości procesu oceny i wyceny ryzyka:

(a) opis osób zaangażowanych w proces i ich kompetencji;

European Railway Agency ● Marc LEFRANCQ, 120 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

(b) w przypadku jednoznacznego oszacowania ryzyka, opis informacji, danych i innych danych statystycznych wykorzystanych w procesie oraz uzasadnienie ich adekwatności (np. analiza poufności wykorzystanych danych).

A.4.10. Dowody zgodności z wymogami bezpieczeństwa:

(a) wykaz zastosowanych norm;
(b) opis projektu i zasad eksploatacji;
(c) dane dotyczące zastosowania dobrego systemu zarządzania jakością i bezpieczeństwem w odniesieniu do inwestycji: zob. pkt [G 3] w części 1.1.2;
(d) podsumowanie sprawozdań z analizy bezpieczeństwa (np. analizy przyczyn zagrożenia), w którym wykazano spełnienie wymogów bezpieczeństwa;
(e) opis i uzasadnienie metod i narzędzi (FMECA, FTA, …), które są stosowane do analizy przyczyny zagrożenia;
(f) podsumowanie testów weryfikacji i legalizacji pod względem bezpieczeństwa.

A.4.11. Dowód bezpieczeństwa: CENELEC radzi, aby wszystkie wyżej wymienione dowody zostały zebrane i podsumowane w jednym dokumencie, który jest przedkładany organowi oceniającemu: zob. pkt. [G 4] i [G 5] w części 5.1.

European Railway Agency ● Marc LEFRANCQ, 120 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

ZAŁĄCZNIK B: PRZYKŁADY TECHNIK I NARZĘDZI WSPOMAGAJĄCYCH PROCES OCENY RYZYKA

B.1. W załączniku E wytycznych do normy EN 50123-2 {Ref. 9} można znaleźć przykłady technik i narzędzi służących do prowadzenia działań związanych z oceną ryzyka uwzględnionych w CSM. Tabela E.1 zawiera podsumowanie technik i narzędzi. Każda technika została opisana i - w stosownie do potrzeb - opatrzona odesłaniem do innych norm w celu uzyskania dodatkowych informacji.

European Railway Agency ● Marc LEFRANCQ, 120 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

ZAŁĄCZNIK C: PRZYKŁADY

C.1. Wprowadzenie

C.1.1. Niniejszy załącznik ma na celu ułatwienie lektury niniejszego dokumentu. W załączniku zgromadzono wszystkie zebrane przykłady, które mają ułatwić zastosowanie CSM.

C.1.2. Przykłady ocen ryzyka lub ocen bezpieczeństwa, które przedstawiono w niniejszym załączniku, nie są wynikiem zastosowania procesu CSM, ponieważ oceny te przeprowadzono jeszcze zanim powstało rozporządzenie CSM. Zastosowano następującą klasyfikację przykładów:

(a) przykłady, z odwołaniem do ich źródła, uzyskane od ekspertów z grupy roboczej ds. CSM;
(b) przykłady, celowo nie opatrzone odwołaniem do ich źródła, również uzyskane od ekspertów z grupy roboczej ds. CSM. Na prośbę ekspertów źródło tych przykładów jest poufne;
(c) przykłady, których źródło nie zostało podane, i które zostały przygotowane przez pracowników Agencji w oparciu o ich własne, wcześniejsze doświadczenie zawodowe.

W odniesieniu do każdego przykładu podano powiązania pomiędzy stosowanym procesem a procesem wymaganym przez CSM, jak również uzasadnienie i wartość dodaną w celu przeprowadzenia (w razie potrzeby) dodatkowych kroków, wymaganych przez CSM.

C.2. Przykłady zastosowania kryteriów znaczącej zmiany w Artykuł 4 ust. 2

C.2.1. Agencja pracuje nad zdefiniowaniem tego, co można uznać za „znaczącą zmianę". W niniejszej części zamieszczono jeden przykład tych prac dotyczący sposobu stosowania kryteriów w Artykuł 4 ust. 2.

C.2.2. Zmiana polega na zmodyfikowaniu sposobu przekazywania informacji przez nastawniczego dróżnikowi przejazdowemu o kierunku jazdy nadjeżdżającego pociągu na poziomie ręcznie obsługiwanego przejazdu kolejowego. Zmianę przedstawiono na Schemat 15.

Schemat 15: Przykład nieznaczącej zmiany
Wiadomość telefoniczna w celu kontrolowania przejazdu kolejowego.

C.2.3. Istniejący system: przed dokonaniem planowanej zmiany dróżnik przejazdowy otrzymywał informację o kierunku jazdy nadjeżdżającego pociągu automatycznie za pomocą sygnału

European Railway Agency ● Marc LEFRANCQ, 120 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

tonowego dzwoniącego telefonu. Sygnał tonowy był różny, w zależności od tego, skąd dzwoniono.

C.2.4. Planowana zmiana: ponieważ stary system telefoniczny staje się przestarzały i trzeba go zastąpić nowym cyfrowym systemem, przekazywanie takich informacji za pomocą sygnału tonowego nie będzie już możliwe ze względów technicznych. Sygnał tonowy jest dokładnie taki sam niezależnie od tego, który nastawniczy dzwoni. Zdecydowano zatem, że tę samą funkcję można osiągnąć, stosując procedurę operacyjną:

(a) po wyjeździe pociągu nastawniczy ustnie informuje dróżnika przejazdowego o kierunku jazdy nadjeżdżającego pociągu;

(b) informacja jest porównywana z rozkładem jazdy i potwierdzana zarówno przez dróżnika przejazdowego, jak i innego nastawniczego, aby upewnić się, że dróżnik właściwie zrozumiał informację.

Schemat 15 przedstawia planowaną zmianę i procedurę operacyjną.

C.2.5. Mimo że wydaje się, iż ta zmiana może mieć potencjalny wpływ na bezpieczeństwo (ryzyko, że szlaban kolejowy nie zostanie opuszczony na czas), pozostałe kryteria podane w Artykuł 4 ust. 2, takie jak:

(a) niewielka złożoność;
(b) brak innowacyjności, oraz;
(c) łatwość monitorowania;

sugerują, że planowana zmiana nie jest zmianą znaczącą.

C.2.6. W tym przykładzie konieczne jest jednak przeprowadzenie analizy bezpieczeństwa lub przedstawienie argumentów, aby wykazać, że w przypadku takiego zadania istotnego z punktu widzenia bezpieczeństwa, zastąpienie starego systemu technicznego procedurą operacyjną (która zakłada, że pracownicy sprawdzają się nawzajem) będzie skutkowało podobnym poziomem bezpieczeństwa. Rodzi się pytanie, czy konieczne będzie zastosowanie pełnego procesu CSM, z rejestrem zagrożeń, niezależną oceną przez jednostkę oceniającą itd. W tym przypadku nie jest pewne, czy z takiej zmiany wyniknęłaby jakakolwiek wartość dodana, co sugeruje, że taka zmiana nie zostałaby w rezultacie uznana za znaczącą.

C.3. Przykłady interfejsów pomiędzy podmiotami sektora kolejowego

C.3.1. Poniżej podano kilka przykładów interfejsów i powodów współpracy pomiędzy podmiotami sektora kolejowego:

(a) zarządca infrastruktury – zarządca infrastruktury: na przykład w obydwu infrastrukturach należy przewidzieć środki bezpieczeństwa w celu zapewnienia bezpiecznego przejazdu pociągów pomiędzy jedną infrastrukturą a drugą;

(b) zarządca infrastruktury – przedsiębiorstwo kolejowe: na przykład można określić szczegółowe zasady eksploatacyjne zależne od infrastruktury, których musi przestrzegać maszynista;

(c) zarządca infrastruktury – producent: na przykład podsystemy producenta mogą mieć ograniczenia stosowania, których musi przestrzegać zarządca infrastruktury;

(d) zarządca infrastruktury – dostawca usług: na przykład mogą istnieć szczególne ograniczenia dotyczące utrzymania infrastruktury, których musi przestrzegać podwykonawca prac związanych z utrzymaniem ruchu;

European Railway Agency ● Marc LEFRANCQ, 120 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

(e) przedsiębiorstwo kolejowe – producent: na przykład podsystemy producenta mogą mieć ograniczenia stosowania, których musi przestrzegać przedsiębiorstwo kolejowe;

(f) przedsiębiorstwo kolejowe – dostawca usług: na przykład mogą istnieć szczególne ograniczenia dotyczące utrzymania infrastruktury, których musi przestrzegać podwykonawca prac w zakresie utrzymania;

(g) przedsiębiorstwo kolejowe – posiadacze: na przykład mogą istnieć ograniczenia użytkowania dotyczące pojazdów, których musi przestrzegać przedsiębiorstwo kolejowe eksploatujące te pojazdy;

(h) producent – producent: na przykład zarządzanie technicznymi interfejsami związanymi z bezpieczeństwem pomiędzy podsystemami pochodzącymi od dwóch różnych producentów;

(i) producent – dostawca usług: na przykład zarządzanie rejestrem zagrożeń przez producenta w przypadku zlecania podwykonania pewnych prac spółce, która jest zbyt mała, aby posiadać organizację bezpieczeństwa w zakresie danej inwestycji;

(j) dostawca usług – dostawca usług: podobny przykład jak w pkt. j) powyżej.

C.3.2. Dostawcy usług wykonują wszystkie prace zlecane przez zarządcę infrastruktury albo przez przedsiębiorstwo kolejowe lub producenta, takie jak utrzymanie ruchu, obsługa biletowa, usługi inżynieryjne itp.

C.3.3. W celu zilustrowania zarządzania interfejsami i identyfikacji powiązanych zagrożeń podano poniższy przykład, który dotyczy interfejsu pomiędzy producentem pociągu i wnioskodawcą (przedsiębiorstwem kolejowym). Przykład opisuje następnie, w jaki sposób można spełnić główne kryteria wymagane zgodnie z pkt. [G 3] części 1.2.1:

(a) Kierownictwo: wnioskodawca (przedsiębiorstwo kolejowe);

(b) Dane wejściowe:

(1) wykazy znaczących zagrożeń pochodzących z podobnych projektów;
(2) opis wszystkich danych wejściowych i wyjściowych (I/O) w odniesieniu do interfejsu, w tym właściwości eksploatacyjnych;

(c) Metody: zob. załącznik A.2 wytycznych do normy EN 50 126-2 {Ref. 9};

(d) Wymagani uczestnicy:

(1) kierownik ds. zapewnienia bezpieczeństwa wnioskodawcy (przedsiębiorstwa kolejowego)
(2) kierownik ds. zapewnienia bezpieczeństwa producenta pociągu;
(3) organ projektowy wnioskodawcy pociągu;
(4) organ projektowy producenta pociągu;
(5) personel ds. utrzymania ruchu wnioskodawcy pociągu (częściowo w zależności od analizowanych danych wejściowych/wyjściowych);
(6) maszyniści (częściowo w zależności od analizowanych danych wejściowych/wyjściowych);

(e) Rezultaty:

(1) wspólnie uzgodniony raport z identyfikacji zagrożeń;
(2) środki bezpieczeństwa dotyczące rejestru zagrożeń z jasnym opisem obowiązków.

European Railway Agency ● Marc LEFRANCQ, 120 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

C.4. Przykłady metod określania ogólnie dopuszczalnych rodzajów ryzyka

C.4.1. Wprowadzenie

C.4.1.1. Ogólnie dopuszczalne ryzyko jest zdefiniowane w rozporządzeniu CSM jako ryzyko, którego poziom *„jest na tyle niski, że nie jest konieczne podejmowanie natychmiastowych działań w celu jego zredukowania".* Sklasyfikowanie niektórych zagrożeń jako zagrożenia związane z ogólnie dopuszczalnym ryzykiem w trakcie identyfikacji zagrożeń pozwala pominąć dalszą analizę tych zagrożeń w procesie oceny ryzyka. Definicja ogólnie dopuszczalnego ryzyka przytoczona powyżej daje pewną swobodę interpretacji. Dlatego też w rozporządzeniu zaznaczono, że decyzję o sklasyfikowaniu zagrożeń jako związane z ogólnie dopuszczalnym ryzykiem pozostawia się w gestii eksperta.

C.4.1.2. Rzeczywiście trudno jest określić wspólne, bardziej jednoznaczne kryterium ogólnie dopuszczalnego ryzyka, które można by było zastosować na wszystkich różnych możliwych poziomach systemu, na których można zidentyfikować zagrożenia, a także które uwzględniałoby różne czynniki związane z unikaniem ryzyka, które mogłyby dominować w przypadku różnych zastosowań. Ponieważ jednak należy zagwarantować, aby opinie ekspertów były zrozumiałe i łatwe do uzasadnienia, przydatne mogą być wytyczne, określające sposób definiowania ryzyka jako ogólnie dopuszczalne. Kryteria definiowania ogólnie dopuszczalnych rodzajów ryzyka mogą być ilościowe, jakościowe lub półjakościowe. Poniżej podano kilka przykładów, w jaki sposób ustalić kryteria, które pozwalają na ocenę ogólnie dopuszczalnych rodzajów ryzyka metodą ilościową i półilościową.

C.4.1.3. Poniższe przykłady ilustrują tę zasadę. Zaczerpnięto je z publikacji: „Die Gefährdungseinstufung im ERA-Risikomanagementprozess*", Kurz, Milius, Signal +Draht (100) 9/2008.*

C.4.2. Ustalenie kryterium ilościowego

C.4.2.1. Ogólnie dopuszczalne ryzyko można zdefiniować jako ryzyko, które jest znacznie mniejsze niż dopuszczalne ryzyko dla danej klasy zagrożeń. Wykorzystując dane statystyczne można byłoby ewentualnie obliczyć bieżący poziom ryzyka dla systemów kolejowych i tym samym uznać taki wyliczony poziom za dopuszczalny. Dzieląc ten poziom ryzyka przez liczbę (L) zagrożeń (na przykład w sposób dowolny można założyć, że istnieje około L = 100 głównych kategorii zagrożeń w systemie kolejowym), otrzymujemy dopuszczalny poziom ryzyka na kategorię zagrożeń. Można następnie stwierdzić, że zagrożenie oznaczające ryzyko, które jest o dwa rzędy wielkości niższe od dopuszczalnego poziomu ryzyka na zagrożenie (jest to parametr x% w pkt. [G 1] części 2.2.3), zostałoby uznane za ogólnie dopuszczalne ryzyko.

C.4.2.2. Należy jednak upewnić się, czy udział wszystkich zagrożeń związanych z ogólnie dopuszczalnym ryzykiem nie przekracza określonej części (np. y%) całego ryzyka na poziomie systemu: zob. część 2.2.3 i wyjaśnienia w pkt. [G 2] części 2.2.3.

C.4.3. Wycena ogólnie dopuszczalnych rodzajów ryzyka

C.4.3.1. Wartości graniczne dla ogólnie dopuszczalnych rodzajów ryzyka, wyprowadzone w wyżej podanych w przykładach, można następnie wykorzystać do kalibracji narzędzi ilościowych, takich jak matryca ryzyka, wykres ryzyka, wskaźnik poziomu ryzyka (risk priority number), aby ułatwić ekspertowi podjęcie decyzji o sklasyfikowaniu ryzyka jako ogólnie dopuszczalne. Należy podkreślić, że przyjęcie wartości ilościowych jako kryteriów ogólnie dopuszczalnych rodzajów ryzyka nie oznacza, że konieczne jest przeprowadzenie dokładnego oszacowania

European Railway Agency ● Marc LEFRANCQ, 120 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

lub analizy ryzyka w celu podjęcia decyzji, czy takie ryzyko jest ogólnie dopuszczalne. W tym momencie ocena eksperta jest stosowana do przeprowadzenia orientacyjnego oszacowania na etapie identyfikacji zagrożeń.

C.4.3.2. Należy również sprawdzić, czy udział wszystkich zagrożeń związanych z ogólnie dopuszczalnym ryzykiem nie przekracza danej części (np. y%) całego ryzyka na poziomie systemu: zob. część 2.2.3 i wyjaśnienia w pkt. [G 2] części 2.2.3.

C.5. Przykład oceny ryzyka znaczącej zmiany organizacyjnej

C.5.1. **Uwaga:** ten przykład oceny ryzyka nie jest wynikiem zastosowania procesu CSM; został przygotowany przed powstaniem CSM. Przykład ten ma na celu:

(a) wskazanie podobieństw pomiędzy istniejącymi metodami oceny ryzyka i procesem CSM;
(b) umożliwienie prześledzenia powiązań pomiędzy istniejącym procesem i procesem wymaganym przez CSM;
(c) uzasadnienie wartości dodanej wynikającej z przeprowadzenia (w razie potrzeby) dodatkowych etapów, wymaganych przez CSM.

Należy zaznaczyć, że ten przykład zamieszczono wyłącznie w celach informacyjnych. Ma on ułatwić czytelnikowi zrozumienie procesu CSM. Samego przykładu nie można jednak przetransponować do systemu odniesienia lub wykorzystać jako systemu odniesienia dla innej znaczącej zmiany. Ocena ryzyka jest dokonywana w odniesieniu do każdej istotnej zmiany zgodnie z rozporządzeniem CSM.

C.5.2. Ten przykład dotyczy zmiany organizacyjnej. Wnioskodawca uznał tę zmianę za istotną. Zastosowano podejście oparte na ocenie ryzyka, aby ocenić tę zmianę.

C.5.3. Wydział organizacji zarządcy infrastruktury, który do momentu wprowadzenia zmiany wykonywał niektóre prace w zakresie utrzymania ruchu (niezwiązane z sygnalizacją i telematyką), musiał stanąć do konkurencji z innymi spółkami prowadzącymi działalność w tej samej dziedzinie. Bezpośrednim skutkiem była konieczność ograniczenia liczby personelu i rozdział pracowników i zadań w wydzielonym oddziale zarządcy infrastruktury, który musiał zmierzyć się z konkurencją.

C.5.4. Obawy zarządcy infrastruktury, którego dotknęła zmiana:

(a) personel zarządcy infrastruktury, na który miała wpływ zmiana, odpowiadał za prace związane z utrzymania ruchu w sytuacjach awaryjnych i naprawy wymuszone przez nagłe błędy w infrastrukturze. Personel wykonywał również pewne zaplanowane lub wynikające z inwestycji prace w zakresie utrzymania ruchu, takie jak: podsypki torów, czyszczenie podsypki, usuwanie roślinności przy torach;

(b) uważano, że zadania te miały decydujące znaczenie dla bezpieczeństwa i terminowości eksploatacji. Należało zatem poddać je analizie, aby znaleźć odpowiednie środki, które zagwarantują, że sytuacja się nie pogorszy w związku z tym, że wiele osób odpowiadających za środki bezpieczeństwa opuści zarządcę infrastruktury.

(c) należy utrzymać taki sam poziom bezpieczeństwa i punktualności pociągów w trakcie i po wprowadzeniu zmiany w organizacji.

C.5.5. W porównaniu do procesu CSM zastosowano następujące etapy (zob. również Schemat 1):

(a) opis systemu [część 2.1.2]:

European Railway Agency ● Marc LEFRANCQ, 120 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

(1) opis zadań wykonywanych przez istniejącą organizację (tj. przez zarządcę infrastruktury przed wprowadzeniem zmiany);
(2) opis planowanych zmian w organizacji zarządcy infrastruktury.
(3) interfejsy między „oddziałem, który ma zostać wydzielony" i innymi organizacjami w środowisku lub środowiskiem fizycznym można opisać jedynie pobieżnie. Nie jest możliwe w 100% jednoznaczne wyznaczenie granic;

(b) identyfikacja zagrożeń [część 2.2]:

(1) narada grupy ekspertów metodą burzy mózgów:

(i) w celu ustalenia wszystkich zagrożeń, które mają istotne znaczenie dla ryzyka wywołanego planowaną zmianą organizacyjną;

(ii) w celu wskazania możliwych działań służących kontrolowaniu ryzyka;

(2) klasyfikacja zagrożeń:

(i) pod względem stopnia powiązanego ryzyka: wysokie, średnie, niskie ryzyko;

(ii) pod względem wpływu zmiany: zwiększone, niezmienione, zmniejszone ryzyko;

(c) wykorzystanie systemu odniesienia [część 2.4]:

Oceniono, że system sprzed zmiany posiadał dopuszczalny poziom bezpieczeństwa. Następnie użyto go jako „system odniesienia", aby ustalić kryteria akceptacji ryzyka dla zmiany w organizacji.

(d) jawne szacowanie i wycena ryzyka [część 2.5]:

W odniesieniu do każdego zagrożenia prowadzącego do zwiększonego ryzyka z powodu zmiany w organizacji wskazuje się środki ograniczenia ryzyka. Ryzyko szczątkowe jest porównywane z zasadami akceptacji ryzyka z systemu odniesienia, aby sprawdzić, czy należy wskazać dodatkowe środki;

(e) wykazanie zgodności systemu z wymogami bezpieczeństwa [część 3]:

(1) z analizy ryzyka i wykazu zagrożeń wynika, że zagrożeń nie można kontrolować, dopóki nie zostaną zweryfikowane i dopóki nie zostanie wykazane, że wymogi bezpieczeństwa (tj. wybrane środki bezpieczeństwa) są przestrzegane;
(2) analiza ryzyka i rejestr zagrożeń były ciągle aktualizowanymi dokumentami. Skuteczność przedsięwziętych działań była monitorowana w regularnych odstępach czasu, aby sprawdzić, czy warunki uległy zmianie i czy konieczna jest aktualizacja analizy ryzyka i wyceny ryzyka;
(3) jeżeli wdrożone środki nie były wystarczająco skuteczne, ponownie aktualizowano i monitorowano analizę ryzyka, wycenę ryzyka oraz rejestr zagrożeń;

(f) zarządzanie zagrożeniami [część 4.1]:

Zidentyfikowane zagrożenia i wskazane środki bezpieczeństwa zamieszczono w rejestrze zagrożeń i monitorowano. Jeden z wniosków wynikających z przykładów dotyczył potrzeby ciągłego aktualizowania analizy ryzyka i rejestru zagrożeń w miarę podejmowania decyzji i działań w trakcie zmiany w organizacji. Analiza ryzyka obejmowała również ryzyko dla interfejsu, na przykład z podwykonawcami i przedsiębiorcami.

W części C.16.2. załącznika C podano strukturę i obszary wykorzystane do sporządzenia rejestru zagrożeń, jak również fragment rejestru.

(g) niezależna ocena [Artykuł 6]:

Przeprowadzono również niezależną ocenę przez osoby trzecie w celu:

European Railway Agency ● Marc LEFRANCQ, 120 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

(1) sprawdzenia, czy zarządzanie ryzykiem i ocena ryzyka zostały prawidłowo przeprowadzone;
(2) sprawdzenia, czy zmiana organizacyjna jest odpowiednia i czy umożliwi utrzymanie poziomu bezpieczeństwa sprzed zmiany.

C.5.6. Ten przykład pokazuje, że zasady wymagane przez wspólną metodę oceny bezpieczeństwa są metodami już istniejącymi w sektorze kolejowym i stosuje się je do oceny ryzyka zmian operacyjnych. Ocena ryzyka zastosowana w przykładzie spełnia wszystkie wymogi z CSM. Zastosowano w niej dwie z trzech zasad akceptacji ryzyka, dopuszczonych w zharmonizowanym podejściu w zakresie CSM:

(a) „system odniesienia" jest stosowany w celu określenia kryteriów akceptacji ryzyka niezbędnych do oceny dopuszczalności ryzyka zmiany organizacyjnej;
(b) „jawne szacowanie i wycena ryzyka":

(1) w celu dokonania analizy odstępstw zmiany od systemu odniesienia;
(2) w celu wskazania środków ograniczenia ryzyka dla zwiększonego ryzyka wynikającego ze zmiany;
(3) w celu oszacowania, czy osiągnięto dopuszczalny poziom ryzyka.

C.6. Przykład oceny ryzyka istotnej zmiany eksploatacyjnej – Zmiana godzin kursowania

C.6.1. **C.5.1.** Uwaga: ten przykład oceny ryzyka nie jest wynikiem zastosowania procesu CSM; został przygotowany przed powstaniem CSM. Przykład ten ma na celu:

(a) wskazanie podobieństw pomiędzy istniejącymi metodami oceny ryzyka i procesem CSM;
(b) umożliwienie prześledzenia powiązań pomiędzy istniejącym procesem i procesem wymaganym przez CSM;
(c) uzasadnienie wartości dodanej wynikającej z przeprowadzenia (w razie potrzeby) dodatkowych etapów, wymaganych przez CSM.

Należy zaznaczyć, że ten przykład zamieszczono wyłącznie w celach informacyjnych. Ma on ułatwić czytelnikowi zrozumienie procesu CSM. Samego przykładu nie można jednak przetransponować do systemu odniesienia lub wykorzystać jako systemu odniesienia dla innej znaczącej zmiany. Ocena ryzyka jest dokonywana w odniesieniu do każdej istotnej zmiany zgodnie z rozporządzeniem CSM.C.6.2. Ten przykład dotyczy zmiany eksploatacyjnej, w wyniku której przedsiębiorstwo kolejowe chciało wyznaczyć maszynistom nowe trasy i w miarę możliwości nowe godziny pracy (w tym system rotacji pracy i system zmianowy).

C.6.3. W porównaniu do procesu CSM zastosowano następujące etapy (zob. również Schemat 1):

(a) znaczenie zmiany [Artykuł 4]:

Przedsiębiorstwo kolejowe przeprowadziło wstępną ocenę ryzyka, w wyniku której stwierdzono, że zmiana eksploatacyjna była znacząca. W związku z tym, że maszyniści musieli pokonywać nowe trasy, prawdopodobnie poza swoimi normalnymi godzinami pracy, nie można było lekceważyć możliwości minięcia sygnału o niebezpieczeństwie, jazdy z nadmierną prędkością lub ignorowania czasowych ograniczeń prędkości.

Porównując tę wstępną ocenę ryzyka z kryteriami podanymi w Artykuł 4 ust. 2 rozporządzenia CSM, zmianę można również sklasyfikować jako istotną na podstawie następujących kryteriów:

European Railway Agency ● Marc LEFRANCQ, 120 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

(1) znaczenie dla bezpieczeństwa: zmiana jest związana z bezpieczeństwem, ponieważ zmiana trybu pracy maszynistów może mieć katastroficzne konsekwencje;
(2) skutki awarii: wyżej wymienione błędy maszynistów mogą potencjalnie doprowadzić do katastroficznych konsekwencji;
(3) innowacyjność: przedsiębiorstwo kolejowe potencjalnie może wprowadzić nowe schematy pracy dla maszynistów;
(4) złożoność zmiany: zmiana godzin kursowania może być skomplikowana, ponieważ będzie wymagała pełnej oceny i zmiany istniejących warunków pracy;

(b) definicja systemu [część 2.1.2]:

Pierwotnie definicja systemu opisywała:

(1) istniejące warunki pracy: godziny pracy, system zmianowy itp.;
(2) zmiany godzin pracy;
(3) interfejsy (np. z zarządcą infrastruktury)

W trakcie różnych iteracji definicję systemu zaktualizowano o wymogi bezpieczeństwa wynikające z procesu oceny ryzyka. W proces iteracji zostali włączeni najważniejsi przedstawiciele personelu w celu zidentyfikowania zagrożeń i zaktualizowania definicji systemu.

(c) identyfikacja zagrożeń [część 2.2]:

W wyniku narady grupy ekspertów, w tym przedstawicieli maszynistów, metodą burzy mózgów zidentyfikowano zagrożenia i wskazano możliwe środki bezpieczeństwa dla nowych tras i systemów zmianowych. Przeanalizowano nowe zadania maszynistów pod kątem nowych warunków, aby ocenić, czy miały one wpływ na maszynistów, ich obciążenie pracą, zakres geograficzny i czas pracy w systemie zmianowym.
Przedsiębiorstwo kolejowe skonsultowało się również ze związkami zawodowymi, aby - w miarę możliwości - uzyskać dodatkowe informacje oraz przeanalizowało ryzyko zmęczenia i zachorowań, które mogłyby wynikać z możliwego wzrostu liczby nadgodzin z powodu wydłużonego czasu jazdy na nieznanych trasach.
Każdemu z zagrożeń przypisano określony stopień ryzyka i skutków (wysoki, średni, niski) oraz w stosunku do nich oceniono wpływ proponowanej zmiany (zwiększone, niezmienione, zmniejszone ryzyko).

(d) wykorzystanie kodeksów postępowania [część 2.3]:

Zastosowano kodeksy postępowania dotyczące godzin pracy i ryzyka zmęczenia ludzi, aby dokonać przeglądu istniejących warunków pracy i określić nowe wymogi bezpieczeństwa. Zgodnie z kodeksami postępowania opracowano niezbędne zasady operacyjne dotyczące nowego, zmianowego systemu pracy. Wszystkie strony zaangażowane w opracowywanie zmienionych procedur operacyjnych zgodziły się na wprowadzenie zmiany.

(e) wykazanie zgodności systemu z wymogami bezpieczeństwa [część 3]:

Do systemu zarządzania bezpieczeństwem przedsiębiorstwa kolejowego wprowadzone zostały zmienione procedury operacyjne. Poza tym, że były one monitorowane, zastosowano proces przeglądu, aby zapewnić właściwe kontrolowanie zidentyfikowanych zagrożeń w trakcie eksploatacji systemu kolejowego.

(f) zarządzanie zagrożeniami [część 4.1]:

European Railway Agency ● Marc LEFRANCQ, 120 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

Zobacz punkt powyżej, ponieważ w odniesieniu do przedsiębiorstw kolejowych proces zarządzania zagrożeniami może być częścią systemu zarządzania bezpieczeństwem w zakresie rejestrowania różnych rodzajów ryzyka i zarządzania nimi. Zidentyfikowane zagrożenia zarejestrowano w rejestrze zagrożeń wraz z wymogami bezpieczeństwa (tj. odniesieniami do zmienionych procedur operacyjnych) ograniczającymi powiązane ryzyko.
Zmienione procedury były monitorowane i, w miarę potrzeby, poddawane przeglądowi, aby zapewnić właściwy nadzór zidentyfikowanych zagrożeń w trakcie eksploatacji systemu kolejowego.

(g) niezależna ocena [Artykuł 6]:

Ocena ryzyka i proces zarządzania ryzykiem zostały ocenione przez kompetentną osobę z przedsiębiorstwa kolejowego, która była obiektywna w stosunku do procesu oceny. Ta kompetentna osoba oceniła zarówno proces, jak i jego rezultaty, tj. wskazane wymogi bezpieczeństwa.

Przedsiębiorstwo kolejowe podjęło decyzję o wprowadzeniu nowego systemu w życie w oparciu o sprawozdanie z niezależnej oceny przygotowane przez kompetentną osobę.

C.6.4. Przykład pokazuje, że zasady i proces stosowane przez przedsiębiorstwo kolejowe są zgodne ze wspólną metodą oceny bezpieczeństwa. Zarządzanie ryzykiem i proces oceny ryzyka spełniały wszystkie wymogi w zakresie CSM.

C.7. Przykład oceny ryzyka znaczącej zmiany technicznej (CCS)

C.7.1. **C.5.1.** Uwaga: ten przykład oceny ryzyka nie jest wynikiem zastosowania procesu CSM; został przygotowany przed powstaniem CSM. Przykład ten ma na celu:

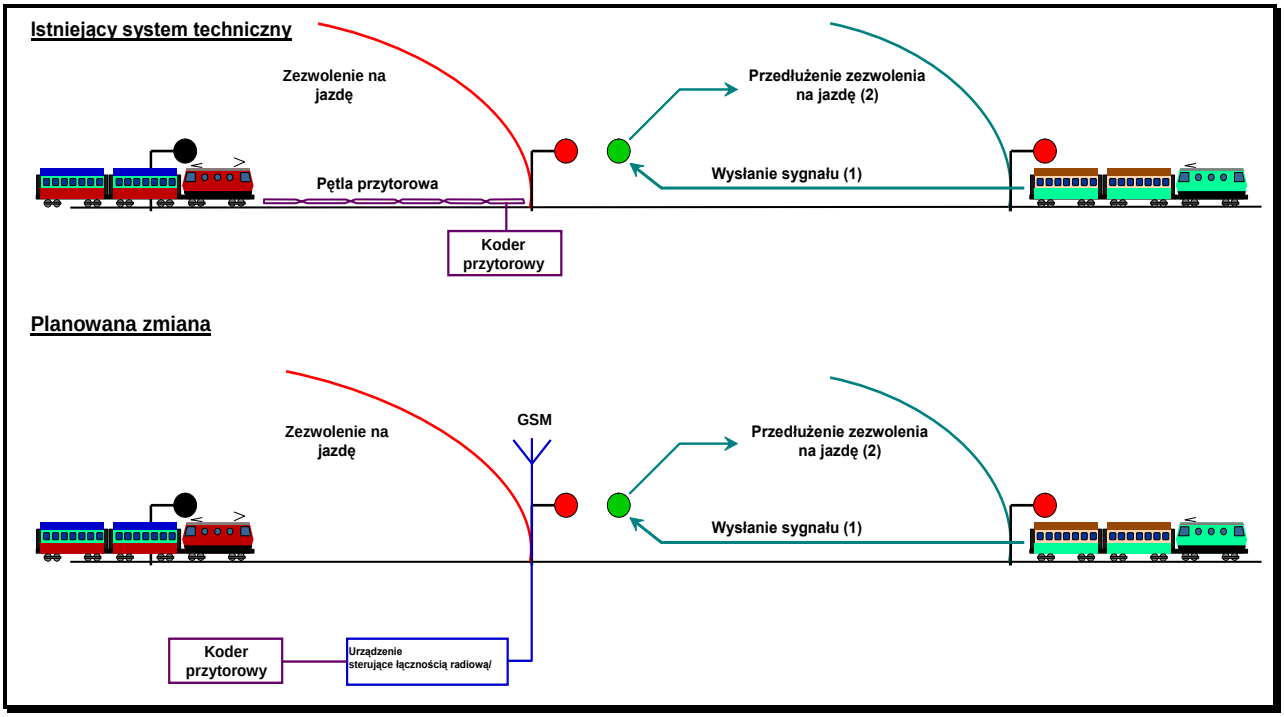
(a) wskazanie podobieństw pomiędzy istniejącymi metodami oceny ryzyka i procesem CSM;
(b) umożliwienie prześledzenia powiązań pomiędzy istniejącym procesem i procesem wymaganym przez CSM;
(c) uzasadnienie wartości dodanej wynikającej z przeprowadzenia (w razie potrzeby) dodatkowych etapów, wymaganych przez CSM.

Należy zaznaczyć, że ten przykład zamieszczono wyłącznie w celach informacyjnych. Ma on ułatwić czytelnikowi zrozumienie procesu CSM. Samego przykładu nie można jednak przetransponować do systemu odniesienia lub wykorzystać jako systemu odniesienia dla innej znaczącej zmiany. Ocena ryzyka jest dokonywana w odniesieniu do każdej istotnej zmiany zgodnie z rozporządzeniem CSM.C.7.2. Ten przykład dotyczy technicznej zmiany systemu sterowania ruchem kolejowym. Producent uznał tę zmianę za znaczącą. W celu oceny zmiany zastosowano podejście oparte na ocenie ryzyka.

C.7.3. Opis zmiany: zmiana polega na zastąpieniu pętli przytorowej położonej przed sygnałem podsystemem „łączność radiowa + GSM” (zob. Schemat 16).

C.7.4. Obawa: utrzymanie poziomu bezpieczeństwa systemu po zmianie.

European Railway Agency ● Marc LEFRANCQ, 120 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu



Schemat 16: Zastąpienie pętli przytorowej podsystemem łączności radiowej.

C.7.5. W porównaniu do procesu CSM stosuje się następujące etapy (zob. również Schemat 1):

(a) ocena znaczenia zmiany [Artykuł 4]

Stosowane są kryteria z Artykuł 4 ust. 2 w celu oceny znaczenia zmiany. Zastosowano głównie aspekty złożoności i innowacyjności, aby ocenić, czy zmiana jest znacząca.

(b) opis systemu [część 2.1.2]:

(1) opis istniejącego systemu: pętla i jej funkcje w systemie sterowania ruchem kolejowym;
(2) opis zmiany planowanej przez wnioskodawcę i producenta;
(3) opis funkcjonalnych i fizycznych interfejsów pętli z pozostałą częścią systemu;

Zadaniem elementu „pętla+koder” w istniejącym systemie jest wysyłanie sygnału w przypadku zbliżania się pociągu, gdy część torów za sygnałem (czyli przed nadjeżdżającym pociągiem) zostaje zwolniona: zob. Schemat 16.

(c) identyfikacja zagrożeń [część 2.2]:

Stosowany jest iteracyjny proces oceny ryzyka i identyfikacji zagrożeń (zob. część 2.1.1) polegający na burzy mózgów z udziałem grupy ekspertów w celu:

(1) zidentyfikowania zagrożeń, które mają istotny wpływ na ryzyko spowodowane planowaną zmianą;
(2) wskazania możliwych działań służących nadzorowaniu ryzyka.

W związku z tym, że pętla wysyła sygnał, a tym samym jest on wysyłany poprzez łączność radiową, istnieje ryzyko wydania zezwolenia na przejazd nadjeżdżającego pociągu w sytuacji niebezpiecznej, gdy poprzedni pociąg ciągle jeszcze zajmuje część torów znajdującą się przed sygnałem. Ryzyko takie należy nadzorować i utrzymywać na dopuszczalnym poziomie.

European Railway Agency ● Marc LEFRANCQ, 120 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

(d) wykorzystanie systemu odniesienia [część 2.4]:

Oceniono, że system sprzed zmiany (pętla) posiadał dopuszczalny poziom bezpieczeństwa. Użyto go zatem jako „systemu odniesienia" w celu ustalenia wymogów bezpieczeństwa dla podsystemu łączności radiowej.

(e) jawne szacowanie i wycena ryzyka [część 2.5]:

(1) różnice pomiędzy podsystemami „pętla" oraz „łączność radiowa+GSM" są analizowane poprzez jawne szacowanie i wycenę ryzyka. Zidentyfikowano następujące nowe zagrożenia dla podsystemu „łączność radiowa+GSM":

(i) bezprzewodowa transmisja niebezpiecznych informacji przez hakerów, ponieważ „łączność radiowa+GSM" jest otwartym podsystemem transmisji;
(ii) opóźniona transmisja lub bezprzewodowa transmisja zapamiętanych pakietów danych;

(2) jednoznaczne oszacowanie ryzyka i zastosowanie RAC-TS w odniesieniu do urządzenia sterującego łącznością radiową;

(f) wykorzystanie kodeksów postępowania [część 2.3]:

(1) norma EN 50159-2 („*Zastosowania kolejowe. Część 2: Łączność systemów bezpieczeństwa w układach otwartych*") zapewnia wymogi bezpieczeństwa w celu kontrolowania nowych zagrożeń i utrzymywania ich na dopuszczalnym poziomie, np.:

(i) kodowanie i ochrona danych;
(ii) określanie porządku dostarczania wiadomości i wprowadzanie znaczników czasowych;

(2) zastosowanie na przykład normy EN 50 128 do opracowania oprogramowania urządzenia sterującego łącznością radiową;

(g) wykazanie zgodności systemu z wymogami bezpieczeństwa [część 3]:

(1) uzupełnienie wdrożenia wymogów bezpieczeństwa poprzez proces opracowywania podsystemu „łączność radiowa+GSM";
(2) sprawdzenie, czy system, w takiej postaci, w jakiej został zaprojektowany i zainstalowany, jest zgodny z wymogami bezpieczeństwa;

(h) zarządzanie zagrożeniami [część 4.1]:

Zidentyfikowane zagrożenia, środki bezpieczeństwa i wymogi bezpieczeństwa wynikające z oceny ryzyka i zastosowania trzech zasad akceptacji ryzyka zamieszcza się w rejestrze zagrożeń i zarządza nimi.

(i) niezależna ocena [Artykuł 6]:

Niezależna ocena przez osobę trzecią jest również przeprowadzana w celu:

(1) sprawdzenia, czy zarządzanie ryzykiem i ocena ryzyka są prawidłowo przeprowadzane;
(2) sprawdzenia, czy zmiana techniczna jest odpowiednia i pozwoli utrzymać poziom bezpieczeństwa sprzed zmiany.

C.7.6. Ten przykład pokazuje, że jako uzupełnienie w celu zdefiniowania wymogów bezpieczeństwa dla systemu objętego oceną stosowane są trzy zasady akceptacji ryzyka wymagane przez wspólną metodę oceny bezpieczeństwa. Ocena ryzyka zastosowana w przykładzie spełnia wszystkie wymogi CSM podsumowane na Schemat 1, w tym wymóg zarządzania rejestrem zagrożeń i niezależnej oceny bezpieczeństwa przez osobę trzecią.

European Railway Agency ● Marc LEFRANCQ, 120 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

C.8. Przykład szwedzkich wytycznych BVH 585.30 dotyczących oceny ryzyka tuneli kolejowych

C.8.1. **C.5.1.** Uwaga: ten przykład oceny ryzyka nie jest wynikiem zastosowania procesu CSM; został przygotowany przed powstaniem CSM. Przykład ten ma na celu:

(a) wskazanie podobieństw pomiędzy istniejącymi metodami oceny ryzyka i procesem CSM;
(b) umożliwienie prześledzenia powiązań pomiędzy istniejącym procesem i procesem wymaganym przez CSM;
(c) uzasadnienie wartości dodanej wynikającej z przeprowadzenia (w razie potrzeby) dodatkowych etapów, wymaganych przez CSM.

Należy zaznaczyć, że ten przykład zamieszczono wyłącznie w celach informacyjnych. Ma on ułatwić czytelnikowi zrozumienie procesu CSM. Samego przykładu nie można jednak przetransponować do systemu odniesienia lub wykorzystać jako systemu odniesienia dla innej znaczącej zmiany. Ocena ryzyka jest dokonywana w odniesieniu do każdej istotnej zmiany zgodnie z rozporządzeniem CSM.

C.8.2. Niniejszy przykład ma na celu porównanie procesu w CSM z wytycznymi BVH 585.30 stosowanymi przez szwedzkiego zarządcę infrastruktury Banverket w celu projektowania nowych tuneli kolejowych i sprawdzania, czy osiągnięto wystarczający poziom bezpieczeństwa podczas planowania i budowy nowych tuneli kolejowych. Poniżej wymienione zostały punkty wspólne i różnice z CSM; szczegółowe wymogi oceny ryzyka można znaleźć w wytycznych BVH 585.30.

C.8.3. W porównaniu do procesu CSM w Schemat 1:

(a) wytyczne BVH 585.30 wykazują następujące punkty wspólne:

(1) opis systemu [część 2.1.2]:

Zgodnie z wytycznymi należy sporządzić szczegółowy opis systemu, zawierający:

(i) opis tunelu;
(ii) opis torów;
(iii) opis rodzaju taboru kolejowego (w tym personelu obsługującego);
(iv) opis ruchu i planowanej eksploatacji;
(v) opis pomocy zewnętrznej (w tym służb ratowniczych);

(2) identyfikacja zagrożeń [część 2.2]:

Wytyczne nie zawierają wyraźnego wymogu identyfikacji zagrożeń, zawierają natomiast wymóg identyfikacji ryzyka i sporządzenia „katalogu wypadków", zawierającego rodzaje zidentyfikowanych, potencjalnych wypadków, które mogą mieć znaczący wpływ na poziom ryzyka w tunelu i które następnie należy poddać ocenie. Przykłady wypadków:

(i) „wykolejenie pociągu pasażerskiego";
(ii) „wykolejenie pociągu towarowego";
(iii) „wypadki z udziałem towarów niebezpiecznych";
(iv) „pożar pojazdu";
(v) „kolizja pociągu pasażerskiego z lekkim/ciężkim obiektem";
(vi) itp.

(3) Nie przewidziano zastosowania kodeksów postępowania lub podobnych systemów odniesienia. Uznano, że analizę ryzyka należy przeprowadzić w każdym przypadku;

(4) jawne szacowanie i wycena ryzyka [część 2.5]:

European Railway Agency ● Marc LEFRANCQ, 120 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

(i) zasadniczo w wytycznych zaleca się wykonanie dla każdego rodzaju wypadku pełnej analizy drzewa zdarzeń w oparciu o ilościową analizę ryzyka. Ponieważ jednak analiza ryzyka ma na celu przeanalizowanie ogólnego poziomu bezpieczeństwa tunelu, a nie bezpieczeństwa na poszczególnych bardziej szczegółowych poziomach, konsekwencje wszystkich scenariuszy są sumowane, aby uzyskać ogólny poziom ryzyka dla tunelu;

(ii) dopuszczalność tego ogólnego poziomu ryzyka dla tunelu jest następnie porównywana z następującym jednoznacznym i ilościowym kryterium akceptacji ryzyka *„ruch kolejowego na kilometr tunelu powinien być tak bezpieczny, jak ruch kolejowy na kilometr torów na otwartym powietrzu, z wyjątkiem przejazdów kolejowych".* Kryterium to przedstawiono w postaci krzywej F-N w oparciu o dane historyczne dotyczące wypadków drogowych w Szwecji i na jego podstawie przewidziano także skutki, których nie uwzględniały dane statystyczne;

(iii) oprócz kryterium ogólnego poziomu ryzyka w tunelu, wytyczne zawierają również dodatkowe wymogi, które muszą być spełnione, przede wszystkim w przypadku ewakuacji w tunelach i możliwości działania służb ratowniczych:

- należy sprawdzić, czy możliwe jest samo ratowanie w przypadku pożaru w pociągu według „najgorszego możliwego scenariusza" (podane są również kryteria takiej oceny);
- tunel należy zaprojektować w taki sposób, aby umożliwiał przeprowadzenie akcji ratowniczej w przypadku określonych scenariuszy;

(5) wyniki oceny ryzyka [część 2.1.6]:

Wyniki oceny ryzyka są następujące:

(i) lista środków bezpieczeństwa wynikających z minimalnej normy w oparciu o TSI-SRT oraz przepisy krajowe, które należy stosować przy projektowaniu tunelu, oraz;

(ii) wszystkie dodatkowe środki bezpieczeństwa, wskazane jako konieczne w procesie analizy ryzyka, określającej ich cel. Stwierdzono, że decyzję o wyborze środków należy podejmować, stosując następującą hierarchię priorytetów:

- zapobieganie wypadkom;
- ograniczenie skutków wypadków;
- ułatwienie ewakuacji;
- ułatwienie akcji ratowniczej;

(6) zarządzanie zagrożeniami [część 4.1]:

Wytyczne nie zawierają wyraźnego wymogu prowadzenia rejestru zagrożeń. Wynika to z faktu, że ocena jest przeprowadzana na poziomie ogólnym, w związku z czym zagrożenia nie są oddzielnie oceniane ani kontrolowane. Oceniana jest dopuszczalność ogólnego ryzyka związanego z tunelem, bez jakiegokolwiek dalszego podziału kryterium dopuszczalności ogólnego ryzyka na różne rodzaje wypadków czy zagrożeń.

Wytyczne zawierają jednak listę wszystkich środków bezpieczeństwa, zarówno tych wynikających z „minimalnej normy", jak i tych wskazanych w procesie analizy ryzyka: zob. punkt (a)(5)(ii) powyżej. Na liście środków bezpieczeństwa powinno znajdować się oznaczenie, czy środki te dotyczą infrastruktury tunelu, torów, eksploatacji czy taboru oraz jakie są oczekiwane skutki tych środków, zgodnie z ponumerowaną listą w punkcie (a)(5)(ii). Niemniej wytyczne nie zawierają wymogu jednoznacznego określenia, jakie zagrożenia kontrolują dane środki bezpieczeństwa, ani kto jest odpowiedzialny za jakie środki.

European Railway Agency ● Marc LEFRANCQ, 120 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

(7) niezależna ocena [Artykuł 6]:

Obowiązkowe jest przeprowadzenie niezależnej oceny przez osobę trzecią w celu:

(i) sprawdzenia, czy proces oceny ryzyka zalecany w wytycznych BVH 585.30 jest przeprowadzany prawidłowo;
(ii) rozważenia, czy analiza ryzyka jest do przyjęcia;
(iii) sprawdzenia, czy wyraźnie określono, w jaki sposób powinno być przeprowadzane zarządzanie bezpieczeństwem w zakresie inwestycji w przyszłości;

Dokument zawierający ostateczną analizę ryzyka jest podpisywany przez niezależny organ oceniający, a także przez koordynatora ds. bezpieczeństwa inwestycji.

(b) wytyczne BVH 585.30 różnią się w następujących aspektach:

(1) wykazanie zgodności systemu z wymogami bezpieczeństwa [część 3]:

Wytyczne BVH 585.30 nie zawierają wymogu sprawdzenia, w jaki sposób wskazane środki bezpieczeństwa są wdrażane, ani sprawdzenia, czy ostateczny projekt tunelu spełnia wymienione wymogi bezpieczeństwa. Wytyczne opisują jedynie, w jaki sposób należy przenieść te wymogi, aby zapewnić ich wdrożenie na etapie budowy.

Wytyczne zapewniają wymogi bezpieczeństwa, które należy stosować w celu sprawdzenia, czy analiza ryzyka została wykonana we właściwy i przejrzysty sposób i czy może być zaakceptowana z punktu widzenia inwestycji.

C.8.4. Podsumowując, z porównania z CSM wynika, że:

(a) wytyczne BVH 585.30 spełniają wymogi stosownych części CSM, mimo że ich zakres i cel niezupełnie pokrywają się z zakresem i celem CSM;

(b) wytyczne BVH 585.30 oceniają ogólny poziom ryzyka w tunelu kolejowym;

(c) zagrożenia nie są oddzielnie nadzorowane i w związku z tym mniej uwagi poświęca się zarządzaniu zagrożeniami;

(d) wymóg wykazania zgodności i sprawdzenia poprawności zastosowania wszystkich środków bezpieczeństwa nie jest wyraźnie określony. Niemniej wytyczne zawierają stwierdzenie, że rolą koordynatora ds. bezpieczeństwa w ramach inwestycji (rola i kompetencje wymagane przez BVH 585.30) jest sprawdzanie, czy wnioski z analizy ryzyka są uwzględniane w dokumentach projektowych i na rysunkach, a także nadzorowanie, czy są one prawidłowo wdrażane na etapie budowy;

C.8.5. CSM są bardziej ogólne niż wytyczne BVH 585.30, ponieważ umożliwiają zastosowanie trzech różnych zasad akceptacji ryzyka. Niemniej zastosowanie wytycznych BVH 585.30 w ramach CSM nie stanowi żadnego problemu, ponieważ jest zgodne z wykorzystaniem trzeciej zasady jawnego szacowania ryzyka.

C.9. Przykład oceny ryzyka na poziomie systemu w odniesieniu do metra w Kopenhadze

C.9.1. **C.5.1.** Uwaga: ten przykład oceny ryzyka nie jest wynikiem zastosowania procesu CSM; został przygotowany przed powstaniem CSM. Przykład ten ma na celu:

(a) wskazanie podobieństw pomiędzy istniejącymi metodami oceny ryzyka i procesem CSM;

European Railway Agency ● Marc LEFRANCQ, 120 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

(b) umożliwienie prześledzenia powiązań pomiędzy istniejącym procesem i procesem wymaganym przez CSM;
(c) uzasadnienie wartości dodanej wynikającej z przeprowadzenia (w razie potrzeby) dodatkowych etapów, wymaganych przez CSM.

Należy zaznaczyć, że ten przykład zamieszczono wyłącznie w celach informacyjnych. Ma on ułatwić czytelnikowi zrozumienie procesu CSM. Samego przykładu nie można jednak przetransponować do systemu odniesienia lub wykorzystać jako systemu odniesienia dla innej znaczącej zmiany. Ocena ryzyka jest dokonywana w odniesieniu do każdej istotnej zmiany zgodnie z rozporządzeniem CSM.

C.9.2. Ten przykład dotyczy w pełni zautomatyzowanego i skomplikowanego systemu metra, w skład którego wchodzą techniczne podsystemy (np. automatyczna ochrona pociągu i tabor kolejowy), jak również eksploatacja i utrzymanie ruchu. Zastosowano podejście oparte na ocenie ryzyka, aby ocenić system i jego podsystemy. Projekt obejmował również certyfikację systemu zarządzania bezpieczeństwem spółki, która obsługiwała ten system. Odnosi się to do zdolności przedsiębiorstwa kolejowego i zarządcy infrastruktury do bezpiecznego eksploatowania i utrzymywania ruchu całego systemu w całym cyklu życia.

C.9.3. W porównaniu do procesu CSM zastosowano następujące etapy (zob. również Schemat 1):

(a) opis systemu [część 2.1.2]:

(1) opis wymogów dotyczących eksploatacji systemu;
(2) opis zasad eksploatacyjnych;
(3) jasny opis interfejsów pomiędzy różnymi podmiotami, przede wszystkim pomiędzy podsystemami technicznymi oraz obowiązków tych podmiotów;
(4) definicja wysokich wymogów dotyczących systemu (pod względem dopuszczalnej częstotliwości wypadków i definicji obszarów ALARP);

(b) identyfikacja zagrożeń [część 2.2]:

(1) wstępna analiza zagrożeń na poziomie systemu;
(2) funkcjonalna analiza na poziomie systemu, ze szczególnym uwzględnieniem wszystkich podsystemów, a nie tylko niewątpliwie najbardziej istotnych ze względów bezpieczeństwa (np. automatyczna ochrona pociągu i tabor kolejowy), które mają swój udział w funkcjach bezpieczeństwa i odgrywają aktywną rolę w zapewnianiu bezpieczeństwa pasażerów i personelu;
(3) ścisła współpraca pomiędzy podmiotami (wykonawcami, dostawcami podsystemów technicznych i wykonawcami obiektów budowlanych):

(i) w celu regularnego identyfikowania wszystkich możliwych do przewidzenia zagrożeń;
(ii) w celu wskazania możliwych działań, służących kontrolowaniu ryzyka powiązanego ze zidentyfikowanymi zagrożeniami i utrzymywaniu go na dopuszczalnym poziomie;

(c) wykorzystanie kodeksów postępowania [część 2.3]:

Zastosowano różne kodeksy postępowania, standardy i przepisy, np.:

(1) normy BOStrab dotyczące budowy i eksploatacji tramwajów (niemieckie przepisy dotyczące miejskich systemów kolei) oraz obsługi zautomatyzowanej;
(2) dokumenty organizacji VDV (niemieckie kodeksy postępowania) związane z wymogami dotyczącymi sprzętu służącego do zapewnienia bezpieczeństwa pasażerów na stacjach obsługiwanych automatycznie;
(3) normy CENELEC dotyczące systemów kolejowych (EN 50 126, 50 128 i 50 129). Normy te dotyczą przede wszystkim technicznych aspektów systemów kolejowych. Jednak w związku z tym, że zawierają również podejście metodologiczne, które

European Railway Agency ● Marc LEFRANCQ, 120 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

powszechnie obowiązuje, zostały w dużej mierze wykorzystane w odniesieniu do metra w Kopenhadze:

(i) normę EN 50 126 zastosowano w odniesieniu do czynności w zakresie zarządzania bezpieczeństwem i oceny ryzyka całego systemu kolejowego;
(ii) normę EN 50 129 zastosowano w odniesieniu do całego systemu sygnalizacji;
(iii) normę EN 50 128 zastosowano do opracowania oprogramowania (w tym do weryfikacji i walidacji) podsystemów technicznych;

(4) normy ochrony przeciwpożarowej dla tuneli (NEPA 130);
(5) normy dotyczące inżynierii lądowej i obiektów budowlanych (Eurokody);

(d) wykorzystanie systemu odniesienia [część 2.4]:

Metro musiało osiągnąć taki poziom bezpieczeństwa, jak podobne nowoczesne instalacje w Niemczech, Francji lub Wielkiej Brytanii. Te istniejące systemy były wykorzystywane jako podobne systemy odniesienia w celu określenia kryteriów akceptacji ryzyka pod względem dopuszczalnej częstotliwości wypadków dla metra w Kopenhadze;

(e) jawne szacowanie i wycena ryzyka [część 2.5]:

(1) w celu oszacowania ryzyka związanego z określonymi zagrożeniami;
(2) w celu kontroli wentylacji tunelu awaryjnego (w tym czynniki ludzkie, np. straż pożarna);
(3) w celu wskazania środków ograniczenia ryzyka;
(4) w celu oszacowania, czy dopuszczalny poziom ryzyka został osiągnięty dla całego systemu;

(f) wykazanie zgodności systemu z wymogami bezpieczeństwa [część 3]:

(1) działania na szczeblu kierowniczym i technicznym uwzględniające złożoność systemu w celu wykazania bezpieczeństwa systemu;
(2) podział wymogów w zakresie bezpieczeństwa systemu na podsystemy techniczne i obiekty budowlane, jak również na wszystkie funkcje metra związane z bezpieczeństwem;
(3) wykazanie, że każdy podsystem spełnia, zgodnie z jego konstrukcją, wymogi bezpieczeństwa;
(4) w odniesieniu do funkcji bezpieczeństwa spełnianych przez więcej podsystemów niż jeden, nie można było zakończyć wykazania zgodności z wymogami bezpieczeństwa na poziomie podsystemu. Wykazano to na poziomie systemu poprzez zintegrowanie różnych podsystemów, narzędzi i procedur;
(5) wykazanie, że cały system jest zgodny z wysokimi wymogami w zakresie bezpieczeństwa;

(g) zarządzanie zagrożeniami [część 4.1]:

Zidentyfikowane zagrożenia, powiązane środki bezpieczeństwa i wynikające wymogi w zakresie bezpieczeństwa były zamieszczane w centralnym rejestrze zagrożeń i monitorowane. Za rejestr zagrożeń odpowiadał kierownik ds. ogólnego bezpieczeństwa inwestycji. Zagrożenia eksploatacyjne powstałe w fazie projektu i instalacji, jak również zagrożenia związane z eksploatacją i utrzymaniem, zostały uwzględnione w rejestrze zagrożeń;

(h) dowody z zarządzania ryzykiem i oceny ryzyka [część 5]:

Wyniki oceny ryzyka zostały formalnie udokumentowane i potwierdzone poprzez dowód bezpieczeństwa zgodnie z wymogami norm CENELEC:

(1) dowód bezpieczeństwa całego systemu;

European Railway Agency ● Marc LEFRANCQ, 120 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

(2) dowód bezpieczeństwa dla każdego podsystemu technicznego (w tym podsystemów sygnalizacyjnych i obiektów budowlanych);
(3) dowód bezpieczeństwa dla obiektów budowlanych (stacje, tunele, wiadukty, nasypy);
(4) dowód bezpieczeństwa instalacji;
(5) dowód bezpieczeństwa pojazdów;
(6) dowód bezpieczeństwa operatora (potwierdzający certyfikację systemu zarządzania bezpieczeństwem przedsiębiorstwa kolejowego i zarządcy infrastruktury, tj. wykazanie zdolności wnioskodawcy do bezpiecznej eksploatacji i utrzymania systemu);

(i) niezależna ocena [Artykuł 6]:

Cały proces został prześledzony i oceniony przez niezależny organ ds. oceny bezpieczeństwa, działający z upoważnienia organu nadzoru technicznego (tj. duńskiego ministerstwa transportu). Zadania niezależnego organu ds. oceny bezpieczeństwa są podane w odpowiednim kodeksie postępowania. Obejmowały one:

(1) sprawdzenie poprawności zarządzania ryzykiem i oceny ryzyka;
(2) sprawdzenie, czy system odpowiada zamierzonemu celowi i czy jego eksploatacja i utrzymanie będzie bezpieczne w całym cyklu życia systemu;
(3) zalecenie, aby organ nadzoru technicznego wydał zgodę.

C.9.4. Cała inwestycja była oparta na odpowiednim procesie zarządzania jakością.

C.9.5. W trakcie inwestycji dostawcy przedłożyli dowody (tj. dowody bezpieczeństwa i szczegółową dokumentację dotyczącą podsystemów technicznych i obiektów budowlanych) kierownikowi ds. bezpieczeństwa wnioskodawcy. Dowody te zostały następnie przeanalizowane przez organizację ds. zarządzania bezpieczeństwem, jak również przez niezależną jednostkę ds. oceny bezpieczeństwa, których wnioski znalazły się w sprawozdaniu z oceny.
Sprawozdanie z niezależnej oceny bezpieczeństwa zostało przeanalizowane przez zarząd ds. bezpieczeństwa wnioskodawcy i przedłożone wnioskodawcy, który przekazał wszystkie dokumenty organowi nadzoru technicznego (tj. duńskiemu ministerstwu transportu) do ostatecznego zatwierdzenia.

C.9.6. Przykład pokazuje, że zasady wymagane przez wspólną metodę oceny bezpieczeństwa już istnieją w sektorze kolejowym. Ocena ryzyka zastosowana w przykładzie spełnia wszystkie wymogi z CSM. Przede wszystkim zastosowano w niej wszystkie trzy zasady akceptacji ryzyka, dopuszczone w zharmonizowanym podejściu w zakresie CSM.

C.10. Przykład wytycznych Międzyrządowej Organizacji Międzynarodowych Przewozów Kolejami (OTIF) dotyczących szacowania ryzyka wynikającego z przewozu towarów niebezpiecznych

C.10.1. **C.5.1.** Uwaga: ten przykład oceny ryzyka nie jest wynikiem zastosowania procesu CSM; został przygotowany przed powstaniem CSM. Przykład ten ma na celu:

(a) wskazanie podobieństw pomiędzy istniejącymi metodami oceny ryzyka i procesem CSM;
(b) umożliwienie prześledzenia powiązań pomiędzy istniejącym procesem i procesem wymaganym przez CSM;

European Railway Agency ● Marc LEFRANCQ, 120 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

(c) uzasadnienie wartości dodanej wynikającej z przeprowadzenia (w razie potrzeby) dodatkowych etapów, wymaganych przez CSM.

Należy zaznaczyć, że ten przykład zamieszczono wyłącznie w celach informacyjnych. Ma on ułatwić czytelnikowi zrozumienie procesu CSM. Samego przykładu nie można jednak przetransponować do systemu odniesienia lub wykorzystać jako systemu odniesienia dla innej znaczącej zmiany. Ocena ryzyka jest dokonywana w odniesieniu do każdej istotnej zmiany zgodnie z rozporządzeniem CSM.

C.10.2. Ogólne założenia wytycznych OTIF zgodne są z celem CSM, ale same wytyczne mają ograniczony zakres. Wytyczne OTIF mają na celu „*uzyskanie bardziej ujednoliconego podejścia do oceny ryzyka w przewozach towarów niebezpiecznych w państwach członkowskich COTIF i w tym samym sprawdzenie, czy pojedyncze oceny ryzyka będą porównywalne*.” W ten sposób wspiera się również wśród państw członkowskich COTIF wzajemne uznawanie oceny ryzyka, w odniesieniu do przewozu kolejami towarów niebezpiecznych.

C.10.3. W porównaniu z CSM i diagramem sekwencji działań na Schemat 1:

(a) Wytyczne OTIF mają następujące punkty wspólne:

(1) wspólne podejście do oceny ryzyka, niemniej jednak oparte tylko na jawnym oszacowaniu ryzyka (tj. trzecia zasada CSM akceptacji ryzyka);
(2) Na ocenę ryzyka OTIF składa się:
(i) faza analizy ryzyka, która obejmuje
- fazę identyfikacji zagrożenia;
- fazę szacowania ryzyka;

(ii) faza wyceny ryzyka oparta na kryteriach (akceptacji) ryzyka, które nie są jeszcze zharmonizowane. W istocie na te kryteria może mieć wpływ wiele specyficznych krajowych aspektów;

(b) Wytyczne OTIF różnią się pod następującymi względami:

(1) zakres stosowania jest inny. CSM stosuje się tylko w przypadku istotnej zmiany systemu kolejowego. Natomiast wytyczne OTIF powinno się stosować do oceny ryzyka w odniesieniu do przewozu kolejami towarów niebezpiecznych, bez względu na to, czy ma to charakter znaczącej zmiany sytemu, czy nie;
(2) nie ma możliwości wyboru pomiędzy trzema zasadami akceptacji ryzyka dotyczącymi kontrolowania ryzyka. Trzecia zasada, tj. jednoznaczne oszacowanie ryzyka, jest jedyną zasadą dopuszczalną w tej sytuacji. Ponadto musi być ona oparta jedynie na oszacowaniu ilościowym, a nie jakościowym. Analiza ryzyka pod względem jakościowym może być odpowiednia jedynie w przypadku porównywania możliwych do zastosowania środków (bezpieczeństwa) w celu zmniejszenia ryzyka;
(3) zaleca się stosowanie zasady ALARP w celu określenia, czy dodatkowe środki bezpieczeństwa mogłyby doprowadzić do dalszego zmniejszenia ocenionego ryzyka za rozsądną cenę;
(4) nie ma pojęcia „zagrożenia powiązane z ogólnie dopuszczalnym ryzykiem”, które pozwala skoncentrować się w ramach oceny ryzyka na zagrożeniach powodujących największe ryzyko. Niemniej jednak zaleca się zmniejszenie liczby scenariuszy potencjalnych wypadków do rozsądnej liczby podstawowych scenariuszy (zob. część 3.2 w {Ref. 10});
(5) proces skupia się na ocenie ryzyka, ale nie obejmuje:

(i) procesu wyboru i wdrożenia środków (bezpieczeństwa) w celu modyfikacji ryzyka;
(ii) procesu akceptacji ryzyka;
(iii) procesu wykazywania zgodności systemu z wymogami bezpieczeństwa;

European Railway Agency ● Marc LEFRANCQ, 120 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

(iv) procesu powiadamiania o ryzyku innych zainteresowanych podmiotów (zob. punkt poniżej);

(6) nie daje wskazówek co do danych, które powinien dostarczyć proces oceny ryzyka;
(7) nie wymaga się zarządzania zagrożeniami;
(8) nie wymaga się dokonania niezależnej oceny właściwego stosowania wspólnego podejścia przez osoby trzecie.

C.10.4. Porównanie wytycznych OTIF z CSM pokazuje, że są one ze sobą zgodne, mimo że ich zakres i cel nie jest dokładnie taki sam. CSM jest bardziej ogólne niż wytyczne OTIF, i w tym sensie jest bardziej elastyczne. Z drugiej strony CSM obejmuje również więcej działań z zakresu zarządzania ryzykiem:

(a) pozwala na stosowanie trzech zasad akceptacji ryzyka, które są oparte na praktykach stosowanych na kolei : zob. część 2.1.4;
(b) jej stosowanie jest konieczne tylko w przypadku znaczących zmian, a dalsza analiza ryzyka wymagana jest tylko w przypadku zagrożeń, które są powiązane z ogólnie dopuszczalnym ryzykiem;
(c) obejmuje wybór i wdrożenie środków bezpieczeństwa, które stosuje się w celu nadzorowania zidentyfikowanych zagrożeń i powiązanego ryzyka;
(d) harmonizuje proces zarządzania ryzykiem, obejmujący:

(1) harmonizację kryteriów akceptacji ryzyka, której dokonuje się w ramach pracy Agencji w zakresie ogólnie dopuszczalnego ryzyka i zasad akceptacji ryzyka.
(2) wykazanie zgodności systemu z wymogami bezpieczeństwa**;**
(3) wyniki i dane uzyskane w procesie oceny ryzyka;
(4) wymianę informacji dotyczących bezpieczeństwa w interfejsach między podmiotami;
(5) zarządzanie wszystkimi zidentyfikowanymi zagrożeniami i powiązanymi środkami bezpieczeństwa w wykazie zagrożeń;
(6) niezależną ocenę właściwego stosowania CSM przeprowadzaną przez osoby trzecie.

C.10.5. Stosowanie wytycznych OTIF w ramach CSM (jeżeli przewóz towarów niebezpiecznych stanowi znaczącą zmianę dla zarządcy infrastruktury lub przedsiębiorstwa kolejowego) nie prowadzi do żadnych problemów, jako że są one zgodne z trzecią zasadą jednoznacznego oszacowania ryzyka.

C.11. Przykład oceny ryzyka w przypadku ubiegania się o zatwierdzenie nowego rodzaj taboru

C.11.1. **C.5.1.** Uwaga: ten przykład oceny ryzyka nie jest wynikiem zastosowania procesu CSM; został przygotowany przed powstaniem CSM. Przykład ten ma na celu:

(a) wskazanie podobieństw pomiędzy istniejącymi metodami oceny ryzyka i procesem CSM;
(b) umożliwienie prześledzenia powiązań pomiędzy istniejącym procesem i procesem wymaganym przez CSM;
(c) uzasadnienie wartości dodanej wynikającej z przeprowadzenia (w razie potrzeby) dodatkowych etapów, wymaganych przez CSM.

Należy zaznaczyć, że ten przykład zamieszczono wyłącznie w celach informacyjnych. Ma on ułatwić czytelnikowi zrozumienie procesu CSM. Samego przykładu nie można jednak przetransponować do systemu odniesienia lub wykorzystać jako systemu odniesienia dla innej znaczącej zmiany. Ocena ryzyka jest dokonywana w odniesieniu do każdej istotnej zmiany zgodnie z rozporządzeniem CSM.

European Railway Agency ● Marc LEFRANCQ, 120 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

C.11.2. Ten przykład oceny ryzyka dotyczy przypadku ubiegania się o zatwierdzenie nowego rodzaju taboru. Przeprowadzono analizę ryzyka w celu dokonania wyceny ryzyka związanego z wprowadzeniem nowego wagonu towarowego.

C.11.3. Zmiana miała na celu zwiększenie wydajności, ładowności, osiągów i niezawodności przewozu towarów masowych specjalną linią towarową. Ponieważ wagony były przeznaczone do użytkowania w ruchu transgranicznym, konieczne było również zatwierdzenie przez dwa różne krajowe organy ds. bezpieczeństwa. Wnioskodawcą był przewoźnik, który należał do przedsiębiorstwa wytwarzającego towary przeznaczone do transportu.

C.11.4. Inwestycja obejmowała budowę, produkcję, montaż, oddanie do użytku nowego taboru i weryfikację jego funkcjonowania. Analizę ryzyka przeprowadzono w celu sprawdzenia nowego rozwiązania projektowego pod względem jego zgodności z wymogami bezpieczeństwa każdego podsystemu, jak również dla całego systemu.

C.11.5. Analiza ryzyka nawiązuje do procedur określonych normą CENELEC EN 50126; definicje i wycena ryzyka są zgodne z tą normą.

C.11.6. W porównaniu do procesu CSM zastosowano następujące etapy:

(a) opis systemu [część 2.1.2]:

Każdy etap projektowania charakteryzował się wymogami w zakresie dokumentacji weryfikującej bezpieczeństwo i opisu projektu systemu:

(1) etap koncepcyjny: wstępny opis wymagań eksploatacyjnych przewoźnika;
(2) etap specyfikacji: specyfikacja ruchowa, obowiązujące normy techniczne, plan przeprowadzania testów i weryfikacji. Uwzględniono również wymogi przewoźnika w zakresie eksploatacji i utrzymania wagonu;
(3) etap produkcji: dokumentacja techniczna producenta, w tym rysunki, normy, obliczenia, analizy itp. Szczegółowa analiza ryzyka dla nowych lub innowacyjnych projektów lub nowych form eksploatacji;
(4) etap weryfikacji:
  (i) weryfikacja osiągów technicznych wagonu przez producenta (sprawozdania z przeprowadzonych testów, obliczenia, weryfikacje zgodne z normami i wymogami funkcjonalnym);
  (ii) dokumentacja środków zmniejszających ryzyko i sprawozdania z przeprowadzonych testów w celu wykazania kompatybilności wagonów z infrastrukturą kolejową;
  (iii) dokumenty dotyczące utrzymania taboru i szkoleń, instrukcje użytkownika itp.
(5) etap odbioru:
  (i) deklaracja bezpieczeństwa i dane dotyczące bezpieczeństwa dostarczane przez producenta (dowód bezpieczeństwa);
  (ii) odbiór wagonu towarowego i jego dokumentacji przez przewoźnika;

(b) identyfikacja zagrożeń [część 2.2]:

przeprowadzana była stale na wszystkich etapach prac projektowych. W pierwszej kolejności stosuje się podejście oddolne, które polega na ocenie przez producentów łańcucha ryzyka wynikającego z awarii podzespołów w ramach jednego podsystemu. Podział na podsystemy był następujący:

(1) podwozie;
(2) układ hamulcowy;
(3) sprzęg;

European Railway Agency ● Marc LEFRANCQ, 120 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

(4) itp.

Następnie zastosowano uzupełniające podejście odgórne w celu wyszukania luk lub brakujących informacji. Rodzaje ryzyka, które nie mogły być od razu zaakceptowane, zamieszczono w rejestrze zagrożeń w celu dalszego ich rozpatrzenia i klasyfikacji.

(c) zastosowanie zasad akceptacji ryzyka [część 2.1.4]:

Dokonano jawnego szacowania ryzyka dla całego systemu. Do oceny poszczególnych zagrożeń można jednak stosować kodeksy postępowania lub systemy odniesienia. Zasada polega na tym, że każdy nowy podsystem powinien być co najmniej tak samo bezpieczny jak podsystem, który zastępuje, prowadząc tym samym do uzyskania zupełnie nowego systemu o wyższym stopniu bezpieczeństwa niż poprzedni. Zastosowano matrycę ryzyka zgodną z normą EN50126 w usystematyzowania zidentyfikowanych zagrożeń. Zastosowano również inne dodatkowe kryteria akceptacji ryzyka, między innymi:

(1) pojedyncza awaria nie powinna prowadzić do sytuacji, w której poważnie ucierpią ludzie, materiały lub środowisko;
(2) jeżeli nie można tego uniknąć stosując odpowiednią konstrukcję techniczną, należy temu zapobiec stosując zasady eksploatacyjne lub wymogi utrzymania ruchu. Stosowano to do zagrożeń tylko w przypadku gdy możliwe było zidentyfikowanie powstałej awarii, zanim doprowadziła ona do niebezpiecznej sytuacji;
(3) w przypadku podzespołów o wysokim prawdopodobieństwie wystąpienia awarii lub w przypadku awarii, których nie można wykryć wcześniej, lub którym nie można zapobiec stosując zasady eksploatacyjne, należy uwzględnić dodatkowe funkcje bezpieczeństwa i bariery ochronne;
(4) systemy rezerwowe z podzespołami, które mogą ulegać niewykrywalnym awariom podczas eksploatacji, należy zabezpieczyć środkami utrzymania ruchu, aby zapobiec ograniczeniu funkcji, jaką mają spełniać;
(5) wynikowy końcowy poziom bezpieczeństwa był decyzją opartą na ilościowej i jakościowej analizie ryzyka;

(d) wykazanie zgodności systemu z wymogami bezpieczeństwa [część 3]:

Wszystkie zidentyfikowane rodzaje ryzyka i zagrożenia zamieszczono w rejestrze, który był na bieżąco konsultowany i aktualizowany. Pozostałe zagrożenia zamieszczono w rejestrze zagrożeń razem z odpowiednią listą środków zmniejszających ryzyko, który należy zastosować na etapie konstrukcji, eksploatacji i utrzymania. Na tej podstawie powstał końcowy raport w sprawie oceny bezpieczeństwa potwierdzający, że wymogi bezpieczeństwa zostały wdrożone;

(e) zarządzanie zagrożeniami [część 4.1]:

Zgodnie z powyższym, zagrożenia i powiązane z nimi środki bezpieczeństwa umieszczono w rejetrze zagrożeń, w którym zamieszczane są wszystkie zidentyfikowane zagrożenia i określone środki bezpieczeństwa. W rejestrze nie ujęto natomiast zagrożeń powiązanych z rodzajami ryzyka, które uznano za dopuszczalne bez stosowania środków bezpieczeństwa.

(f) niezależna ocena [Artykuł 6]:

W otrzymanych dokumentach dotyczących znaczącej zmiany nie było żadnej wzmianki na temat niezależnej oceny.

C.11.7. Przykład oceny ryzyka przygotowano na podstawie normy CENELEC EN 50126 i dlatego też jest on zgodny z procesem CSM. Ocena ryzyka zastosowana w przykładzie spełnia wszystkie wymogi z CSM, z wyjątkiem wymogu przeprowadzenia niezależnej oceny, który

European Railway Agency ● Marc LEFRANCQ, 120 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

nie został jednoznacznie określony w otrzymanych dokumentach. Zastosowano i wyraźnie wskazano jednoznaczną zasadę akceptacji ryzyka

C.12. Przykład oceny ryzyka w przypadku istotnej zmiany w eksploatacji – prowadzenia pociągu przez pojedynczego maszynistę

C.12.1. **C.5.1.** Uwaga: ten przykład oceny ryzyka nie jest wynikiem zastosowania procesu CSM; został przygotowany przed powstaniem CSM. Przykład ten ma na celu:

(a) wskazanie podobieństw pomiędzy istniejącymi metodami oceny ryzyka i procesem CSM;
(b) umożliwienie prześledzenia powiązań pomiędzy istniejącym procesem i procesem wymaganym przez CSM;
(c) uzasadnienie wartości dodanej wynikającej z przeprowadzenia (w razie potrzeby) dodatkowych etapów, wymaganych przez CSM.

Należy zaznaczyć, że ten przykład zamieszczono wyłącznie w celach informacyjnych. Ma on ułatwić czytelnikowi zrozumienie procesu CSM. Samego przykładu nie można jednak przetransponować do systemu odniesienia lub wykorzystać jako systemu odniesienia dla innej znaczącej zmiany. Ocena ryzyka jest dokonywana w odniesieniu do każdej istotnej zmiany zgodnie z rozporządzeniem CSM.

C.12.2. Ten przykład dotyczy zmiany w eksploatacji, gdy przedsiębiorstwo kolejowe podjęło decyzję, że pociąg musi być prowadzony przez pojedynczego maszynistę (prowadzenia pociągu przez pojedynczego maszynistę ang. Driver Only Operated (DOO)) na trasie, na której poprzednio maszyniście pomagał dyżurny ruchu .

C.12.3. W porównaniu z procesem CSM zastosowano następujące etapy (zob. również Schemat 1):

(a) znaczenie zmiany [Artykuł 4]:

Przedsiębiorstwo kolejowe dokonało wstępnej oceny ryzyka, która wykazała, że zmiana w eksploatacji jest znacząca. Ponieważ maszynista prowadzi pociąg bez niczyjej pomocy, należy uwzględnić prawdopodobieństwo przytrzaśnięcia pasażera drzwiami lub wypadnięcia na tory (np. jeżeli drzwi otworzą się z niewłaściwej strony).

Porównując tę wstępną ocenę ryzyka z kryteriami określonymi w Artykuł 4 rozporządzenia CSM, zmianę tę można również zaklasyfikowana jako znaczącą na podstawie następujących kryteriów:

(1) znaczenie dla bezpieczeństwa: zmiana związana jest z bezpieczeństwem, ponieważ konieczność zupełnie innego sposobu zarządzania obsługą pociągu mogłaby mieć katastroficzne konsekwencje;
(2) skutki awarii: potencjalny wpływ pracy maszynisty może mieć katastroficzne konsekwencje, jeżeli obsługa nie jest skutecznie kontrolowana;
(3) innowacyjność: prowadzenia pociągu przez pojedynczego maszynistę może wymagać nowych sposobów obsługi pociągów, które należy ocenić pod względem ryzyka;

(b) definicja systemu [część 2.1.2]:

Definicja systemu opisuje:

(1) istniejący system, jasno określa, które zadania zostały wykonane przez maszynistę, a które przez pomagającego mu pracownika obsługi pociągu (lub strażnika)
(2) zmianę obowiązków maszynisty na skutek usunięcia pomagającego mu pracownika obsługi pociągu;

European Railway Agency ● Marc LEFRANCQ, 120 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

(3) wymogi techniczne systemu, które pokrywają zmiany w obsłudze;
(4) istniejące płaszczyzny oddziaływania między pomocniczym personelem obsługi pociągu, maszynistą a personelem przytorowym zarządcy infrastruktury;

W trakcie różnych iteracji definicję systemu zaktualizowano o wymogi bezpieczeństwa wynikające z procesu oceny ryzyka. W ten iteracyjny proces były zaangażowane najważniejsze osoby (w tym maszyniści, przedstawiciele personelu oraz zarządca infrastruktury) w celu zidentyfikowania zagrożeń i zaktualizowania definicji systemu.

(c) identyfikacja zagrożeń [część 2.2]:

Metodą burzy mózgów zidentyfikowano zagrożenia i wskazano możliwe środki bezpieczeństwa podczas narady grupy ekspertów, w której uczestniczyli między inny:

(1) przedstawiciele maszynistów i personelu, ze względu na ich doświadczenie w zakresie obsługi;
(2) przedstawiciele zarządcy infrastruktury, ponieważ zmiana mogła również dotyczyć infrastruktury, na przykład zmiany na stacjach kolejowych (np. zainstalowanie luster/systemu telewizji przemysłowej [CCTV] na peronach);

Zbadano dodatkowe zadania maszynisty w celu zidentyfikowania dających się przewidzieć zagrożeń, które mogą wystąpić na skutek usunięcia pracownika obsługi pociągu. Przy identyfikacji zagrożeń szczególnie zwraca się uwagę, jakie zagrożenia w eksploatacji mogą wystąpić na stacjach, istniejących trasach, na których zapewniano pomoc ze strony personelu obsługi i personelu przytorowego, w tym bezpieczne kierowanie ruchem pociągów, konkretne kwestie związane z maszynistą, taborem (np. kontrola drzwi przy zamykaniu i otwieraniu), wymogi dotyczące utrzymania ruchu itp.

Każdemu ze zidentyfikowanych zagrożeń przypisano określony stopień ryzyka i skutków (wysoki, średni, niski) oraz w stosunku do nich oceniono wpływ proponowanej zmiany (zwiększone, niezmienione, zmniejszone ryzyko).

(d) stosowanie kodeksów postępowania [część 2.3] i podobnych systemów odniesienia [część 2.4]:

Zastosowano oba kodeksy postępowania (tj. pakiet norm prowadzenia pociągu przez pojedynczego maszynistę) i podobne systemy odniesienia w celu określenia wymogów bezpieczeństwa dla zidentyfikowanych zagrożeń. Wymogi bezpieczeństwa obejmowały:

(1) zmienione procedury operacyjne dla maszynistów, których stosowanie wymagane jest w przypadku prowadzenia pociągów bez pomocy ze strony personelu obsługi;
(2) wszelki dodatkowy sprzęt konieczny na pokładzie pociągu lub na torowisku w celu zapewnienia bezpiecznego i rzetelnego kierowania ruchem pociągów;
(3) listę kontrolną w celu zapewnienia odpowiedniej kabiny maszynisty, przy uwzględnieniu interfejsu między systemem kolejowym (na pokładzie pociągu i przy torach) a maszynistą;

Zmieniono niezbędne zasady eksploatacyjne zgodnie z wymogami określonymi w obowiązujących kodeksach postępowania i z odpowiednimi systemami odniesienia. Wszystkie niezbędne strony były zaangażowane w opracowywanie zmienionych procedur operacyjnych i zgodę na kontynuowaniu zmiany.

(e) wykazanie zgodności systemu z wymogami bezpieczeństwa [część 3]:

System wdrożono zgodnie z określonymi wymogami bezpieczeństwa (dodatkowym sprzętem i zmienionymi procedurami), zweryfikowanymi jako właściwe środki zapewniające wystarczający poziom bezpieczeństwa systemu objętego oceną.

Zmienione procedury obsługi wprowadzono do systemu zarządzania bezpieczeństwem przedsiębiorstwa kolejowego. Były one monitorowane i w razie potrzeby weryfikowane,

European Railway Agency ● Marc LEFRANCQ, 120 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

aby zapewnić właściwy nadzór nad zidentyfikowanymi zagrożeniami w trakcie eksploatacji systemu kolejowego.

(f) zarządzanie zagrożeniami [część 4.1]:

Zobacz punkt wyżej, ponieważ w przypadku przedsiębiorstw kolejowych proces zarządzania zagrożeniami może stanowić część ich systemu zarządzania bezpieczeństwem, jeżeli chodzi o odnotowywanie ryzyka i zarządzanie nim. Zidentyfikowane zagrożenia zamieszczono w rejstrze zagrożeń razem z wymogami bezpieczeństwa mającymi na celu nadzorowanie powiązanego ryzyka, tj. odniesienie do dodatkowego sprzętu na pokładzie pociągu i na torowisku, a także do zmienionych procedur obsługi.
Zmienione procedury monitorowano i w razie potrzeby weryfikowano, aby zapewnić właściwy nadzór nad zidentyfikowanymi zagrożeniami w trakcie eksploatacji systemu kolejowego.

(g) niezależna ocena [Artykuł 6]:

Procesy oceny ryzyka i zarządzania ryzykiem zostały ocenione przez kompetentną osobę w przedsiębiorstwie kolejowym, która nie była związana z procesem oceny. Kompetentna osoba dokonała oceny zarówno procesu, jak i jego wyników, tj. zidentyfikowanych wymogów bezpieczeństwa.

Na podstawie sprawozdania z niezależnej oceny przygotowanego przez kompetentną osobę przedsiębiorstwo kolejowe podejmuje decyzję o eksploatacji systemu.

C.12.4. Przykład pokazuje, że zasady i proces zastosowany przez przedsiębiorstwo kolejowe są zgodne z wspólną metodą bezpieczeństwa. Proces zarządzania ryzykiem i oceny ryzyka spełnił wszystkie wymagania z CSM.

C.13. Przykład zastosowania systemu odniesienia w celu określenia wymogów bezpieczeństwa dla nowych nastawnic elektronicznych

C.13.1. **C.5.1.** Uwaga: ten przykład oceny ryzyka nie jest wynikiem zastosowania procesu CSM; został przygotowany przed powstaniem CSM. Przykład ten ma na celu:

(a) wskazanie podobieństw pomiędzy istniejącymi metodami oceny ryzyka i procesem CSM;
(b) umożliwienie prześledzenia powiązań pomiędzy istniejącym procesem i procesem wymaganym przez CSM;
(c) uzasadnienie wartości dodanej wynikającej z przeprowadzenia (w razie potrzeby) dodatkowych etapów, wymaganych przez CSM.

Należy zaznaczyć, że ten przykład zamieszczono wyłącznie w celach informacyjnych. Ma on ułatwić czytelnikowi zrozumienie procesu CSM. Samego przykładu nie można jednak przetransponować do systemu odniesienia lub wykorzystać jako systemu odniesienia dla innej znaczącej zmiany. Ocena ryzyka jest dokonywana w odniesieniu do każdej istotnej zmiany zgodnie z rozporządzeniem CSM.

C.13.2. W celu określenia standardowych wymogów bezpieczeństwa dla przyszłych nastawnic elektronicznych, Deutsche Bahn przeprowadziło analizę ryzyka już zatwierdzonego systemu elektronicznego. System został poprzednio zatwierdzony zgodnie z niemieckimi kodeksami postępowania (Mü 8004).

C.13.3. Analiza ryzyka została przeprowadzona zgodnie z normami CENELEC (EN 50126 i EN 50129) i obejmowała następujące etapy:

European Railway Agency ● Marc LEFRANCQ, 120 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

(a) definicję systemu;
(b) identyfikację zagrożeń;
(c) analizę zagrożeń i kwantyfikację.

C.13.4. W celu zdefiniowania systemu dołożono starań, by zdefiniować granice systemu, jego funkcje i interfejsy. Największym wyzwaniem było zdefiniowanie systemu w taki sposób, by zachować jego niezależność od wewnętrznej architektury systemu nastawnic, zachowując jego kompatybilność z istniejącymi systemami nastawnic. Szczególną uwagę zwrócono na jasne zdefiniowanie interfejsów z systemami zewnętrznymi współpracującymi z nastawnicami, bez szczegółowego wyliczania wewnętrznych funkcji nastawnic.

C.13.5. Następnie zidentyfikowano zagrożenia tylko na płaszczyznach interfejsów tak, by zachować pewien stopień ogólności (tj. uniknąć zależności od architektury konkretnych systemów). Uwzględniono tylko zagrożenia wynikające z awarii. Dla każdego przypadku interfejsu zidentyfikowano dwa ogólne zagrożenia:

(a) niepoprawne dane wyjściowe na temat nastawnic przekazane w interfejsie
(b) (poprawne) dane wejściowe ulegają zniekształceniu w interfejsie

C.13.6. Następnie te ogólne zagrożenia zostały bardziej szczegółowo opisane w kontekście każdego przypadku interfejsu.

C.13.7. Na tym etapie przeanalizowano i umieszczono w analizie drzewa niezdatności czynniki związane z komponentami istniejącego systemu przyczyniające się do zidentyfikowanych zagrożeń. Pozwoliło to, na podstawie oszacowanego stopnia zawodności podzespołów, obliczyć współczynnik występowania każdego zagrożenia i wykorzystać te dane jako współczynnik tolerowanego zagrożenia (THR) dla kolejnych generacji nastawnic elektronicznych.

C.13.8. Krajowy organ ds. bezpieczeństwa (EBA) zapoznał się z analizą ryzyka i dokonał jej oceny.

C.13.9. W ramach analizy ryzyka przeprowadzono również analizę funkcji sterowania i wyświetlania systemu elektronicznego. Ponownie zastosowano już istniejący i zatwierdzony system nastawnic elektronicznych jako system odniesienia w celu określenia wymogów bezpieczeństwa dla funkcji związanych z interfejsem człowiek-maszyna (ang. Man-Machine-Interface (MMI)), mających na celu kontrolowanie losowych uszkodzeń i błędów, a także kontrolowanie systematycznych błędów. W wyniku tego ustalono poziomy integralności bezpieczeństwa (SIL) dla różnych funkcji: funkcji związanych z interfejsem człowiek-maszyna w standardowej eksploatacji, funkcji związanych z interfejsem człowiek-maszyna w eksploatacji typu Command-Release (funkcjonowanie pogorszone) oraz dla funkcji wyświetlania.

C.13.10. Krajowy organ ds. bezpieczeństwa (EBA) również zapoznał się z analizą ryzyka i dokonał jej oceny.

C.13.11. Powyższe przykłady oceny ryzyka ilustrują, w jaki sposób można stosować drugą zasadę akceptacji ryzyka CSM (system odniesienia) w celu określenia wymogów bezpieczeństwa dla nowego systemu. Ponadto przygotowano je na podstawie norm CENELEC i dlatego też są one zgodnie z procesem CSM. Ocena ryzyka zastosowana w przykładach spełnia wszystkie wymogi z CSM dotyczące faz uwzględnionych w CSM. Ponieważ brak etapu projektu, nie ma tu odniesienia do zarządzania rejestrem zagrożeń ani do wykazywania zgodności systemu objętego oceną z określonymi wymogami bezpieczeństwa.

C.13.12. Więcej informacji na temat tych analiz ryzyka można znaleźć w:

European Railway Agency ● Marc LEFRANCQ, 120 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

(a) Ziegler, P., Kupfer, L., Wunder, H.: „Erfahrungen mit der Risikoanalyse ESTW (DB AG)", Signal+Draht, 10, 2003, 10-15; oraz

(b) Bock, H., Braband, J., and Harborth, M.: "Safety Assessment of Vital Control and Display Functions in Electronic Interlockings, in Proc. AAET2005 Automation, Assistance and Embedded Real Time Platforms for Transportation", GZVB, Braunschweig, 2005, 234-253.

C.14. Przykład jednoznacznego kryterium akceptacji ryzyka w przypadku ruchu pociągów w oparciu o łączność radiową FFB w Niemczech

C.14.1. **C.5.1.** Uwaga: ten przykład oceny ryzyka nie jest wynikiem zastosowania procesu CSM; został przygotowany przed powstaniem CSM. Przykład ten ma na celu:

(a) wskazanie podobieństw pomiędzy istniejącymi metodami oceny ryzyka i procesem CSM;
(b) umożliwienie prześledzenia powiązań pomiędzy istniejącym procesem i procesem wymaganym przez CSM;
(c) uzasadnienie wartości dodanej wynikającej z przeprowadzenia (w razie potrzeby) dodatkowych etapów, wymaganych przez CSM.

Należy zaznaczyć, że ten przykład zamieszczono wyłącznie w celach informacyjnych. Ma on ułatwić czytelnikowi zrozumienie procesu CSM. Samego przykładu nie można jednak przetransponować do systemu odniesienia lub wykorzystać jako systemu odniesienia dla innej znaczącej zmiany. Ocena ryzyka jest dokonywana w odniesieniu do każdej istotnej zmiany zgodnie z rozporządzeniem CSM.

C.14.2. Przeprowadzono analizę ryzyka zgodną z normami CENELEC dla całkowicie nowej procedury eksploatacyjnej, którą planowano (ale której nigdy nie wprowadzono) w Niemczech na konwencjonalnych liniach kolejowych. Pomysł polegał na bezpiecznej eksploatacji pociągów tylko za pośrednictwem sterowania (trasą i pociągiem) za pośrednictwem łączności radiowej. Ponieważ nie istniały żadne normy czynnościowe (zatwierdzone zasady techniki) i systemy odniesienia dla takiego nowego systemu, przeprowadzono jawne szacowanie ryzyka w celu wykazania bezpieczeństwa nowej procedury. Należało wykazać, że poziom ryzyka dla pasażera związany z nowym systemem nie przekroczy dopuszczalnej wartości ryzyka (jawna zasada akceptacji ryzyka).

C.14.3. Ta jawna zasada akceptacji ryzyka została oszacowane na podstawie statystyk wypadków w Niemczech, które związane były z systemami sygnalizacji i sterowania: jej wiarygodność sprawdzono także, zestawiając ją z MEM. Takie wykazanie bezpieczeństwa zgodne jest z niemieckim wymogiem EBO, zgodnie z którym należy zachować ten sam poziom bezpieczeństwa na wypadek odstępstw od zasad techniki. Krajowy organ ds. bezpieczeństwa (EBA) zapoznał się z analizą ryzyka i dokonał jej oceny.

C.14.4. Przykład oceny ryzyka pokazuje, jak dla nowych systemów, dla których nie ma obowiązujących kodeksów postępowania czy systemów odniesienia, można wypracować uniwersalną jawną zasadę (trzecia zasada akceptacji ryzyka CSM). Analiza ryzyka, którą następnie przeprowadzono dla nowego systemu, była oparta o normy CENELEC i w związku z tym zgodna była z procesem CSM. Ocena ryzyka wymieniona w przykładzie spełnia wymogi CSM, ale nie ma odniesienia do zarządzania rejestrem zagrożeń ani do wykazania zgodności systemu objętego oceną z określonymi wymogami bezpieczeństwa.

European Railway Agency ● Marc LEFRANCQ, 120 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

C.14.5. Dodatkowe informacje na temat analizy ryzyka można znaleźć w: Braband, J., Günther, J., Lennartz, K., Reuter, D.: *"Risikoakzeptanzkriterien für den FunkFahrBetrieb (FFB)"*, Signal + Draht, Nr.5, 2001, 10-15

C.15. Przykład testu stosowalności RAC-TS

C.15.1. Niniejszy załącznik ma na celu pokazanie, na przykładzie funkcji podsystemu pokładowego ETCS, jak stosować kryterium określone w części 2.5.4 i jak ustalić, czy RAC-TS ma zastosowanie.

C.15.2. Podsystem pokładowy ETCS jest systemem technicznym. Bierze się pod uwagę następującą funkcję: *„dostarczyć maszyniście informacji pozwalających mu na prowadzenie pociągu w sposób bezpieczny i uruchomić funkcję hamowania w przypadku przekroczenia dopuszczalnej prędkości".*

Opis funkcji: na podstawie informacji uzyskanych na trasie pociągu (dozwolona prędkość) i w oparciu o prędkość obliczoną przez podsystem pokładowy ETCS:

(a) maszynista prowadzi pociąg zachowując dozwoloną prędkość;
(b) jednocześnie podsystem pokładowy ETCS nadzoruje, czy pociąg nie przekracza dozwolonej prędkości. Jeżeli zostanie rozwinięta nadmierna prędkość, podsystem uruchamia automatyczne hamowanie.

Zarówno maszynista, jak i podsystem pokładowy ETCS uwzględniają obliczenia prędkości dostarczanych przez podsystem pokładowy ETCS.

C.15.3. Pytanie: Czy stosuje się RAC-TS do obliczeń prędkości dostarczanych przez podsystem pokładowy ETCS?

C.15.4. Stosowanie diagramu sekwencji działań na Schemat 14 i odpowiedzi na różne pytania:

(a) zagrożenie uwzględnione w odniesieniu do systemu technicznego:

„Przekroczenie prędkości bezpiecznej zaleconej w ramach ETCS" (zob. UNISIG SUBSET 091)

(b) Czy można nadzorować zagrożenie poprzez stosowanie kodeksu postępowania lub systemu odniesienia?

NIE. Zakłada się, że system ETCS jest nowy i innowacyjny, w związku z czym nie istnieją kodeksy postępowania lub systemy odniesienia, które umożliwiają utrzymanie zagrożenia na dopuszczalnym poziomie.

(c) Czy istnieje prawdopodobieństwo, że zagrożenie może mieć katastroficzne konsekwencje?

TAK, ponieważ *„przekroczenie prędkości bezpiecznej zaleconej w ramach ETCS" może skutkować wykolejeniem pociągu, a to z kolei może doprowadzić do „ofiar śmiertelnych lub licznych poważnych obrażeń lub poważnych szkód w środowisku spowodowanych wypadkiem*".

(d) Czy katastroficzne konsekwencje są bezpośrednim skutkiem awarii systemu technicznego?

TAK, jeżeli nie istnieją żadne dodatkowe bariery ochronne. To samo wyliczenie prędkości dokonane przez podsystem pokładowy ETCS przekazywane jest zarówno maszyniście, jak i przesyłane do układu sterowania hamulców podsystemu pokładowego ETCS. W związku z tym, zakładając, że maszynista prowadzi pociąg (ze względu na wydajność) z maksymalną prędkością dozwoloną na tej trasie, wówczas ani

European Railway Agency ● Marc LEFRANCQ, 120 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

maszynista, ani podsystem pokładowy ETCS nie wykryje, że pociąg porusza się z nadmierną prędkością, jeżeli prędkość pociągu została zbyt nisko oszacowana. To może doprowadzić do katastrofalnego w skutkach wykolejenia się pociągu.

(e) Wnioski:

(1) dotyczące wymogów ilościowych: należy zastosować współczynnik tolerowanego zagrożenia wynoszący 10^{-9}/godzinę dla uszkodzeń losowych, gwarantując, że:

(i) ocena tego wymogu ilościowego uwzględnia wspólne podzespoły systemów rezerwowych (np. pojedyncze lub wspólne wejścia do wszystkich kanałów, wspólne zasilanie, komparatory, … itp.);
(ii) uwzględniono czas wykrycia wad ukrytych;
(iii) przeprowadzono analizę uszkodzeń wywołanych wspólną przyczyną (CCF/CMF);
(iv) dokonywana jest niezależna ocena;

(2) w przypadku wymogów technologicznych: należy zastosować proces związany z 4. poziomem integralności bezpieczeństwa (SIL) w celu zarządzania systematycznymi awariami/błędami podsystemu pokładowego ETCS. Wymaga to zastosowania:

(i) procesu zarządzania jakością zgodnego z 4. poziomem integralności bezpieczeństwa;

(ii) procesu zarządzania jakością zgodnego z 2. poziomem integralności bezpieczeństwa;

(iii) odpowiednich norm, np.:

- do opracowania oprogramowania należy zastosować normę EN 50 128;
- do rozbudowywania sprzętu należy zastosować normy EN 50 121-3-2, EN 50 121-4, EN 50 124-1, EN 50 124-2, EN 50 125-1 EN 50 125-3, EN 50 50081, EN 50 155, EN 61000-6-2 itp.;

(3) niezależna ocena procesów.

C.16. Przykładowy układ wykazu zagrożeń

C.16.1. Wprowadzenie

C.16.1.1. Minimalne wymogi zamieszczone w rejestrze zagrożeń określono w części 4.1.2 rozporządzenia CSM. Zostały one zaznaczone szarym tłem w poniższych przykładach rejestrów ryzyka.

C.16.1.2. Rejestr zagrożeń może mieć różny układ; to samo dotyczy dodatkowych informacji określających zagrożenia i powiązane środki bezpieczeństwa. Na przykład zagrożenia i powiązane środki bezpieczeństwa można umieścić w jednym polu dla każdej informacji. Niemniej jednak bez względu na to, jaki układ jest stosowany, ważne jest, by rejestr zagrożeń w jasny sposób pokazywał związki między zagrożeniami a powiązanymi środkami bezpieczeństwa. Jednym rozwiązaniem może być rejestr zagrożeń, który - dla każdego zagrożenia i środka bezpieczeństwa - zawiera co najmniej jedno pole z:

(a) zrozumiałym opisem zawierającym informacje na temat pochodzenia zasady akceptacji ryzyka wybranej do nadzorowania powiązanego zagrożenia. Pole to umożliwi zrozumienie zagrożenia i powiązanych środków bezpieczeństwa, a także zorientowanie się, w której analizie bezpieczeństwa zostały one określone.

European Railway Agency ● Marc LEFRANCQ, 120 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

Ponieważ rejestr zagrożeń stosowany jest i prowadzony przez cały cykl życia systemu (tj. podczas eksploatacji i utrzymania systemu), przydatny jest zrozumiały sposób wykrywania zależności, lub związku, między każdym zagrożeniem a:

(1) powiązanym ryzykiem;
(2) przyczynami zagrożenia, o ile zostały ustalone;
(3) powiązanymi środkami bezpieczeństwa, jak również założeniami definiującymi granice systemu objętego oceną;
(4) powiązanymi analizami bezpieczeństwa, w których zidentyfikowano zagrożenie;

Ponadto sformułowania dotyczące środków bezpieczeństwa (zwłaszcza tych, które mają być przekazane innym podmiotom np. wnioskodawcy), a także sformułowania dotyczące powiązanych zagrożeń i rodzajów ryzyka, muszą być zrozumiałe i wystarczające. „Zrozumiałe i wystarczające" tj. sformułowane w taki sposób, żeby można było zrozumieć, jakie rodzaje ryzyka mają być nadzorowane w przypadku danych środków bezpieczeństwa i powiązanych zagrożeń, bez konieczności wracania do analiz dotyczących bezpieczeństwa.

(b) zasadą akceptacji ryzyka stosowaną do kontrolowania danego zagrożenia tak, by wspierać wzajemne uznawanie oraz pomóc organowi oceniającemu w dokonaniu oceny właściwego stosowania CSM;

(c) zrozumiałą informacją o statusie: w polu tym określa się, czy powiązane zagrożenie/środek bezpieczeństwa jest „otwarty", czy nadzorowany/zatwierdzony.

(1) śledzi się „otwarte" zagrożenie/środek bezpieczeństwa aż do czasu objęcia go nadzorem/ zatwierdzenia;
(2) z kolei nie śledzi się już nadzorowanych/zatwierdzonych zagrożeń/ środków bezpieczeństwa, chyba że zajdzie istotna zmiana w eksploatacji lub utrzymaniu systemu: zob. część 2.1.1 pkt. [G 6](b). Jeżeli to nastąpi:
(i) ponownie stosuje się CSM w odniesieniu do wymaganych zmian zgodnie z Artykuł 2. zob. również część 2.1.1 pkt. [G 6](b) (1).
(ii) ponownie analizuje się wszystkie nadzorowane zagrożenia i środki bezpieczeństwa w celu sprawdzenia, czy zmiany nie wywarły na nie wpływu. Jeżeli wywarły wpływ, powiązane zagrożenia i środki bezpieczeństwa są ponownie „otwierane", umieszczane w rejestrze zagrożeń i monitorowane;

Może się tak zdarzyć, że wdrożone zostają inne środki bezpieczeństwa niż środki zamieszczone w rejestrze zagrożeń (np. ze względu na koszty). Wówczas wdrożone środki bezpieczeństwa zamieszcza się w rejestrze zagrożeń razem z dowodami/ uzasadnieniem ich stosowności i wykazaniem, że przy zastosowaniu tych środków system zgodny jest z wymogami bezpieczeństwa.

(d) odniesieniem do powiązanego dowodu wykorzystywanego do kontrolowania zagrożenia lub zatwierdzenia środka bezpieczeństwa. To pole umożliwia późniejsze odnalezienie danych, które umożliwiły nadzorowanie danego zagrożenia lub zatwierdzenie powiązanych środków bezpieczeństwa;

Zagrożenie może być umieszczone w rejestrze zagrożeń i kontrolowane, jeżeli wszystkie powiązane środki bezpieczeństwa (dotyczące zagrożenia) zostały wcześniej zatwierdzone;

(e) informacjami na temat organizacji lub podmiotów odpowiedzialnych za zarządzanie.

C.16.1.3. Inny przykład ewentualnej zawartości rejestru zagrożeń podany jest w załączniku A.3 wytycznych do normy EN 50126-2 {Ref. 9}.

European Railway Agency ● Marc LEFRANCQ, 120 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

C.16.2. Przykład rejestru zagrożeń w przypadku zmiany organizacyjnej w części C.5. załącznika C

Tabela 6: Przykład rejestru zagrożeń w przypadku zmiany organizacyjnej w części C.5 załącznika C.

Opis zagrożenia	**Środki bezpieczeństwa**	**Znaczenie/ Bezpieczeństwo Terminowość**	**Wdrażanie**[18]	**Komentarze**	**Odpowiedzialność**[18]	**Pochodzenie**	**Zastosowana zasada akceptacji ryzyka**	**Odpowiedzialność za weryfikację**	**Sposób weryfikacji**	**Status xx.xx.xx**
Niska motywacja pracowników Przedsiębiorstwa. Wynikające z tego zwolnienia pracowników Brak motywacji / zmęczenie kierowników	Nowe zadania, które zmotywowałyby pracowników; praca w mniejszych grupach Przesunięcie funduszy, żeby przedsiębiorstwo mogło wykonywać bardziej poważne zadania Więcej częstych kontroli przeprowadzanych przez zarządcę torowiska kolejowego. Taki przydział funduszy, który pozwoli na zatrzymanie kluczowych pracowników w trakcie całego procesu. Zwrócenie szczególnej uwagi na to, by odchodzący pracownicy przekazywali swoją wiedzę nowym pracownikom przejmującym ich zadania. itp.	Wysokie/Wysokie	Koordynowane przez XYZ. W regionach należy przyjrzeć się środkom mającym na celu zwiększenie kontroli nad torowiskami, zmianami pracowników i działaniami następczymi zarządcy linii kolejowej	W umowach powinny być uwzględnione częstsze kontrole itp.	dyrektor przedsiębiorstwa	Metoda burzy mózgów. Sprawozdanie R_X z identyfikacji zagrożenia (HAZID)	NIE DOTYCZY			Zmiana warunków znacznie zmniejszyła to ryzyko. Przeprowadzono analizę środowiska pracy; szkolenie personelu
Podwykonawcy przedsiębiorców, którzy nie mają umiejętności, kompetencji i nie prowadzą kontroli jakości	Zwiększone zapotrzebowanie na udokumentowane kompetencje. Systematyczna kontrola wykonywanych zadań	Wysokie/średnie	Zarządca infrastruktury koordynuje. W regionach należy wdrożyć środki w zakresie wymagania	Wdrożone poprzez umowne działania następcze. Dane wejściowe do planowania przeglądu	Zarządca infrastruktury	Metoda burzy mózgów. Sprawozdanie RX z identyfikacji zagroże	NIE DOTYCZY	Kierownik ds. bezpieczeństwa		Zwiększony nacisk na regularne kontrole (2 kontrole eksploatacji miesięcznie na dany obszar eksploatacji)

(18) *Te dwie kolumny odnoszą się do pola z informacjami na temat podmiotów odpowiedzialnych za kontrolowanie zidentyfikowanych zagrożeń.*

European Railway Agency ● Marc LEFRANCQ, 120 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

Tabela 6: Przykład rejestru zagrożeń w przypadku zmiany organizacyjnej w części C.5 załącznika C.

Opis zagrożenia	**Środki bezpieczeństwa**	**Znaczenie/ Bezpieczeństwo Terminowość**	**Wdrażanie**[18]	**Komentarze**	**Odpowiedzialność**[18]	**Pochodzenie**	**Zastosowana zasada akceptacji ryzyka**	**Odpowiedzialność za weryfikację**	**Sposób weryfikacji**	**Status xx.xx.xx**
			kompetencji i kontrolowania pracy			nia (HAZID)				
Brak pewności co do ról i obowiązków w interfejsie między przedsiębiorstwem a zarządcą infrastruktury (zarządcą torowiska kolejowego).	Należy zdefiniować role i obowiązki. Należy rozrysować wszystkie interfejsy i zdefiniować, kto jest za nie odpowiedzialny.	Średnie/średnie	W każdym regionie oddzielnie	Wdrożony umową o utrzymaniu i planem strategicznym reorganizacji	Dyrektorzy regionalni	Metoda burzy mózgów. Sprawozdanie RX z identyfikacji zagrożenia (HAZID)	NIE DOTYCZY	Kierownik ds. bezpieczeństwa		Regiony zaprezentowały swoją strategię.

European Railway Agency ● Marc LEFRANCQ, 120 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

C.16.3. Przykład pełnego rejestru zagrożeń w przypadku pokładowego podsystemu sterowania ruchem pociągu

C.16.3.1. Ta część podaje przykład jednego wykazu zagrożeń (zob. część 4.1.1 pkt 4.1.1) do zarządzania zarówno:

(a) wszystkimi wewnętrznymi wymogami bezpieczeństwa mającymi zastosowanie do podsystemu, za który odpowiedzialny jest podmiot; jak i

(b) wszystkimi zagrożeniami i powiązanymi środkami bezpieczeństwa, których podmiot nie może wdrożyć, i które muszą być przekazane innym podmiotom.

Tabela 7: Przykład rejestru zagrożeń producenta w przypadku pokładowego podsystemu sterowania ruchem pociągu

Zagrożenie nr	Pochodzenie	Opis zagrożenia	Dodatkowe informacje	Podmiot odpowiedzialny	Środek bezpieczeństwa	Zastosowana zasada akceptacji ryzyka	Przekazane	Status
1	Sprawozdanie R_X HAZOP	Zawyżona maksymalna prędkość pociągu (Vmax)	Niepoprawna szczegółowa konfiguracja pokładowego podsystemu (personel odpowiedzialny za utrzymanie). Wprowadzenie niepoprawnych danych na pokładzie (maszynista)	Przedsiębiorstwo kolejowe	• Należy zdefiniować procedurę zatwierdzania danych konfiguracyjnych pokładowego podsystemu; • Należy zdefiniować procedurę eksploatacyjną dla procesu wprowadzania danych przez maszynistę;	jawne oszacowanie	Tak	Kontrolowane (przekazane do przedsiębiorstwa kolejowego) zob. również część C.16.4.2. w załączniku C
2	Sprawozdanie RX HAZOP	Krzywa hamowania (tj. zezwolenia na jazdę) w pokładowym podsystemie konfiguracji danych niewłaściwa	Procedura szczegółowej konfiguracji pokładowego podsystemu zależy od: • marginesu bezpieczeństwa uwzględnionego w układzie hamulcowym pociągu; • czas reakcji układu hamulcowego (zależy on bezpośrednio od długości pociągu, zwłaszcza w przypadku pociągów towarowych)	Przedsiębiorstwo kolejowe	• Należy właściwie określić wymogi techniczne systemu w definicji systemu; • Należy przyjąć wystarczające marginesy bezpieczeństwa dla układu hamulcowego danego pociągu;	jawne oszacowanie	Tak	Kontrolowane (przekazane do przedsiębiorstwa kolejowego) zob. również część C.16.4.2. w załączniku C
3	Sprawozdanie RX HAZOP	• Zawyżona maksymalna prędkość pociągu (Vmax) • niewłaściwa krzywa hamowania (tj. uprawnienie ruchu) w pokładowym podsystemie danych konfiguracyjnych	Brak aktualizacji średnicy koła pociągu w konkretnej konfiguracji pokładowego podsystemu (personel utrzymania ruchu).	Przedsiębiorstwo kolejowe	• Należy zdefiniować procedurę pomiaru średnicy koła pociągu przez personel utrzymania ruchu; • Należy zdefiniować procedurę mierzenia średnicy koła pociągu przez personel utrzymania ruchu;	jawne oszacowanie	Tak	Kontrolowane (przekazane do przedsiębiorstwa kolejowego) zob. również część C.16.4.2. w załączniku C
			Błąd w procedurze producenta dotyczącej	Producent	Należy zdefiniować procedurę	jawne	Tak	Kontrolowane

European Railway Agency ● Marc LEFRANCQ, 120 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

Tabela 7: Przykład rejestru zagrożeń producenta w przypadku pokładowego podsystemu sterowania ruchem pociągu

Zagrożenie nr	Pochodzenie	Opis zagrożenia	Dodatkowe informacje	Podmiot odpowiedzialny	Środek bezpieczeństwa	Zastosowana zasada akceptacji ryzyka	Przekazane	Status
			przygotowania i wprowadzenia danych konfiguracyjnych do pokładowego podsystemu		aktualizacji średnicy koła pociągu w pokładowych danych konfiguracyjnych	oszacowanie		Procedurą P_X
4	Sprawozdanie RX HAZOP	Wjazd pociągu z dużą prędkością na tory (160 km/h, jeżeli sygnalizacja wskazuje, że droga jest wolna), który nie ma aktywnego pokładowego podsystemu sterowania ruchem pociągu i bez sygnalizacji przytorowej	Może być kontrolowane tylko dzięki czujności maszynisty. Wjazd na teren przytorowy z ATP uwarunkowane jest procedurą potwierdzenia przeprowadzona przez maszynistę przed punktem przejścia. Jeżeli brak potwierdzenia, pokładowy system sterowania ruchem pociągu automatycznie uruchamia układ hamulcowy.	Zarządca infrastruktury	Zarządca infrastruktury gwarantuje, że pociągi niewyposażone w aktywny pokładowy podsystem sterowania nie wjadą na dane tory. Należy zdefiniować procedurę zarządzania ruchem pociągów.	jawne oszacowanie	Tak	Kontrolowane (przekazane do zarządcy infrastruktury) zob. również część C.16.4.2. w załączniku C
				Przedsiębiorstwo kolejowe	Należy zapewnić szkolenie dla maszynistów w zakresie wjeżdżania na obszar z ATP	jawne oszacowanie	Tak	Kontrolowane (przekazane do przedsiębiorstwa kolejowego) zob. również część C.16.4.2. w załączniku C
5	Sprawozdanie RX HAZOP	Zawyżona maksymalna prędkość pociągu (Vmax) wyświetlająca się maszyniście	Informacja wyświetlona na interfejsie maszynisty jest monitorowana przez pokładowy podsystem sterowania ruchem pociągu o 4. poziomie integralności bezpieczeństwa, który automatycznie uruchamia hamowanie awaryjne w przypadku rozbieżności między wyświetloną a oczekiwaną wartością. W przypadku braku zgodności z zezwoleniem na jazdę, pokładowy podsystem sterowania ruchem pociągu uruchamia awaryjne hamowanie	Producent	Należy opracować pokładowy podsystem sterowania ruchem pociągu o 4. poziomie integralności bezpieczeństwa	jawne oszacowanie	Tak	Dowód bezpieczeństwa wykazujący ocenę podsystemu o 4. poziomie integralności bezpieczeństwa dokonaną przez organ ds. oceny bezpieczeństwa
6	Sprawozdanie RX HAZOP	Pociąg odjeżdża bez interfejsu człowiek-maszyna	Utrata struktury nadmiarowej pokładowego podsystemu	Producent	Należy opracować pokładowy podsystem sterowania ruchem pociągu o 4. poziomie integralności bezpieczeństwa	jawne oszacowanie	Tak	Dowód bezpieczeństwa wykazujący ocenę podsystemu o 4. poziomie integralności bezpieczeństwa dokonaną przez

European Railway Agency ● Marc LEFRANCQ, 120 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

Tabela 7: Przykład rejestru zagrożeń producenta w przypadku pokładowego podsystemu sterowania ruchem pociągu

Zagrożenie nr	Pochodzenie	Opis zagrożenia	Dodatkowe informacje	Podmiot odpowiedzialny	Środek bezpieczeństwa	Zastosowana zasada akceptacji ryzyka	Przekazane	Status
								organ ds. oceny bezpieczeństwa
itp.								

C.16.4. Przykład rejestru zagrożeń w przypadku przekazywania informacji innym podmiotom

C.16.4.1 W tej części podany jest przykład rejestru zagrożeń w przypadku, gdy dany podmiot przekazuje innym podmiotom zidentyfikowane zagrożenia i powiązane środki bezpieczeństwa, których nie może wdrożyć. Zobacz część [G 1] pkt. 4.1.1.
Jest to ten sam przykład, co podany w części C.16.3. załącznika C. Jedyną różnicą jest to, że usunięto wszystkie wewnętrzne zagrożenia i środki bezpieczeństwa, które ten podmiot mógł kontrolować.

C.16.4.2. Ostatnia kolumna w Tabela 8 jest wykorzystana do spełnienia wymogu w części 4.2 rozporządzenia CSM. Można przyjąć różne rozwiązania, żeby spełnić ten warunek. Jednym sposobem jest odniesienie się do dowodów wykorzystanych przez podmiot, który otrzymał przekazane informacje na temat bezpieczeństwa. Inny sposobem jest spotkanie dwóch podmiotów mające na celu wspólne wypracowanie adekwatnego rozwiązania w zakresie kontrolowania powiązanym ryzykiem. Wyniki takiego spotkania można by przedstawić w uzgodnionym dokumencie (na przykład protokole ze spotkania), do którego może odnieść się podmiot, któremu przekazano informacje związane z bezpieczeństwem, w celu „zamknięcia" powiązanych zagrożeń w swoim rejestrze zagrożeń.

European Railway Agency ● Marc LEFRANCQ, 120 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

Tabela 8: Przykład rejestru zagrożeń w przypadku przekazywania innym podmiotom informacji związanych z bezpieczeństwem

ZAGROŻENIE NR	Pochodzenie zagrożenia: Nr w Tabela 7	Pochodzenie zagrożenia: Inne	Opis zagrożenia	Dodatkowe informacje	Podmiot odpowiedzialny	Środek bezpieczeństwa	Komentarze od podmiotów otrzymujących
1	N°1	Sprawozdanie RX HAZOP	Zawyżona maksymalna prędkość pociągu (Vmax)	Niepoprawnie określona konfiguracja pokładowego podsystemu (personel odpowiedzialny za utrzymanie). Wprowadzenie niepoprawnych danych na pokładzie (maszynista)	Przedsiębiorstwo kolejowe	• Należy zdefiniować procedurę zatwierdzania danych konfiguracyjnych pokładowego podsystemu; • Należy zdefiniować procedurę eksploatacyjną dla procesu wprowadzania danych przez maszynistę;	• Dane konfiguracyjne pokładowego podsystemu sterowania ruchem pociągu zależą od fizycznych właściwości taboru. • Wówczas do tych danych stosowane są marginesy bezpieczeństwa ustalone miedzy zarządca infrastruktury i przedsiębiorstwem kolejowym. • Dane te następnie wprowadza się do pokładowego podsystemu zgodnie z odpowiednią procedurą producenta na etapie instalacji, integracji z taborem i akceptacji podsystemu sterowania ruchem pociągu. • Maszynistów szkoli się i ocenia w zakresie procedury D_P. • Maszyniści są również oceniani przez zarządcę infrastruktury pod względem zasad obowiązujących w obrębie infrastruktury zarządcy infrastruktury.
2	N°2	Sprawozdanie RX HAZOP	Krzywa hamowania (tj. upoważnienie do ruchu) w pokładowym podsystemie konfiguracji danych niewłaściwa	Procedura szczegółowej konfiguracji pokładowego podsystemu zależy od: • marginesu bezpieczeństwa uwzględnianego w układzie hamulcowym pociągu; • czasu reakcji układu hamulcowego (zależy on bezpośrednio od długości pociągu, zwłaszcza w przypadku pociągów towarowych)	Przedsiębiorstwo kolejowe	• Należy prawidłowo określić wymogi techniczne systemu w definicji systemu; • Należy przyjąć wystarczające marginesy bezpieczeństwa dla układu hamulcowego danego pociągu;	Zobacz komentarz dla pierwszego wiersza powyżej.
3	N°3	Sprawozdanie RX HAZOP	• Zawyżona maksymalna prędkość pociągu (Vmax) • Krzywa hamowania (tj. upoważnienie do ruchu) w pokładowym podsystemie konfiguracji danych niewłaściwa	Brak aktualizacji średnicy koła pociągu w konkretnej konfiguracji pokładowego podsystemu (personel utrzymania ruchu).	Przedsiębiorstwo kolejowe	• Należy zdefiniować procedurę pomiaru średnicy koła pociągu przez personel utrzymania ruchu; • Należy zdefiniować procedurę mierzenia średnicy koła pociągu przez personel utrzymania ruchu;	• Utrzymanie pokładowego podsystemu sterowania ruchem pociągu prowadzone jest na podstawie procedury utrzymania ruchu (ang. Maintenance Procedure MP_Z). • Średnica koła pociągu aktualizowana jest w określonych odstępach czasu zgodnie z procedurą P_W. • Jeżeli chodzi o proces wprowadzania danych, maszynistów szkoli się i ocenia w zakresie „procedury P_{DE}”.

European Railway Agency ● Marc LEFRANCQ, 120 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

Tabela 8: Przykład rejestru zagrożeń w przypadku przekazywania innym podmiotom informacji związanych z bezpieczeństwem

ZAGROŻENIE NR	Pochodzenie zagrożenia		Opis zagrożenia	Dodatkowe informacje	Podmiot odpowiedzialny	Środek bezpieczeństwa	Komentarze od podmiotów otrzymujących
	Nr w Tabela 7	Inne					
4	N°4	Sprawozdanie RX HAZOP	Wjazd pociągu z dużą prędkością na tory (160 km/h jeżeli sygnalizacja wskazuje, że droga jest wolna), który nie ma aktywnego pokładowego podsystemu sterowania ruchem pociągu i bez sygnalizacji przytorowej	Może być kontrolowane tylko dzięki czujności maszynisty. Wjazd na obszar z przytorowym ATP uwarunkowane jest procedurą zatwierdzenia przeprowadzona przez maszynistę przez miejscem zmiany kierunku. Jeżeli brak potwierdzenia, pokładowy system sterowania ruchem pociągu automatycznie uruchamia układ hamulcowy.	Zarządca infrastruktury	Zarządca infrastruktury gwarantuje, że pociągi niewyposażone w aktywny pokładowy podsystem sterowania ruchem pociągu nie wjadą na dane tory. Należy zdefiniować procedurę zarządzania ruchem pociągów.	Zarządzanie ruchem w obrębie infrastruktury zarządcy regulowane jest regulaminem R_{TM}
					Przedsiębiorstwo kolejowe	Należy zapewnić szkolenie dla maszynistów w zakresie wjeżdżania na teren z ATP	• Maszynistów szkoli się w regularnych odstępach czasu w zakresie procedury zarządcy infrastruktury P_{IM_DP}. • Maszyniści są również oceniani przez zarządcę infrastruktury pod względem regulaminu (S_R) obowiązującego w obrębie infrastruktury zarządcy infrastruktury.
itp.							

European Railway Agency ● Marc LEFRANCQ, 120 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

C.17. Przykład ogólnego rejestru zagrożeń w eksploatacji kolei

C.17.1. Analiza optymalizacji ruchu kolejowego (ROSA), projekt w ramach DEUFRAKO (współpracy francusko-niemieckiej) mający na celu stworzenie ogólnego i kompleksowego wykazu zagrożeń obejmującego standardową eksploatację kolei. Celem i wyzwaniem było zdefiniowanie tych zagrożeń przy zachowaniu maksymalnego stopnia szczegółowości, nie odzwierciedlając jednocześnie specyfiki kolei francuskiej i niemieckiej. Rejestr sporządzono na podstawie obecnie funkcjonujących rejestrów zagrożeń z obu tych państwach (SNCF i DB), które również porównano z rejestrami zagrożeń z innych państw. Pomimo zadeklarowanego założenia, że rejestr będzie ogólny i kompleksowy, zostaje on tutaj zamieszczony jedynie jako przykład, który może posłużyć jako pomoc dla podmiotów, które muszą zagrożenia w kontekście danego projektu. Oczekuje się, że zagrożenia wymienione w rejestrze zostaną prawdopodobnie dopracowane i uzupełnione, by odzwierciedlić specyfikę projektu.

C.17.2. Zagrożenia zamieszczone w poniższym rejestrze roboczym nazwane zostały „zagrożeniami wyjściowymi", tzn. zagrożeniami, na podstawie których można przeprowadzić zarówno analizę skutków, jak i analizę przyczyn, w celu określenia środków bezpieczeństwa/barier ochronnych i wymogów bezpieczeństwa w kontekście nadzorowania zagrożeń.

C.17.3. Wykaz zagrożeń projektu ROSA:

SPH 01	Nieprawidłowe początkowe określenie dopuszczalnej prędkości (związane z infrastrukturą)
SPH 02	Nieprawidłowe określenie dopuszczalnej prędkości (związane z pociągiem)
SPH 03	Nieprawidłowe określenie drogi hamowania/ niewłaściwa prędkość/ niewłaściwa krzywa hamowania
SPH 04	Niewystarczające wytracanie prędkości (przyczyny fizyczne)
SPH 05	Nieprawidłowe / niewłaściwe polecenie przyspieszenia/ hamowania
SPH 06	Nieprawidłowa odnotowana prędkość (pociąg poruszający się z niewłaściwą prędkością)
SPH 07	Nieprzekazanie informacji na temat dopuszczalnej prędkości
SPH 08	Pociąg odjeżdża samoistnie
SPH 09	Niewłaściwy kierunek jazdy/ celowy ruch wsteczny – (połączenie SPH 08 i SPH 14)
SPH 10	Nieprawidłowo odnotowana pozycja bezwzględna i względna
SPH 11	Niewykrycie pociągu
SPH 12	Utrata integralności pociągu
SPH 13	Możliwa zła trasa pociągu
SPH 14	Brak przekazania/ dostarczenia informacji na temat rozkładu/zezwolenia na jazdę
SPH 15	Awaria konstrukcyjna torowiska
SPH 16	Uszkodzony element przełącznika
SPH 17	Użycie niewłaściwego przełącznika
SPH 18	Status niewłaściwej zwrotnicy
SPH 19	Element systemu na torowisku /w obrębie przestrzeni swobodnej (z wyłączeniem obciążenia)
SPH 20	Obcy obiekt na torowisku/ w obrębie przestrzeni swobodnej
SPH 21	Osoba korzystająca z ruchu drogowego
SPH 22	Wpływ strumienia aerodynamicznego na obciążenie
SPH 23	Wpływ sił aerodynamicznych na pociąg
SPH 24	Wyposażenie/ element/ ładunek ogranicza przestrzeń swobodną pociągu
SPH 25	Nieprawidłowe wymiary przestrzeni swobodnej pociągu (przytorowej)
SPH 26	Niewłaściwe rozłożenie ładunku

European Railway Agency ● Marc LEFRANCQ, 120 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

SPH 27	Uszkodzone koło, uszkodzona oś
SPH 28	Rozgrzana oś/ koło/ łożysko
SPH 29	Awaria zespołu kół podwozia/ zawieszenia, amortyzatorów
SPH 30	Awaria ramy wagonu/nadwozia
SPH 31	Łamanie zakazu wstępu (aspekt związany z bezpieczeństwem)
SPH 32	Upoważniona osoba przechodzi przez tory
SPH 33	Personel pracujący na torach
SPH 34	Nieupoważniona osoba wkracza na tory (zaniedbanie)
SPH 35	Osoba spada z krawędzi peronu na tory
SPH 36	Cień aerodynamiczny/ osoba zbyt blisko krawędzi peronu
SPH 37	Personel pracujący w pobliżu torów np. na sąsiednich torach
SPH 38	Osoba celowo opuszcza pociąg (z wyłączeniem czasu wsiadania i wysiadania pasażerów)
SPH 39	Osoba wypada przez (boczne) drzwi
SPH 40	Osoba wypada przez tylnie drzwi w ostatnim wagonie pociągu
SPH 41	Pociąg rusza/ jedzie z otwartymi drzwiami (nienaruszona przestrzeń swobodna)
SPH 42	Osoba wpada w lukę między dwoma wagonami
SPH 43	Pasażer wychyla się przez drzwi
SPH 44	Pasażer wychyla się przez okno
SPH 45	Pracownik obsługi pociągu wychyla się przez drzwi
SPH 46	Pracownik obsługi pociągu wychyla się przez okno
SPH 47	Członek personelu manewrowego pojazdu wychyla się na stopniu
SPH 48	Osoba spada/ schodzi w lukę między pojazdem a peronem
SPH 49	Osoba wypada/ wysiada z pociągu w miejscu, gdzie nie ma peronu
SPH 50	Osoba przewraca się w okolicy drzwi w czasie wsiadania i wysiadania pasażerów
SPH 51	Drzwi zamykają się, przytrzaskując osobę
SPH 52	Pociąg rusza w czasie wsiadania i wysiadania pasażerów
SPH 53	Możliwość zranienia osoby w pociągu
SPH 54	Zagrożenia związane z pożarem/ wybuchem (w/ przy pociągu) – kategoria wypadku, skutek SPH 55, SPH 56)
SPH 55	Niewłaściwa temperatura (w pociągu)
SPH 56	Zatrucie/ uduszenie (w/ przy pociągu)
SPH 57	Śmiertelne porażenie prądem elektrycznym (w/ przy pociągu)
SPH 58	Osoba przewraca się na peronie (ale nie w czasie wsiadania i wysiadania pasażerów
SPH 59	Niewłaściwa temperatura (na peronie)
SPH 60	Zatrucie/ uduszenie (na peronie)
SPH 61	Śmiertelne porażenie prądem elektrycznym (na peronie)

European Railway Agency ● Marc LEFRANCQ, 120 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu