STANDARDY TECHNICZNE
SZCZEGÓŁOWE WARUNKI TECHNICZNE DLA BUDOWY INFRASTRUKTURY KOLEJOWEJ CENTRALNEGO PORTU KOMUNIKACYJNEGO - WYTYCZNE PROJEKTOWANIA

TOM XVIII
WYMAGANIA W ZAKRESIE SPÓJNOŚCI BEZPIECZEŃSTWA, OCHRONY I CYBERBEZPIECZEŃSTWA

Wersja 3.0.0

[strona intencjonalnie pozostawiona pusta]

Zestawienie tomów współtworzących szczegółowe warunki techniczne dla budowy infrastruktury kolejowej Centralnego Portu Komunikacyjnego:

Tom A	Wprowadzenie do standardów kolejowych CPK
Tom I.1	Droga szynowa – układy geometryczne
Tom I.2	Droga szynowa – konstrukcja obiektów budowlanych
Tom I.3	Droga szynowa – odwodnienie układu torowego
Tom I.4	Droga szynowa – skrajnia
Tom I.5	Droga szynowa – badania i projektowanie geotechniczne
Tom II.1	Sieć trakcyjna i zasilanie trakcyjne 2x25 kV 50 Hz AC
Tom II.2	Sieć trakcyjna i zasilanie trakcyjne 3 kV DC
Tom III.1	Obiekty inżynieryjne
Tom III.2	Tunele
Tom IV	Elektroenergetyka nietrakcyjna
Tom V.1	Drogi niepubliczne
Tom V.2	Drogi publiczne
Tom VI.1	Sterowanie ruchem kolejowym – wyposażenie podstawowe
Tom VI.2	Sterowanie ruchem kolejowym – Europejski System Sterowania Pociągiem ETCS
Tom VII.1	Łączność przewodowa i bezprzewodowa oraz transmisja danych
Tom VII.2	Teletechnika i telematyka
Tom VII.3	Detekcja stanów awaryjnych taboru (DSAT)
Tom VIII.1	Budynki stacji i dworców kolejowych
Tom VIII.2	Budynki techniczne
Tom VIII.3	Budowle
Tom VIII.4	Mała architektura
Tom IX	Środki minimalizujące oddziaływanie na środowisko
Tom X	Kolizje z sieciami zewnętrznymi
Tom XI	Kompatybilność elektromagnetyczna (EMC)
Tom XII	Osłona linii kolejowych
Tom XIII	Zaplecze techniczne
Tom XIV	Systemy wspomagania zdrowia oraz bezpieczeństwa osób i mienia
Tom XV	Osnowa geodezyjna
Tom XVI	Tabor kolejowy
Tom XVII	Systemy automatycznej odprawy bagażu
Tom XVIII	**Wymagania w zakresie spójności bezpieczeństwa, ochrony i cyberbezpieczeństwa** Definiuje wymagania dla dokumentowania i weryfikowania spójności bezpieczeństwa, ochrony i cyberbezpieczeństwa stosowane na różnych etapach realizacji infrastruktury kolejowej CPK, w szczególności dla koncepcji, projektów oraz realizacji bodowy infrastruktury kolejowej Centralnego Portu Komunikacyjnego.

[strona intencjonalnie pozostawiona pusta]

Wersjonowanie dokumentu „Szczegółowe warunki techniczne dla budowy infrastruktury kolejowej Centralnego Portu Komunikacyjnego; Tom XVIII; Wymagania w zakresie spójności bezpieczeństwa, ochrony i cyberbezpieczeństwa”:

wersja	zmiany
1.0.0	Opracowanie dokumentu
	Opracowanie zamknięto w dniu 29.04.2021 r.
1.1.0	Uwzględnienie istotnych i edycyjnych uwag z pisma CPK nr KRI/1901/2021/GB/25
	Opracowanie zamknięto w dniu 10.06.2021 r.
1.2.0	Uwzględnienie istotnych i edycyjnych uwag z pisma CPK nr KRI/2025/2021/NAB.1983/GB/25
	Opracowanie zamknięto w dniu 8.07.2021 r.
1.3.0	Uwzględnienie istotnych i edycyjnych uwag z pisma CPK nr KRI/2658/2021/25/GB
	Opracowanie zamknięto w dniu 5.08.2021 r.
2.0.0	Uwzględnienie uwag z konsultacji z rynkiem wykonawców
	Opracowanie zamknięto w dniu 8.07.2022 r.
3.0.0	Uwzględnienie uwag CPK z konsultacji z rynkiem wykonawców
	Opracowanie zamknięto w dniu 25.09.2023 r.

UWAGA: Przywołane w dokumencie akty prawne zostały wskazane na dzień opracowania wersji 1.0.0. Późniejsze zmiany uwzględniono tylko w przypadku zmian bezpośrednio wpływających na kluczowe parametry infrastruktury kolejowej CPK. Jednocześnie zwraca się uwagę, że użytkownicy tego dokumentu z mocy prawa zobowiązani są do stosowania dokumentów wiążących prawnie także wówczas, gdy niniejszy dokument wskazuje wcześniejszy stan prawny.

[strona intencjonalnie pozostawiona pusta]

1. Wprowadzenie

Niniejszy dokument stanowi część wielotomowych standardów kolejowych opracowanych przez Instytut Kolejnictwa na zlecenie spółki Centralny Port Komunikacyjny.

Tom A stanowi wprowadzenie do standardów kolejowych CPK. Tomy od I.1 do XVII zawierają wymagania dla rozwiązań technicznych infrastruktury kolejowej CPK. Spis tomów znajduje się na stronie 3 każdego tomu standardów kolejowych CPK. Niniejszy tom XVIII standardów kolejowych CPK definiuje zasady dokumentowania i weryfikowania spójności bezpieczeństwa, ochrony i cyberbezpieczeństwa.

Tom XVIII określa zasady dokumentowania i weryfikowania spójności bezpieczeństwa, ochrony i cyberbezpieczeństwa, które mają zastosowanie na różnych etapach realizacji prac, w szczególności dla koncepcji, projektów oraz realizacji budowy infrastruktury kolejowej Centralnego Portu Komunikacyjnego. Zasady te zdefiniowano w rozdziale 3.

W celu zapewnienia właściwego całościowego podejścia do bezpieczeństwa użytkowników niniejszego tomu, przed rozdziałem 2. pokazującym powiązania pomiędzy wymaganiami zasadniczymi a dokumentowaniem spójności bezpieczeństwa, ochrony i cyberbezpieczeństwa opisanym w rozdziale 3., w dwóch dodatkowych podrozdziałach rozdziału 1. omówiono poszczególne aspekty wymagania zasadniczego ‘bezpieczeństwo’ oraz kontekst dopuszczania rozwiązań technicznych na poziomie podsystemów strukturalnych. Rozdział 1.1. omawia poszczególne aspekty bezpieczeństwa rozumianego jako wymaganie zasadnicze ‘bezpieczeństwo’ czyli aspekty od 1.1.1. do 1.1.11. wymagania zasadniczego ‘bezpieczeństwo’, uwarunkowania ochrony czyli aspekty 1.1.12. oraz 1.1.13. wymagań ogólnych dla infrastruktury kolejowej CPK oraz uwarunkowania cyberbezpieczeństwa infrastruktury kolejowej CPK. Rozdział 1.2. wskazuje obowiązujące zasady potwierdzania spełnienia wymagania zasadniczego ‘bezpieczeństwo’, komplementarne do dokumentowania i weryfikowania bezpieczeństwa, ochrony i cyberbezpieczeństwa infrastruktury kolejowej CPK opisanego w rozdziale 3.

1.1. Bezpieczeństwo, ochrona i cyberbezpieczeństwo infrastruktury kolejowej CPK

Bezpieczeństwo, ochronę i cyberbezpieczeństwo w kontekście standardów kolejowych CPK należy rozumieć zgodnie z doprecyzowaniem odpowiednio w podrozdziałach 1.1.1., 1.1.2. i 1.1.3. Zawarte w tych podrozdziałach szerokie postrzeganie bezpieczeństwa transportu kolejowego realizowanego z wykorzystaniem infrastruktury kolejowej CPK nie ograniczające się do bezpieczeństwa ruchu kolejowego powinno być uwzględniane podczas opracowywania dokumentów, których charakter, zawartość i struktura zostały zdefiniowane w rozdziale 3.

1.1.1. Bezpieczeństwo

Bezpieczeństwo jako wymaganie zasadnicze w odniesieniu do systemu kolei oraz podsystemów współtworzących system kolei zostało zdefiniowane w załączniku III do Dyrektywy w sprawie interoperacyjności kolei [1]. Opis **wymagania zasadniczego ‘bezpieczeństwo’** został przytoczony za dyrektywą w rozdziale 2.1. Tomu A Standardów kolejowych CPK. **Wymaganie zasadnicze ‘bezpieczeństwo’** obejmuje zapewnienie:

a) bezpieczeństwa w przypadku awarii
   (patrz tom A, wymaganie zasadnicze 1.1.1.);

b) bezpiecznej współpracy koło–szyna z uwzględnieniem wpływu sił od taboru na tor (patrz tom A, wymaganie zasadnicze 1.1.2.);
c) bezpieczeństwa przy ponadnormatywnych obciążeniach konstrukcji (patrz tom A, wymaganie zasadnicze 1.1.3.);
d) zabezpieczeń przed pożarem, jak i skutkami ognia i dymu (patrz tom A, wymaganie zasadnicze 1.1.4.);
e) zabezpieczeń przed użyciem niezgodnie z przeznaczeniem (patrz tom A, wymaganie zasadnicze 1.1.5.);
f) zabezpieczeń przed nieuprawnionym dostępem oraz zapewnienie możliwości ewakuacji i dostępu dla służb ratunkowych (patrz tom A, wymaganie zasadnicze 1.1.6.);
g) bezpieczeństwa elektrycznego (patrz tom A, wymaganie zasadnicze 1.1.7.);
h) bezpiecznego i nieprzerwanego działania systemów sterowania ruchem kolejowym (patrz tom A, wymaganie zasadnicze 1.1.8.);
i) przepisów ruchowych oraz kwalifikacji personelu uwzględniających kwestie bezpieczeństwa (patrz tom A, wymaganie zasadnicze 1.1.9.);
j) wsparcia informatycznego bezpieczeństwa transportu kolejowego (patrz tom A, wymaganie zasadnicze 1.1.10.);
k) bezpiecznych instalacji technicznych i procedur w centrach utrzymania (patrz tom A, wymaganie zasadnicze 1.1.11.).

Spełnianie **wymagania zasadniczego 'bezpieczeństwo'** przez poszczególne podsystemy systemu kolejowego podlega weryfikacji WE (patrz rozdział 1.2.)

1.1.2. Ochrona

W procesie eksploatacji konieczne jest także zapewnienie szeroko rozumianej **ochrony** transportu, czyli bezpieczeństwa osób i mienia odpowiednimi środkami wspomagającymi ich ochronę. Dla ochrony życia, zdrowia i mienia stosuje się:

a) monitorowanie stref dostępnych publicznie i wspomaganie działań personelu (patrz tom A, **wymaganie ogólne w zakresie ochrony** 1.1.12.);
b) monitorowanie stref niedostępnych publicznie i wspomaganie działań personelu (patrz tom A, **wymaganie ogólne w zakresie ochrony** 1.1.13.);

Środki techniczne wspomagające ochronę to w szczególności: środki wspomagania ochrony zdrowia pasażerów, zabezpieczenia przed wandalizmem, zabezpieczenia przed terroryzmem, środki ochrony mienia, a także środki ochrony przed katastrofami oraz niekorzystnymi warunkami atmosferycznymi.

1.1.3. Cyberbezpieczeństwo

Cyberbezpieczeństwo, czyli „bezpieczeństwo sieci i systemów informatycznych", w odniesieniu do sieci i systemów informatycznych w tym systemów wykorzystywanych dla potrzeb transportu kolejowego zdefiniowane zostało w Dyrektywie w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych [2] następująco:

> „bezpieczeństwo sieci i systemów informatycznych" oznacza odporność sieci i systemów informatycznych, przy danym poziomie zaufania, na wszelkie działania naruszające dostępność, autentyczność, integralność lub poufność przechowywanych lub przekazywanych, lub przetwarzanych danych lub związanych z nimi usług oferowanych lub dostępnych poprzez te sieci i systemy informatyczne;
>
> *[zgodnie z art. 4 Dyrektywy 2016/1148]*

Tak zdefiniowane **cyberbezpieczeństwo** ma zastosowanie zarówno do systemów informatycznych wykorzystywanych dla potrzeb transportu kolejowego jak i do systemów eksploatacyjnych wykorzystywanych dla zapewnienia bezpieczeństwa ruchu i dla ochrony transportu kolejowego.

Systemy i rozwiązania informatyczne, systemy IT (ang. Information Technologies), obejmują zarówno IT wspomagające zarządcę infrastruktury w realizacji zadań ogólnych i działań gospodarczych (np. systemy zarządzania personelem czy majątkiem, fakturowania, pracy grupowej z wykorzystaniem narzędzi IT) jak i w realizacji zadań związanych z transportem kolejowym (np. systemy do tworzenia rozkładów jazdy). Systemy i rozwiązania eksploatacyjne, systemy OT (ang. Operational Technologies), obejmują zarówno elektroniczne komponenty systemów sterowania ruchem kolejowym i systemów bezpiecznej kontroli jazdy oraz łączności eksploatacyjnej (np. nastawnice komputerowe czy Europejski System Sterowania Pociągiem ETCS) jak i systemy i rozwiązania zapewniające ochronę transportu a nie bezpieczeństwo ruchu.

Zarówno systemy IT jak i systemy OT korzystają z tego samego typu mechanizmów podnoszących bezpieczeństwo sieci i systemów informatycznych. Należą do nich:

- zabezpieczenia organizacyjne i proceduralne, w tym systemy zarządzania bezpieczeństwem informacji [3] oraz systemy nadawania i odbierania praw dostępu;
- systemy i rozwiązania zapewniające ciągłość działania systemów IT i systemów OT, w tym systemy tworzenia i wykorzystywania kopii zapasowych, nadmiarowości sprzętowe i programowe, zabezpieczenia centrów przetwarzania danych przed utratą zasilania czy pożarem;
- zabezpieczenia technologiczne, w tym systemy uwierzytelniania, ochrona przed złośliwym oprogramowaniem oraz systemy kontroli procesów przetwarzania i transmisji danych; a także
- zabezpieczenia fizyczne, w tym zdalnie nadzorowane zamki, systemy monitoringu wizyjnego oraz inne systemy wspomagające ochronę fizyczną.

Standardy techniczne dla infrastruktury kolejowej CPK ze względu na ich zakres i przeznaczenie obejmują wymagania dla systemów OT zarówno zapewniających bezpieczeństwo ruchu kolejowego jak i wspomagających ochronę transportu.

Zarządzanie bezpieczeństwem informacji i ochrona systemów IT będą musiały być wdrożone przez zarządcę infrastruktury zgodnie z normami serii PN-EN ISO/IEC 27000, w tym w szczególności zgodnie z normą PN-EN ISO/IEC 27001 [6] definiującą wymagania dla systemu zarządzania bezpieczeństwem informacji. Przyjęte w tym zakresie regulacje wewnętrzne mogą wymagać stosowania przez cyfrowe systemy eksploatacyjne zapewniające bezpieczeństwo i/lub ochronę określonych mechanizmów podnoszących bezpieczeństwo sieci i systemów np. określonej procedury logowania się przez operatorów czy określonego sposobu gromadzenia logów czy tworzenia kopii zapasowych i odtwarzania systemów i danych z kopii po awariach.

Osobną kwestią jest stosowanie, tam gdzie jest to zasadne, wymagania powiązania systemów OT, tak jak i systemów IT z systemami podnoszącymi bezpieczeństwo sieci i systemów informatycznych zgodnie z zasadami zarządzania bezpieczeństwem informacji oraz zgodnie z zaleceniami branżowymi np. zaleceniami ISAC-Kolej.

1.2. Potwierdzenie spełnienia wymagania zasadniczego bezpieczeństwo a spójność bezpieczeństwa, ochrony i cyberbezpieczeństwa

Dla potwierdzenia spełnienia wymagań zasadniczych zdefiniowanych w dyrektywie [1], w tym wymagania zasadniczego ‘bezpieczeństwo’, wymaga się:

a) aby wszystkie typy składników interoperacyjności przewidziane do zabudowy w infrastrukturze kolejowej CPK posiadały certyfikaty zgodności WE wydane przez właściwe jednostki notyfikowane dla poszczególnych rozwiązań technicznych.
b) aby wszystkie składniki interoperacyjności zabudowywane w infrastrukturze kolejowej CPK były dostarczane wraz z indywidualnymi deklaracjami zgodności WE wydanymi przez ich producentów lub były objęte zbiorczymi deklaracjami zgodności WE wydanymi przez ich producentów.
c) aby wszystkie typy budowli i urządzeń podlegające pod wymóg uzyskania świadectwa typu przewidziane do zabudowy w infrastrukturze kolejowej CPK posiadały świadectwa typu wydane przez Prezesa UTK dla poszczególnych rozwiązań technicznych.
d) aby wszystkie budowle i urządzenia podlegające pod wymóg uzyskania świadectwa typu zabudowywane w infrastrukturze kolejowej CPK były dostarczane wraz z indywidualnymi deklaracjami zgodności z typem wydanymi przez ich producentów lub były objęte zbiorczymi deklaracjami zgodności z typem wydanymi przez ich producentów.
e) aby wszystkie projekty wykonawcze podsystemów strukturalnych (podsystemów „Infrastruktura", „Energia" oraz „Sterowanie – urządzenia przytorowe") współtworzących infrastrukturę kolejową CPK posiadały pośrednie potwierdzenia weryfikacji WE na etapie projektu wydane przez właściwe jednostki notyfikowane dla poszczególnych projektów podsystemów.
f) aby wszystkie podsystemy strukturalne (podsystemy „Infrastruktura", „Energia" oraz „Sterowanie – urządzenia przytorowe") współtworzące infrastrukturę kolejową CPK posiadały certyfikaty weryfikacji WE wydane przez właściwe jednostki notyfikowane dla poszczególnych podsystemów.
g) aby wszystkie podsystemy strukturalne (podsystemy „Infrastruktura", „Energia" oraz „Sterowanie – urządzenia przytorowe") współtworzące infrastrukturę kolejową CPK posiadały deklaracje weryfikacji WE wydane przez wykonawców poszczególnych podsystemów.
h) aby wszystkie podsystemy strukturalne (podsystemy „Infrastruktura", „Energia" oraz „Sterowanie – urządzenia przytorowe") współtworzące infrastrukturę kolejową CPK przed rozpoczęciem ich eksploatacji uzyskały zezwolenia na przekazanie do eksploatacji wydane przez Prezesa UTK.

Przywołane powyżej wymagania wynikają z przepisów prawa z wyjątkiem pośrednich potwierdzeń weryfikacji WE na etapie projektu, które zgodnie z zapisami prawa pozostają opcjonalne, ale są wymagane kontraktowo przez spółkę Centralny Port Komunikacyjny.

Certyfikaty i deklaracje zgodności WE oraz świadectwa typu i deklaracje zgodności z typem a także pośrednie potwierdzenia weryfikacji WE i certyfikaty weryfikacji WE i deklaracje weryfikacji WE potwierdzają zgodność z wymaganiami zasadniczymi, w tym z **wymaganiem zasadniczym 'bezpieczeństwo'** (wymagania zasadnicze od 1.1.1. do 1.1.11.). Potwierdzenia te uznaje się za niewystarczające w odniesieniu do spójności bezpieczeństwa, ochrony i cyberbezpieczeństwa infrastruktury kolejowej CPK ponieważ wymaganie zasadnicze 'bezpieczeństwo' nie ma zastosowania do części rozwiązań wspierających ochronę (**wymagań ogólnych w zakresie ochrony** 1.1.12. i 1.1.13. obowiązujących dla infrastruktury kolejowej CPK) oraz do rozwiązań wspierających **cyberbezpieczeństwo**.

1.3. Definicje użytych określeń

1) **Bezpieczeństwo** – brak niedopuszczalnego ryzyka [7].
2) **Cyberbezpieczeństwo** – odporność sieci i systemów informatycznych, przy danym poziomie zaufania, na wszelkie działania naruszające dostępność, autentyczność, integralność lub

poufność przechowywanych lub przekazywanych, lub przetwarzanych danych lub związanych z nimi usług oferowanych lub dostępnych poprzez te sieci i systemy informatyczne [2].

3) **Dowód bezpieczeństwa** – udokumentowane wykazanie, że wyrób (np. system, podsystem lub urządzenie) jest zgodny z wyspecyfikowanymi wymaganiami bezpieczeństwa [7].
4) **Dowód spójności bezpieczeństwa, ochrony i cyberbezpieczeństwa** – dokument opracowany przez **wykonawcę** dla koncepcji, projektu lub realizacji, zgodny z wymaganiami rozdziału 3.1. niniejszego dokumentu, podlegający ocenie zgodnie z wymaganiami rozdziału 3.2 niniejszego dokumentu.
5) **Wewnętrzny zespół odpowiedzialny za bezpieczeństwo** – część struktury wewnętrznej, która koordynuje wewnętrzne procesy w spółce CPK w odniesieniu do bezpieczeństwa.
6) **Kompetentna niezależna jednostka inspekcyjna** – jednostka posiadającą akredytację Polskiego Centrum Akredytacji dla jednostki oceniającej ryzyko dla pięciu podsystemów strukturalnych – podsystemów „Infrastruktura", „Energia", „Sterowanie – urządzenia przytorowe" oraz „Tabor" i „Sterowanie – urządzenia pokładowe" prowadząca weryfikację '**dowodu spójności bezpieczeństwa, ochrony i cyberbezpieczeństwa**'.
7) **Ryzyko** – kombinacja oczekiwanej częstotliwości występowania szkody oraz oczekiwanej dotkliwości takiej szkody [7].
8) **Wykonawca** – podmiot opracowujący koncepcję lub projekt względnie budujący infrastrukturę kolejową CPK lub zabudowujący urządzenia współtworzące infrastrukturę kolejową CPK lub wprowadzający zmiany w koncepcji, projekcie lub infrastrukturze CPK lub jej wyposażeniu.
9) **Wymagania ogólne w zakresie ochrony** – wymagania 1.1.12 i 1.1.13. podane w Tomie A standardów kolejowych CPK (zdefiniowane jako wymagania ogólne dla potrzeb infrastruktury kolejowej CPK).
10) **Wymaganie zasadnicze 'bezpieczeństwo'** – wymagania od 1.1.1. do 1.1.11. podane w Tomie A standardów kolejowych CPK (zaczerpnięte z załącznika III do dyrektywy w sprawie interoperacyjności [1]).

[pozostałą część strony intencjonalnie pozostawiono pustą]

[strona intencjonalnie pozostawiona pusta]

2. Wymagania zasadnicze, podstawowe i ogólne dla infrastruktury kolejowej CPK

Każdy Tom branżowy zawiera zestawienie tabelaryczne definiujące powiązanie szczegółowych warunków technicznych dla budowy infrastruktury kolejowej CPK zdefiniowanych w ramach danego tomu branżowego z wymaganiami zasadniczymi, podstawowymi i ogólnymi podanymi w rozdziale 2.1 Tomu A. Niniejszy Tom XVIII uwzględnia wymagania od 1.1.1. do 1.1.11. wymagania zasadniczego „bezpieczeństwo" oraz związane z bezpieczeństwem wymagania ogólne dla infrastruktury kolejowej CPK czyli wymagania 1.1.12. i 1.1.13. ponieważ dla rozwiązań technicznych zapewniających spełnienie tych wymagań zapewnić należy spójność bezpieczeństwa, ochrony i cyberbezpieczeństwa czyli upraszczając właściwą odporność na awarie na wandalizm i terroryzm oraz cyberzagrożenia.

Wszystkie wymagania zasadnicze podlegają weryfikacji na poziomie składników interoperacyjności oraz podsystemów strukturalnych zgodnie z opisem w rozdziale 1.2. Wymagania podstawowe podlegają weryfikacji dla wyrobów, materiałów i obiektów budowlanych. Konieczność uzyskiwania zezwoleń na eksploatację dla podsystemów strukturalnych i pozwoleń na użytkowanie dla obiektów budowlanych gwarantuje odpowiednio dochowanie wszystkich właściwych wymagań zasadniczych i wszystkich właściwych wymagań podstawowych. Zezwolenia takie nie uwzględniają jednak ani wymagań dotyczących ochrony ani cyberbezpieczeństwa ani spójności bezpieczeństwa, ochrony i cyberbezpieczeństwa.

Tabela 1. Powiązanie szczegółowych wymagań zdefiniowanych w zakresie dokumentowania i weryfikowania spójności bezpieczeństwa, ochrony i cyberbezpieczeństwa z wymaganiami zasadniczymi, podstawowymi i ogólnymi dla infrastruktury kolejowej CPK

podrozdział niniejszego tomu definiujący szczegółowe warunki techniczne	wymagania zasadnicze (dyrektywa w sprawie interoperacyjności kolei)						wymagania podstawowe	wymagania ogólne dla infrastruktury kolejowej CPK			
	1.1. bezpieczeństwo	1.2. niezawodność i dostępność	1.3. zdrowie	1.4. ochrona środowiska naturalnego	1.5. zgodność techniczna	1.6. dostępność	2.1. nośność i stateczność 2.2. bezpieczeństwo pożarowe 2.3. higiena, zdrowie i środowisko 2.4. bezpieczeństwo użytkowania i dostępność 2.5. ochrona przed hałasem 2.6. oszczędność energii i izolacyjność cieplna 2.7. zrównoważone wykorzystanie zasobów nat.	3.1. ukierunkowanie na potrzeby gospodarki	3.2. ukierunkowanie na potrzeby pasażera	3.3. ukierunkowanie na potrzeby przewoźników	3.4. zgodność z infrastrukturą kolejową połączoną z infrastrukturą kolejową CPK
3.1.1	1.1.1. 1.1.4. 1.1.5. 1.1.6. 1.1.7. 1.1.8. 1.1.10. 1.1.11. 1.1.12. 1.1.13.	-	-	-	-	-	-	-	-	-	-
3.1.2		-	-	-	-	-	-	-	-	-	-
3.1.3		-	-	-	-	-	-	-	-	-	-
3.1.4		-	-	-	-	-	-	-	-	-	-
3.1.5		-	-	-	-	-	-	-	-	-	-
3.1.6		-	-	-	-	-	-	-	-	-	-
3.1.7		-	-	-	-	-	-	-	-	-	-
3.2		-	-	-	-	-	-	-	-	-	-

Wymagania ujęte w rozdziałach dedykowanych dokumentowaniu i weryfikacji poziomów spójności bezpieczeństwa, ochrony i cyberbezpieczeństwa odnoszą się do wybranych dziesięciu aspektów wymagania zasadniczego bezpieczeństwo, z których osiem sformułowano w dyrektywie w sprawie interoperacyjności kolei [1] a dwa ostatnie 1.1.12. oraz 1.1.13. sformułowano dla potrzeb infrastruktury kolejowej CPK. Jednocześnie zaznaczyć należy, że wymaga się, aby wszystkie wymagania zasadnicze, w tym wszystkie aspekty ujęte w wymaganiu zasadniczym bezpieczeństwo były potwierdzane odpowiednimi certyfikatami i deklaracjami. Podstawowe informacje w tym zakresie, zgodnie z wymaganiami prawa, podano w rozdziale 1.2.

Wymagania zasadnicze 1.1.2. (wpływ sił od taboru na tor oraz współpraca koło–szyna), 1.1.3. (bezpieczeństwo konstrukcji) i 1.1.9. (przepisy ruchowe oraz kwalifikacje personelu) zapewniane są poprzez właściwą konstrukcję układów biegowych taboru i geometrię torów, właściwą konstrukcję pudeł pojazdów oraz obiektów inżynieryjnych uwzględniającą ponadnormatywne obciążenia oraz doskonalenie przepisów ruchowych i szkolenie personelu. Wymagania te są niezależne od wymagań dla rozwiązań eksploatacyjnych zapewniających bezpieczeństwo ruchu i wspomagających ochronę transportu, dla których, zgodnie z wymaganiami niniejszego tomu, potwierdzona powinna być spójność bezpieczeństwa, ochrony i cyberbezpieczeństwa.

Zakres dokumentów opracowywanych a następnie weryfikowanych zgodnie z wymaganiami zawartymi w niniejszym tomie standardów kolejowych CPK obejmuje systemy OT i systemy IT współpracujące z systemami OT, które gromadzą, przechowują, przetwarzają, udostępniają lub transmitują dane mające wpływ na bezpieczeństwo i/lub ochronę a także wykorzystywane przez nie do celów eksploatacyjnych sieci i systemy informatyczne, których bezpieczeństwo może zostać naruszone. Poszczególne tomy standardów na końcu rozdziałów 2. przywołują i omawiają definicję cyberbezpieczeństwa, jako komplementarną do wymagań zasadniczych, wymagań podstawowych i wymagań ogólnych dla infrastruktury kolejowej CPK wskazując także czy zakres merytoryczny danego tomu obejmuje: sieci i systemy informatyczne, których bezpieczeństwo może zostać naruszone i/lub rozwiązania techniczne, które gromadzą, przechowują, przetwarzają, udostępniają lub transmitują dane mające wpływ na bezpieczeństwo i/lub ochronę.

[pozostałą część strony intencjonalnie pozostawiono pustą]

3. Szczegółowe wymagania w zakresie dokumentowania i weryfikowania spójności bezpieczeństwa, ochrony i cyberbezpieczeństwa infrastruktury kolejowej CPK

Zasady dokumentowania i weryfikowania spójności bezpieczeństwa, ochrony i cyberbezpieczeństwa zdefiniowane w rozdziale 3 niniejszego dokumentu łącznie stanowią przyjętą metodę weryfikowania funkcjonalnej kompletności i adekwatności bezpieczeństwa, ochrony oraz cyberbezpieczeństwa infrastruktury kolejowej CPK.

Rozdział 3.1. definiuje zasady dokumentowania spójności bezpieczeństwa, ochrony i cyberbezpieczeństwa przez **wykonawców** opracowujących koncepcje i projekty infrastruktury kolejowej CPK oraz **wykonawców** realizujących budowy i wprowadzających zmiany techniczne mające wpływ na bezpieczeństwo, ochronę lub cyberbezpieczeństwo infrastruktury kolejowej CPK.

Rozdział 3.2. definiuje zasady weryfikowania spójności bezpieczeństwa, ochrony i cyberbezpieczeństwa przez wewnętrzny zespół odpowiedzialny za bezpieczeństwo oraz **kompetentną niezależną jednostkę inspekcyjną**.

Niezależnie tych zasad obowiązuje także Ustawa o krajowym systemie cyberbezpieczeństwa [5].

3.1 Zasady dokumentowania spójności bezpieczeństwa, ochrony i cyberbezpieczeństwa infrastruktury kolejowej CPK

Niniejszy rozdział podaje zasady dokumentowania spójności bezpieczeństwa, ochrony i cyberbezpieczeństwa przez **wykonawców** opracowujących koncepcje i projekty infrastruktury kolejowej CPK oraz **wykonawców** realizujących budowy i wprowadzających zmiany techniczne mające wpływ na bezpieczeństwo, ochronę lub cyberbezpieczeństwo infrastruktury kolejowej CPK.

3.1.1. Wymagania ogólne dla dowodów spójności bezpieczeństwa, ochrony i cyberbezpieczeństwa

Dla koncepcji, projektów oraz realizacji infrastruktury kolejowej CPK wymaga się opracowania przez **wykonawcę** '**dowodu spójności bezpieczeństwa, ochrony i cyberbezpieczeństwa**' oraz uzyskania raportu z niezależnej oceny takiego dowodu.

Wymaga się, aby '**dowód spójności bezpieczeństwa, ochrony i cyberbezpieczeństwa**':

a) uwzględniał uszkodzenia losowe i uszkodzenia systematyczne oraz potwierdzał zastosowanie zabezpieczeń wskazanych w normach [7, 8, 9, 10, 11] jako właściwe dla poziomów nienaruszalności bezpieczeństwa przypisanych poszczególnym rozwiązaniom technicznym zgodnie z zasadami wskazanymi w tych normach;
b) obejmował rozwiązania techniczne zapewniające funkcjonalną kompletność i adekwatność bezpieczeństwa technicznego, bezpieczeństwa życia, zdrowia i mienia oraz cyberbezpieczeństwa w przypadkach awarii oraz nieuprawnionych ingerencji, w tym cyberataków;
c) był podzielony na analizę zabezpieczeń technicznych związanych z zapewnieniem bezpieczeństwa ruchu udokumentowaną zgodnie z wymaganiami zawartymi w rozdziale 3.1.2 oraz analizę zabezpieczeń technicznych związanych z zapewnieniem ochrony transportu czyli zapewnieniem odpowiedniego poziomu bezpieczeństwa osób i mienia udokumentowaną zgodnie z wymaganiami zawartymi w rozdziale 3.1.3.;

d) uwzględniał zarówno dla zabezpieczeń technicznych związanych z zapewnieniem bezpieczeństwa ruchu pojazdów jak i zabezpieczeń technicznych związanych z zapewnieniem ochrony transportu zabezpieczenia przed cyberberzagrożeniami i dokumentował je zgodnie z wymaganiami zawartymi w rozdziale 3.1.4.
e) określał poziom spójności bezpieczeństwa, ochrony i cyberbezpieczeństwa zgodnie z wymaganiami zawartymi w rozdziale 3.1.5.

Wykonawcy koncepcji infrastruktury kolejowej CPK powinni wraz z koncepcją przedłożyć '**dowód spójności bezpieczeństwa, ochrony i cyberbezpieczeństwa**' infrastruktury zgodnej z proponowaną koncepcją, chyba że zapisy umowy, ze względu na charakter koncepcji, wprost przesądzają, że opracowanie '**dowodu spójności bezpieczeństwa, ochrony i cyberbezpieczeństwa**' nie jest wymagane.

Wykonawcy projektów infrastruktury kolejowej CPK powinni wraz z projektami przedłożyć pośrednie potwierdzenia weryfikacji WE na etapie projektu oraz '**dowód spójności bezpieczeństwa, ochrony i cyberbezpieczeństwa**' infrastruktury zgodnej z proponowanymi projektami.

Wykonawcy realizujący budowę infrastruktury kolejowej CPK powinni wraz z deklaracjami weryfikacji WE i certyfikatami weryfikacji WE przedłożyć '**dowód spójności bezpieczeństwa, ochrony i cyberbezpieczeństwa**' infrastruktury kolejowej CPK objętej deklaracjami i certyfikatami weryfikacji WE.

Wykonawcy wprowadzający zmiany w infrastrukturze kolejowej CPK także powinni przedkładać '**dowody spójności bezpieczeństwa, ochrony i cyberbezpieczeństwa**' infrastruktury CPK zgodnej z proponowaną(-ymi) zmianą(-ami), chyba że zapisy umowy, ze względu na charakter zmiany, wprost przesądzają, że opracowanie '**dowodu spójności bezpieczeństwa, ochrony i cyberbezpieczeństwa**' nie jest wymagane.

'**Dowód spójności bezpieczeństwa, ochrony i cyberbezpieczeństwa**' dla koncepcji lub projektu lub realizacji lub zmiany infrastruktury kolejowej CPK powinien obejmować pięć następujących rozdziałów:

1. Rozdział 1 - Wstęp wraz z określeniem systemu podlegającego ocenie (opis patrz podrozdział 3.1.1.)
2. Rozdział 2 - Analiza zabezpieczeń technicznych związanych z zapewnieniem bezpieczeństwa ruchu (opis patrz podrozdział 3.1.2.)
3. Rozdział 3 - Analiza zabezpieczeń technicznych związanych z zapewnieniem ochrony transportu (opis patrz podrozdział 3.1.3.)
4. Rozdział 4 - Analiza zabezpieczeń przed cyberzagrożeniami (opis patrz podrozdział 3.1.4.)
5. Rozdział 5 - Określenie poziomu bezpieczeństwa, ochrony i cyberbezpieczeństwa i poziomu ich spójności (opis patrz podrozdział 3.1.5. i 3.1.6.)
6. Rozdział 6 - Podsumowanie dowodu spójności bezpieczeństwa, ochrony i cyberbezpieczeństwa (opis patrz podrozdział 3.1.7.)

W ramach Rozdział 1 '**dowodu spójności bezpieczeństwa, ochrony i cyberbezpieczeństwa**' zdefiniować należy system podlegający ocenie, czyli infrastrukturę kolejową CPK, której dotyczy '**dowód spójności bezpieczeństwa, ochrony i cyberbezpieczeństwa**' oraz zdefiniować granice analizowanego systemu. Granice systemu należy uwzględnić przy opracowywaniu kolejnych rozdziałów.

W toku opracowywania '**dowodów spójności bezpieczeństwa, ochrony i cyberbezpieczeństwa**' **wykonawcy** mogą stosować upraszczanie systemów dla potrzeb oceny (patrz podrozdział 3.1.8) tylko

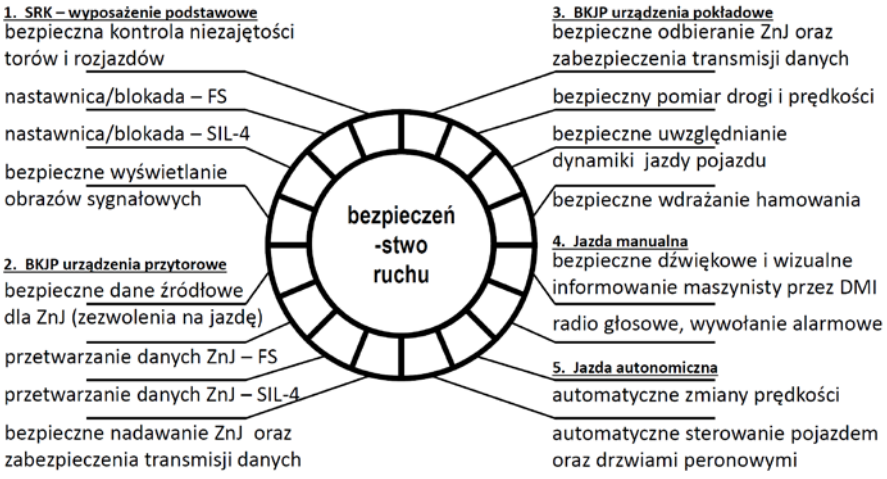
jeśli uzyskają stosowną zgodę od spółki CPK. Korespondencję w tym zakresie prowadzić należy z **wewnętrznym zespołem odpowiedzialnym za bezpieczeństwo**.

Dla każdego '**dowodu spójności bezpieczeństwa, ochrony i cyberbezpieczeństwa**' **wykonawcy** dla etapu projektowania oraz budowy i realizacji zmian powinni uzyskać pozytywną niezależną ocenę od **kompetentnej niezależnej jednostki inspekcyjnej** (patrz rozdział 3.2. niniejszego dokumentu). '**Dowody spójności bezpieczeństwa, ochrony i cyberbezpieczeństwa**' na etapie koncepcji mogą podlegać weryfikacji przez wewnętrzny zespół odpowiedzialny za bezpieczeństwo.

3.1.2. Analiza zabezpieczeń technicznych związanych z zapewnieniem bezpieczeństwa ruchu

Wymagania dla wyposażenia podstawowego w zakresie sterowania ruchem kolejowym zawiera Tom VI.1. Wymagania dla Europejskiego Systemu Sterowania Pociągiem ETCS zawiera Tom VI.2. Wymagania dla systemów łączności wykorzystywanych dla potrzeb sterowania ruchem kolejowym zawiera Tom VII.1. Uwzględniając fakt, że systemy techniczne posiadają ograniczoną niezawodność wymaga się, aby systemy sterowania ruchem i bezpiecznej kontroli jazdy same były systemami bezpiecznymi. Wyróżnia się przy tym dwie zasady: zasadę uszkodzony-bezpieczny - zasadę FS (ang. fail-safe) oraz zasadę SIL-4 narzucającą stosowanie dla rozwiązań elektronicznych zabezpieczeń gwarantujących czwarty poziom nienaruszalności bezpieczeństwa (ang. Safety Integrity Level) dla uszkodzeń losowych i uszkodzeń systematycznych. Stosowania norm definiujących wymagania dla niezawodności, dostępności, podatności utrzymaniowej i bezpieczeństwa [7, 8, 9, 10, 11] dla systemów sterowania ruchem kolejowym i bezpiecznych systemów kontroli jazdy wykorzystujących elektroniczne Zezwolenia na Jazdę (dalej **ZnJ**) wymagają już zapisy Tomów VI.1 oraz VI.2.

Analiza zabezpieczeń technicznych związanych z zapewnieniem bezpieczeństwa ruchu powinna opierać się na **referencyjnym modelu funkcjonalnym** (dalej **RMF**) przedstawionym na Rysunku XVIII.1.



Rysunek. XVIII.1. Referencyjny model funkcjonalny
zabezpieczeń technicznych związanych z bezpieczeństwem ruchu

W modelu RMF zostało wyróżnionych szesnaście czynników obejmujących funkcjonalności wpływające na bezpieczeństwo. Przywołują one zasady FS oraz SIL-4, a także funkcjonalności systemów sterowania i bezpiecznej kontroli jazdy kluczowe z punktu widzenia bezpieczeństwa eksploatacji. Są to następujące czynniki:

RMF-b01 – bezpieczna kontrola niezajętości odcinków izolowanych i odstępów blokowych,

RMF-b02 – stosowanie zasady FS przez systemy sterowania ruchem kolejowym – przez nastawnice stacyjne, blokady liniowe oraz systemy zabezpieczenia przejazdów kolejowo-drogowych,
RMF-b03 – stosowanie zasady SIL-4 przez systemy sterowania ruchem kolejowym – przez nastawnice stacyjne, blokady liniowe oraz systemy zabezpieczenia przejazdów kolejowo-drogowych,
RMF-b04 – bezpieczne wyświetlanie obrazów sygnałowych na sygnalizatorach świetlnych,
RMF-b05 – bezpieczne pobieranie danych źródłowych dla definiowania elektronicznych zezwoleń na jazdę ZnJ przekazywanych w formie cyfrowej z urządzeń przytorowych do urządzeń pokładowych,
RMF-b06 – stosowanie zasady FS przez systemy przetwarzania danych źródłowych w zezwolenia na jazdę ZnJ przekazywane do urządzeń pokładowych,
RMF-b07 – stosowanie zasady SIL-4 przez systemy przetwarzania danych źródłowych w zezwolenia na jazdę ZnJ przekazywane do urządzeń pokładowych,
RMF-b08 – bezpieczna transmisja danych, w tym wysyłanie zezwoleń na jazdę ZnJ,
RMF-b09 – bezpieczna transmisja danych, w tym odbieranie zezwoleń na jazdę ZnJ,
RMF-b10 – bezpieczny pomiar drogi przejechanej przez pociąg od punktu referencyjnego, którego odległość od końca zezwolenia ZnJ jest znana, oraz bezpieczny pomiar prędkości, z jaką porusza się pociąg,
RMF-b11 – bezpieczne uwzględnianie dynamiki jazdy pociągu na potrzeby inicjowania interwencji systemu bezpiecznej kontroli jazdy,
RMF-b12 – bezpieczne wdrażanie hamowania z uwzględnieniem hamowania służbowego oraz hamowania nagłego,
RMF-b13 – bezpieczne generowanie sygnałów dźwiękowych i wizualnych w kabinie maszynisty oraz informowanie maszynisty poprzez sygnalizację kabinową,
RMF-b14 – zapewnienie głosowego połączenia radiowego pomiędzy służbą ruchu i personelem pokładowym, w szczególności pomiędzy dyżurnym ruchu i maszynistą, oraz możliwości bezpiecznego generowania wywołań alarmowych,
RMF-b15 – bezpieczne automatyczne dostosowywanie prędkości do zezwolenia ZnJ,
RMF-b16 – bezpieczne automatyczne sterowanie pozostałymi systemami pokładowymi, w tym sterowanie pantografem, wyłącznikiem głównym, drzwiami w pojeździe, oraz bezpieczne automatyczne sterowanie drzwiami peronowymi.

Szesnaście czynników, grup funkcjonalności, wpływających na bezpieczeństwo ruchu uwzględnionych w modelu RMF połączono w pięć grup. Są to następujące grupy czynników:
RMF-GB-01 – funkcjonalności przytorowych systemów sterowania od kontroli niezajętości do wyświetlania obrazów sygnałowych na sygnalizatorach świetlnych (RMF-b01 ÷ RMF-b04),
RMF-GB-02 – funkcjonalności przytorowych urządzeń systemów bezpiecznej kontroli jazdy pociągu od obrazów sygnałowych do wysyłania elektronicznych zezwoleń ZnJ (RMF-b05 ÷ RMF-b08),
RMF-GB-03 – funkcjonalności pokładowych urządzeń systemów bezpiecznej kontroli jazdy pociągu od odebrania zezwolenia ZnJ do interwencyjnego wdrażania hamowania (RMF-b09 ÷ RMF-b12),
RMF-GB-04 – funkcjonalności wspierające manualne prowadzenie pociągów przez maszynistów w oparciu o obrazy sygnałowe na sygnalizatorach świetlnych przy wykorzystaniu radia (RMF-b13 ÷ RMF-b14),
RMF-GB-05 – funkcjonalności automatycznego prowadzenia pociągu zastępujące maszynistę w przyspieszaniu i hamowaniu oraz obsłudze innych urządzeń pokładowych i drzwi peronowych (RMF-b15 ÷ RMF-b16).

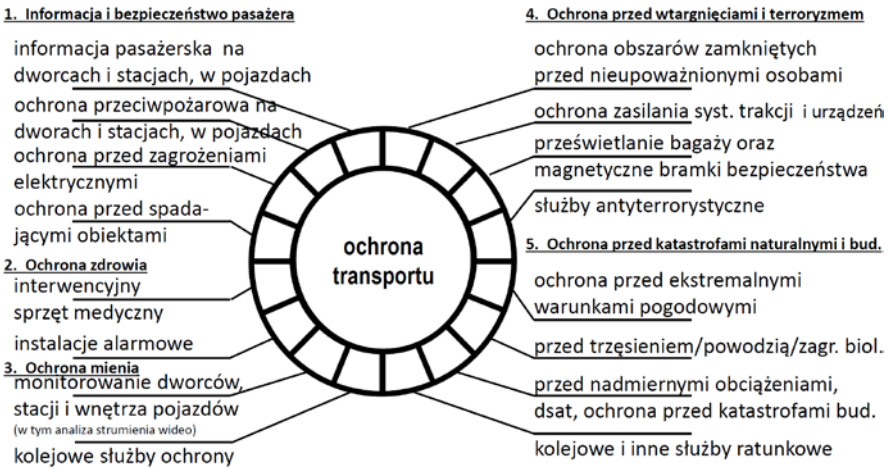
Rozdział 2 '**dowodu spójności bezpieczeństwa, ochrony i cyberbezpieczeństwa**' dedykowany analizie zabezpieczeń technicznych związanych z zapewnieniem bezpieczeństwa ruchu powinien być

podzielony na szesnaście podrozdziałów dedykowanych poszczególnym czynnikom, tak aby pola modelu RMF mogły zostać wykorzystane do przedstawienia poziomu zabezpieczenia np. przy wykorzystaniu odcieni szarości lub kolorów.

3.1.3. Analiza zabezpieczeń technicznych związanych z zapewnieniem ochrony transportu

Wymagania dla teletechniki i telematyki, w tym informacji pasażerskiej zawiera Tom VII.2. Wymagania dla detekcji stanów awaryjnych taboru (dalej **dsat**) zawiera Tom VII.3. Wymagania dla systemów wspomagania zdrowia oraz bezpieczeństwa osób i mienia zawiera Tom XIV. Także te systemy techniczne posiadają ograniczoną niezawodność, a ich uszkodzenia mogą negatywnie wpływać na bezpieczeństwo. Niestety dla tych systemów prawo nie wymaga stosowania zasad FS czy SIL-4. Odpowiednie zabezpieczenie tych systemów jest jednak konieczne w świetle standardów kolejowych CPK i podlega udokumentowaniu zgodnie z zapisami niniejszego podrozdziału.

Analiza zabezpieczeń technicznych związanych z zapewnieniem ochrony transportu (Rozdział 3 '**dowodu spójności bezpieczeństwa, ochrony i cyberbezpieczeństwa**') powinna opierać się na **referencyjnym modelu funkcjonalnym** (dalej **RMF**) przedstawionym na Rysunku XVIII.2.



Rysunek. XVIII.2. Referencyjny model funkcjonalny
zabezpieczeń technicznych związanych z ochroną transportu

W modelu RMF wyróżnionych zostało szesnaście czynników obejmujących funkcjonalności wpływające na bezpieczeństwo życia, zdrowia i mienia. Uwzględniają one zarówno wykorzystywanie służb ochrony w przypadkach losowych dotyczących pojedynczych osób, jak i ochronę w przypadkach wystąpienia kumulacji zagrożeń i obejmują przeciwdziałanie zagrożeniom, ograniczanie ich eskalacji, ewakuację, udzielanie pomocy czy zabezpieczanie miejsc ich wystąpienia. Są to następujące czynniki:

- RMF-o01 – zapewnienie informacji pasażerskiej na stacjach i w pociągach,
- RMF-o02 – zapewnienie ochrony przeciwpożarowej na stacjach i w pociągach,
- RMF-o03 – zapewnienie ochrony przed porażeniem prądem elektrycznym,
- RMF-o04 – zapewnienie ochrony przed spadającymi obiektami,
- RMF-o05 – zapewnienie interwencyjnego sprzętu medycznego oraz urządzeń i systemów wspierających dostępność transportu kolejowego dla osób o ograniczonej sprawności ruchowej oraz osób na wózkach inwalidzkich,
- RMF-o06 – zapewnienie możliwości wzywania pomocy poprzez udostępnianie instalacji alarmowych i/lub wdrożenia hamowania przez pasażera,
- RMF-o07 – monitorowanie obszarów stacji i wnętrz pojazdów systemami wizyjnymi,

RMF-o08 – zapewnienie dostępności i warunków działania dla kolejowych służb ochrony oraz ich współpracy z innymi służbami ochrony, w tym koniecznych środków technicznych,
RMF-o09 – ochrona obszarów zamkniętych przed osobami nieupoważnionymi, w tym w szczególności dostępu do miejsc pracy osób odpowiedzialnych za bezpieczeństwo techniczne i prowadzenie ruchu kolejowego oraz systemów i urządzeń bezpieczeństwa technicznego i zasilania,
RMF-o10 – systemy wspomagania czujności służb ochrony, w tym w szczególności systemy bieżącej analizy strumieni wideo,
RMF-o11 – prześwietlanie bagaży oraz magnetyczne bramki bezpieczeństwa,
RMF-o12 – współpraca ze służbami antyterrorystycznymi, w tym konieczne środki techniczne,
RMF-o13 – ochrona przed ekstremalnymi warunkami pogodowymi,
RMF-o14 – ochrona przed trzęsieniami ziemi zarówno w obszarach aktywnych sejsmicznie, jak i w obszarach górniczych oraz ochrona przed powodzią, a także przed zagrożeniami biologicznymi,
RMF-o15 – wspieranie bezpieczeństwa poprzez śledzenie ładunków niebezpiecznych oraz pociągów z przekroczonym obciążeniem i przekroczoną skrajnią,
RMF-o16 – współpraca ze służbami ratunkowymi zarówno kolejowymi, wykorzystującymi w szczególności pociągi ratownictwa technicznego, jak i publicznymi, w tym zapewnienie koniecznych środków technicznych.

Szesnaście czynników, grup funkcjonalności, wpływających na ochronę transportu uwzględnionych w modelu RMF połączono w pięć grup. Są to następujące grupy czynników:
RMF-GO-01 – funkcjonalności dedykowane dla zapewnienia minimum bezpieczeństwa osób (RMF-o01 ÷ RMF-o04),
RMF-GO-02 – funkcjonalności dedykowane dla wspierania zdrowia oraz osób o ograniczonych możliwościach ruchowych i osób na wózkach inwalidzkich (RMF-o05 ÷ RMF-o06),
RMF-GO-03 – funkcjonalności dedykowane dla ochrony przed złodziejami i osobami agresywnymi oraz przed wandalizmem, a także współpracy kolejowych służb ochrony z innymi służbami ochrony (RMF-o07 ÷ RMF-o08),
RMF-GO-04 – funkcjonalności dedykowane dla ochrony przed terroryzmem oraz współpracy ze służbami antyterrorystycznymi (RMF-o09 ÷ RMF-o12),
RMF-GO-05 – funkcjonalności dedykowane dla ochrony przed katastrofami oraz współpracy ze służbami ratunkowymi (RMF-o13 ÷ RMF-o16).

Rozdział 3 **‘dowodu spójności bezpieczeństwa, ochrony i cyberbezpieczeństwa’** dedykowany analizie zabezpieczeń technicznych związanych z zapewnieniem ochrony transportu powinien być podzielony na szesnaście podrozdziałów dedykowanych poszczególnym czynnikom, tak aby pola modelu RMF mogły zostać wykorzystane do przedstawienia poziomu zabezpieczenia np. przy wykorzystaniu odcieni szarości lub kolorów.

3.1.4. Analiza zabezpieczeń przed cyberzagrożeniami

Zarówno zabezpieczenia techniczne związane z zapewnieniem bezpieczeństwa ruchu jak i zabezpieczenia techniczne związane z zapewnieniem ochrony transportu korzystają z przechowywania, przekazywania i przetwarzania danych.

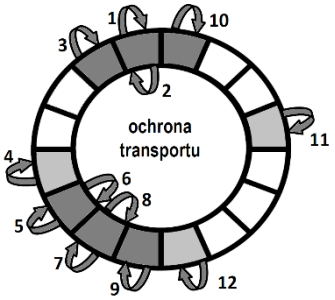
Rozdział 4 ‘**dowodu spójności bezpieczeństwa, ochrony i cyberbezpieczeństwa**’ dedykowany ‘Analizie zabezpieczeń przed cyberzagrożeniami’ powinien być podzielony na pięć następujących podrozdziałów:
4.1 Przechowywanie i przetwarzanie danych dla zapewnienia bezpieczeństwo ruchu,
4.2. Przechowywanie i przetwarzanie danych dla zapewnienia ochrony transportu,
4.3. Przekazywanie danych związanych z bezpieczeństwem ruchu,

4.4. Przekazywanie danych związanych z ochroną transportu,
4.5. Powiązanie systemów bezpieczeństwa ruchu i systemów ochrony transportu z mechanizmami podnoszenia bezpieczeństwa sieci i systemów informatycznych.

Podrozdziały dedykowane przechowywaniu i przetwarzaniu danych, podrozdziały 4.1. i 4.2., powinny obejmować precyzyjne odwołania do opisów rozwiązań technicznych. W przypadku zabezpieczeń technicznych związanych z zapewnieniem bezpieczeństwa ruchu (podrozdział 4.1.) do opisów w Rozdziale 2 '**dowodu spójności bezpieczeństwa, ochrony i cyberbezpieczeństwa**' oraz dokumentów szczegółowo definiujących rozwiązania techniczne. W przypadku zabezpieczeń technicznych związanych z zapewnieniem ochrony transportu (podrozdział 4.2.) do opisów w Rozdziale 3 '**dowodu spójności bezpieczeństwa, ochrony i cyberbezpieczeństwa**' oraz dokumentów szczegółowo definiujących rozwiązania techniczne. Dopuszcza się oparcie tych podrozdziałów wyłącznie na odwołaniach do opisów w Rozdziałach 1. i 2 '**dowodu spójności bezpieczeństwa, ochrony i cyberbezpieczeństwa**' oraz precyzyjnie wskazanych dokumentach szczegółowo definiujących rozwiązania techniczne.

Podrozdziały dedykowane przekazywaniu danych związanych z bezpieczeństwem ruchu oraz ochroną transportu, podrozdziały 4.3. i 4.4. '**dowodu spójności bezpieczeństwa, ochrony i cyberbezpieczeństwa**', powinny identyfikować wszystkie wykorzystywane w tym celu systemy transmisji i uwzględniać zarówno zabezpieczenie danych przed zmianą podczas przekazywania jak i ochronę przed wpływem pobierania danych na systemy, z których dane są pobierane. Podrozdział 4.3. powinien odwoływać się do dokumentów potwierdzających właściwe zastosowanie normy PN EN 50159 [11], lub wprost obejmować stosowne dowody. Podrozdział 4.4., powinien odwoływać się do tej normy jeśli wymagają tego zapisy właściwego tomu standardów CPK.

Systemy transmisji opisane w podrozdziałach 4.3. oraz 4.4. '**dowodu spójności bezpieczeństwa, ochrony i cyberbezpieczeństwa**' powinny zostać przedstawione na modelach RMF z rozdziałów dedykowanych zabezpieczeniom technicznym bezpieczeństwa ruchu i ochrony transportu przy wykorzystaniu strzałek blokowych, tak aby pola strzałek mogły zostać wykorzystane do przedstawienia poziomu zabezpieczenia np. przy wykorzystaniu odcieni szarości lub kolorów. Obok każdej strzałki reprezentującej system transmisji umieszczony powinien być odnośnik na przykład w postaci numeru. Przykładowe zobrazowanie dla transmisji dla potrzeb ochrony transportu przedstawiono na Rysunku XVIII.3.



Rysunek. XVIII.3. Przykład zobrazowania systemów transmisji
z wykorzystaniem referencyjnego modelu funkcjonalnego
dla zabezpieczeń technicznych związanych z ochroną transportu

Podrozdział 4.5. '**dowodu spójności bezpieczeństwa, ochrony i cyberbezpieczeństwa**' powinien zawierać opis powiązania systemów bezpieczeństwa ruchu i systemów ochrony transportu z mechanizmami podnoszenia bezpieczeństwa sieci i systemów informatycznych. Uwzględnić należy wszelkie powiązania z wymaganiami systemu zarządzania bezpieczeństwem informacji wdrożonego przez zarządcę infrastruktury zgodnie z normą PN-EN ISO/IEC 27001 [6].

Szczególną uwagę należy zwrócić na:
- uwierzytelnianie użytkowników,
- pobieranie danych do celów monitorowania i/lub diagnostyki,
- tworzenie kopii zapasowych i odtwarzanie programów i danych z kopii.

3.1.5. Karty kontrolne bezpieczeństwa, ochrony i cyberbezpieczeństwa

Określenie poziomu spójności bezpieczeństwa, ochrony i cyberbezpieczeństwa dla zabezpieczeń technicznych związanych z bezpieczeństwem ruchu jak i zabezpieczeń technicznych związanych z ochroną transportu powinno opierać się na pytaniach kontrolnych zdefiniowanych dla grup czynników wpływających na bezpieczeństwo ruchu i grup czynników wpływających na ochronę transportu oraz dla cyberbezpieczeństwa.

Dla potrzeb określenia poziomu bezpieczeństwa, ochrony i cyberbezpieczeństwa oraz poziomu ich spójności stosuje się następujące zasady:
- dla poszczególnych czynników zdefiniowano pytania kontrolne; odpowiedziom przypisano wartości „0” lub „1” dla pytań dyskwalifikujących oraz „1” lub „2” dla pytań różnicujących rozwiązania techniczne,
- wartość „0” jest przypisywana wówczas, gdy odpowiedź wskazuje, że bezpieczeństwo lub ochrona lub cyberbezpieczeństwo nie są zapewnione w sposób odpowiadający zagrożeniom, o których wiadomo, że rzeczywiście występują i że nie tylko możliwe, ale i szeroko stosowane są rozwiązania techniczne, których niestosowanie powoduje istotne braki bezpieczeństwa lub ochrony lub cyberbezpieczeństwa,
- wartość „1” jest przypisywana wówczas, gdy odpowiedź wskazuje, że bezpieczeństwo lub ochrona lub cyberbezpieczeństwo są zapewnione w sposób odpowiadający zagrożeniom, o których wiadomo, że rzeczywiście występują i że nie tylko możliwe, ale i szeroko stosowane są rozwiązania techniczne, które w istotny sposób minimalizują takie zagrożenia,
- wartość „2” jest przypisywana wówczas, gdy odpowiedź wskazuje, że bezpieczeństwo lub ochrona lub cyberbezpieczeństwo są zapewnione w najlepszy dostępny obecnie, sposób,
- wartości referencyjne dla poszczególnych czynników określono jako iloczyny wartości przypisanych odpowiedziom na pytania kontrolne,
- zbiorcze wartości referencyjne dla grup funkcjonalności określono jako iloczyny wartości referencyjnych dla poszczególnych czynników,
- skumulowane wartości referencyjne dla bezpieczeństwa, ochrony i cyberbezpieczeństwa określono jako iloczyny zbiorczych wartości referencyjnych właściwych grup funkcjonalności.

Pytania kontrolne zestawiono w jedenastu kartach kontrolnych – pięciu dedykowanym bezpieczeństwu i pięciu dedykowanym ochronie oraz w karcie kontrolnej dedykowanej cyberbezpieczeństwu.

UWAGA: Karty kontrolne nie służą do weryfikowania wszystkich wymagań stawianych infrastrukturze kolejowej CPK. Zgodnie z zapisami w rozdziale 1.2. oraz zgodnie z obowiązującymi przepisami prawa wymagania zasadnicze w całości potwierdzane są na poziomie podsystemów infrastruktury kolejowej CPK certyfikatami i deklaracjami weryfikacji WE oraz we właściwych częściach, na poziomie wyrobów, którym prawo nadaje status składników interoperacyjności, certyfikatami i deklaracjami zgodności WE. Karty kontrolne uwzględniają natomiast wymagania dla rozwiązań cyfrowych, które mają wpływ na spójność bezpieczeństwa, ochrony i cyberbezpieczeństwa systemu kolei i uwzględniają zarówno infrastrukturę jak i wyposażenie taboru kolejowego. Jednocześnie zaznaczyć należy, że ocena spójności bezpieczeństwa, ochrony i cyberbezpieczeństwa infrastruktury kolejowej CPK, która zgodnie z zapisami niniejszego dokumentu ma być realizowana z uwzględnieniem wymagań rozporządzenia w sprawie oceny i wyceny ryzyka [3, 4], nie wyczerpuje zakresu stosowania oceny i wyceny ryzyka dla infrastruktury kolejowej CPK, bo ta zgodnie z obowiązującym prawem powinna być stosowana do wszelkich zmian technicznych, eksploatacyjnych i organizacyjnych wpływających na bezpieczeństwo.

Karta kontrolna bezpieczeństwa RMF-GB-01 funkcjonalności przytorowych systemów sterowania od kontroli niezajętości do wyświetlania obrazów sygnałowych na sygnalizatorach świetlnych (RMF-b01 ÷ RMF-b04)
Założenia: 1. Infrastruktura torowa podzielona jest na odstępy, na których co do zasady w normalnych warunkach eksploatacyjnych powinien w danym czasie znajdować się jeden pociąg. 2. Sterowanie ruchem realizowane jest pod nadzorem urządzeń sterowania (nastawnicy lub nastawnicy i/lub blokady i/lub systemu sterowania rozrządem.

Pytania kontrolne	Wartości ref.
RMF-b01 1. Czy wszystkie tory na całej długości objęte są kontrolą niezajętości? TAK = 1, NIE = 0 2. Czy wszystkie zastosowane rozwiązania techniczne stosują zasadę FS? (Czy możliwe uszkodzenia modułów prowadzą do zgłaszania zajętości?) TAK = 1, NIE = 0 3. Czy wszystkie zastosowane rozwiązania techniczne stosują zasadę SIL-4? (Czy dostępne są wiarygodne dowody bezpieczeństwa określonego zastosowania potwierdzające SIL-4, zweryfikowane przez niezależnego audytora?) TAK = 1, NIE = 0, NIE, ale system jest w pełni analogowy = 1	Iloczyn odpowiedzi: 0 lub 1
RMF-b02 1. Czy wszystkie zastosowane rozwiązania techniczne stosują zasadę FS? (Czy możliwe uszkodzenia modułów prowadzą do stanów bezpiecznych?) TAK = 1, NIE = 0	0 lub 1
RMF-b03 1. Czy wszystkie zastosowane rozwiązania techniczne stosują zasadę SIL-4? (Czy dostępne są wiarygodne dowody bezpieczeństwa określonego zastosowania potwierdzające SIL-4, zweryfikowane przez niezależnego audytora?) TAK = 1, NIE = 0	0 lub 1
RMF-b04 1. Czy wszystkie odstępy (ew. grupy odstępów) są osłonięte sygnalizatorami? TAK = 1, NIE = 0, NIE, ale zastosowano system BKJP = 1 2. Czy wszystkie zastosowane rozwiązania techniczne stosują zasadę FS? (Czy możliwe uszkodzenia modułów prowadzą do stanów bezpiecznych?) TAK = 1, NIE = 0 3. Czy wszystkie zastosowane rozwiązania techniczne stosują zasadę SIL-4? (Czy dostępne są wiarygodne dowody bezpieczeństwa określonego zastosowania potwierdzające SIL-4, zweryfikowane przez niezależnego audytora?) TAK = 1, NIE = 0, NIE, ale system jest w pełni analogowy = 1	Iloczyn odpowiedzi: 0 lub 1
Zbiorcza wartość referencyjna dla grupy RMF-GB-01 iloczyn wartości referencyjnych RMF-b01 ÷ RMF-b04	0 lub 1
Korekta do RMF-GB-01 brak	

--- --- ---

Karta kontrolna bezpieczeństwa RMF-GB-02 funkcjonalności przytorowych urządzeń systemów bezpiecznej kontroli jazdy pociągu od obrazów sygnałowych do wysyłania elektronicznych zezwoleń ZnJ (RMF-b05 ÷ RMF-b08)
Założenia: 1. Bezpieczna kontrola jazdy pociągu wykorzystuje system klasy ATP lub ATC.

Pytania kontrolne	Wartości ref.
RMF-b05 1. Czy potwierdzono, że pobieranie danych źródłowych dla ZnJ z systemów srk nie wpływa na działanie systemów srk nawet w warunkach awarii? TAK = 1, NIE = 0 2. Czy wszystkie zastosowane rozwiązania techniczne stosują zasadę FS? (Czy możliwe uszkodzenia modułów prowadzą do stanów bezpiecznych?) TAK = 1, NIE = 0 3. Czy wszystkie zastosowane rozwiązania techniczne stosują zasadę SIL-4? (Czy dostępne są wiarygodne dowody bezpieczeństwa określonego zastosowania potwierdzające SIL-4, zweryfikowane przez niezależnego audytora?) TAK = 1, NIE = 0, NIE, ale system jest w pełni analogowy = 1	Iloczyn odpowiedzi: 0 lub 1
RMF-b06 1. Czy wszystkie systemy przetwarzania danych źródłowych definiujące ZnJ w pełnym zakresie stosują zasadę FS? (Czy możliwe uszkodzenia modułów prowadzą do stanów bezpiecznych?) TAK = 1, NIE = 0	0 lub 1
RMF-b07 1. Czy wszystkie systemy przetwarzania danych źródłowych definiujące ZnJ w pełnym zakresie stosują zasadę SIL-4? (Czy dostępne są wiarygodne dowody bezpieczeństwa określonego zastosowania potwierdzające SIL-4, zweryfikowane przez niezależnego audytora?) TAK = 1, NIE = 0	0 lub 1
RMF-b08 1. Czy wysyłane ZnJ zawierają dane pozwalające na identyfikację nadawcy i identyfikację odbiorcy – czy system transmisji jest systemem zamkniętym? TAK = 1, NIE = 0 2. Czy wysyłane ZnJ zawierają dane pozwalające na weryfikację ważności (np. czas żądania i czas nadania lub stempel czasu wspólnego)? TAK = 1, NIE = 0 3. Czy wysyłane ZnJ zawierają dane pozwalające na weryfikację kompletności oraz spójności danych (np. sumy kontrolne, kody hamminga)? TAK = 2, NIE = 1 **4.** Czy wysyłane ZnJ są zabezpieczane technikami kryptograficznymi? TAK = 2, NIE = 1	Iloczyn odpowiedzi: 0 lub 1 lub 2 lub 4
Zbiorcza wartość referencyjna dla grupy RMF-GB-02 iloczyn wartości referencyjnych RMF-b05 ÷ RMF-b08	0 lub 1 lub 2 lub 4
Korekta do RMF-GB-02 **a)** Jeśli odpowiedź na pytanie RMF-b08 nr 3 jest TAK, a RMF-b09 nr 2 NIE, to wartość zbiorczą RMF-GB-02 należy podzielić przez 2. **b)** Jeśli odpowiedź na pytanie RMF-b08 nr 4 jest TAK, a RMF-b09 nr 3 NIE, to wartość zbiorczą RMF-GB-02 należy podzielić przez 2.	

--- --- ---

Karta kontrolna bezpieczeństwa RMF-GB-03 funkcjonalności pokładowych urządzeń systemów bezpiecznej kontroli jazdy pociągu od odebrania zezwolenia ZnJ do interwencyjnego wdrażania hamowania (RMF-b09 ÷ RMF-b12)
Założenia: 1. Bezpieczna kontrola jazdy pociągu wykorzystuje system klasy ATP lub ATC.

Pytania kontrolne	Wartości ref.
RMF-b09 1. Czy odbierane ZnJ podlegają uwierzytelnieniu poprzez sprawdzenie identyfikatorów nadawcy i odbiorcy oraz weryfikację ważności ZnJ? TAK = 1, NIE = 0 2. Czy odbierane ZnJ podlegają weryfikacji kompletności oraz spójności? TAK = 1 (bez korekty RMF-GB-02), NIE = 1 (ew. korekta RMF-GB-02) 3. Czy weryfikowana jest poprawność zabezpieczeń kryptograficznych ZnJ? TAK = 1 (bez korekty RMF-GB-02), NIE = 1 (ew. korekta RMF-GB-02)	Iloczyn odpowiedzi: 0 lub 1
RMF-b10 1. Czy dla pomiaru drogi od punktu referencyjnego określany jest maksymalny błąd przeszacowania i czy jest on odejmowany od zmierzonej wartości? TAK = 1, NIE = 0 2. Czy dla pomiaru prędkości określany jest maksymalny błąd niedoszacowania i czy jest on dodawany do zmierzonej wartości? TAK = 1, NIE = 0 3. Czy zastosowane rozwiązania techniczne stosują zasadę SIL-4? TAK = 1, NIE = 0	Iloczyn odpowiedzi: 0 lub 1
RMF-b11 1. Czy wszystkie zastosowane rozwiązania techniczne BKJP stosują zasadę FS? (Czy możliwe uszkodzenia modułów prowadzą do stanów bezpiecznych?) TAK = 1, NIE = 0 2. Czy wszystkie zastosowane rozwiązania techn. BKJP stosują zasadę SIL-4? (Czy dostępne są wiarygodne dowody bezpieczeństwa określonego zastosowania potwierdzające SIL-4, zweryfikowane przez niezależnego audytora?) TAK = 1, NIE = 0, NIE, ale system jest w pełni analogowy = 1 **3.** Czy określana jest lokalizacja, gdzie najpóźniej należy rozpocząć hamowanie dla odpowiedniego zmniejszenia prędkości przed ograniczeniem prędkości? TAK = 2, NIE = 1 (zastosowany system należy do klasy ATP)	Iloczyn odpowiedzi: 0 lub 1 lub 2
RMF-b12 1. Czy systemy automatycznego wdrażania hamowania interwencyjnego w pełnym zakresie stosują zasadę SIL-4? (Czy dostępne są wiarygodne dowody bezpieczeństwa określonego zastosowania potwierdzające SIL-4, zweryfikowane przez niezależnego audytora?) TAK = 1, NIE = 0 2. Czy automatyczne wdrażanie hamowania interwencyjnego uwzględnia więcej niż jeden tryb hamowania interwencyjnego (np. hamowanie służbowe i nagłe)? TAK = 2, NIE = 1	Iloczyn odpowiedzi: 0 lub 1 lub 2
Zbiorcza wartość referencyjna dla grupy RMF-GB-03 iloczyn wartości referencyjnych RMF-b09 ÷ RMF-b12	0 lub 1 lub 2 lub 4
Korekta do RMF-GB-03 brak	

--- --- ---

Karta kontrolna bezpieczeństwa RMF-GB-04 funkcjonalności wspierające manualne prowadzenie pociągów przez maszynistów w oparciu o obrazy sygnałowe na sygnalizatorach świetlnych przy wykorzystaniu radia (RMF-b13 ÷ RMF-b14)
Założenia: 1. Pociągi prowadzone są przez maszynistów. 2. Zapewniona jest łączność eksploatacyjna.

Pytania kontrolne	Wartości ref.
RMF-b13 1. Czy systemy klasy AWS ostrzegają maszynistów o zbliżaniu się do miejsc niebezpiecznych? TAK = 1, NIE = 0 2. Czy wszystkie urządzenia generujące sygnały ostrzegawcze (dźwiękowe i wizualne) w kabinie maszynisty stosują zasadę FS? (Czy możliwe uszkodzenia modułów prowadzą do stanów bezpiecznych?) TAK = 1, NIE = 0 3. Czy eksploatowany system bezpiecznej kontroli jazdy pociągu klasy ATP lub ATC prezentuje ZnJ na pulpicie w kabinie maszynisty? TAK = 1, NIE = 0 (Uwaga: jeśli brak jest systemu BKJP klasy ATP lub ATC, należy przyjąć 1)	Iloczyn odpowiedzi: 0 lub 1
RMF-b14 1. Czy zapewnione jest głosowe połączenie radiowe między maszynistą i dyżurnym ruchu (ew. dyspozytorem)? TAK = 1, NIE = 0 2. Czy zapewniona jest możliwość generowania sygnałów alarmowych przez dyżurnych ruchu (ew. dyspozytorów)? TAK = 1, NIE = 0 3. Czy zapewniona jest możliwość generowania sygnałów alarmowych przez maszynistów i odbierania sygnałów alarmowych generowanych przez maszynistów i dyżurnych ruchu? TAK = 1, NIE = 0 4. Czy odebranie sygnału alarmowego przez pojazd powoduje automatyczne wdrożenie hamowania i zatrzymanie w miejscu, gdzie możliwa jest ewakuacja względnie działania służb ratunkowych? TAK = 2, NIE = 1	Iloczyn odpowiedzi: 0 lub 1 lub 2
Zbiorcza wartość referencyjna dla grupy RMF-GB-04 iloczyn wartości referencyjnych RMF-b13 ÷ RMF-b14	0 lub 1 lub 2
Korekta do RMF-GB-04 Brak	

--- --- ---

Karta kontrolna bezpieczeństwa RMF-GB-05 funkcjonalności automatycznego prowadzenia pociągu zastępujące maszynistę w przyspieszaniu i hamowaniu oraz obsłudze innych urządzeń pokładowych i drzwi peronowych (RMF-b15 ÷ RMF-b16)
Założenia: 1. Pociągi prowadzone są przez systemy klasy ATO. 2. Ruch pociągów jest nadzorowany przez systemy klasy ATS.

Pytania kontrolne	Wartości ref.
RMF-b15 1. Czy wszystkie pojazdy trakcyjne poruszające się po linii w normalnych warunkach eksploatacji są wyposażone w systemy klasy ATO? TAK = 1, NIE = 0 2. Czy zastosowane systemy klasy ATO same lub w powiązaniu z innymi urządzeniami pokładowymi zapewniają bezpieczne sterowanie prędkością pociągów zgodnie z zasadami FS oraz SIL-4? (Czy dostępne są wiarygodne dowody bezpieczeństwa określonego zastosowania potwierdzające SIL-4, zweryfikowane przez niezależnego audytora?) TAK = 1, NIE = 0	Iloczyn odpowiedzi: 0 lub 1
RMF-b16 1. Czy zapewnione jest bezpieczne automatyczne sterowanie pokładowymi urządzeniami pomocniczymi takimi jak np. systemy poboru prądu (pantografy) czy drzwi zewnętrzne? TAK = 1, NIE = 0 2. Czy zapewnione jest bezpieczne automatyczne sterowanie drzwiami peronowymi wraz z synchronizacją otwierania drzwi peronowych i pokładowych? TAK = 1, NIE = 0 3. Czy zapewniony jest bezpieczny system gromadzenia, przetwarzania i prezentowania danych dla prowadzenia nadzoru nad jazdą wszystkich pojazdów przez dyspozytora? TAK = 1, NIE = 0 4. Czy zapewniony jest bezpieczny system automatycznego nadzoru nad jazdą wszystkich pojazdów, który w normalnych warunkach eksploatacyjnych zastępuje dyspozytora? TAK = 2, NIE = 1	Iloczyn odpowiedzi: 0 lub 1 lub 2
Zbiorcza wartość referencyjna dla grupy RMF-GB-05 iloczyn wartości referencyjnych RMF-b15 ÷ RMF-b16	0 lub 1 lub 2
Korekta do RMF-GB-05 Brak	

--- --- ---

Karta kontrolna ochrony RMF-GO-01 funkcjonalności dedykowane dla zapewnienia minimum bezpieczeństwa osób (RMF-o01 ÷ RMF-o04)
Założenia: 1. Minimum bezpieczeństwa osób musi być zapewnione zarówno w obszarach dostępnych dla pasażerów w infrastrukturze, jak i w taborze.

Pytania kontrolne	Wartości ref.
RMF-o01 1. Czy w obszarach dostępnych dla pasażerów w infrastrukturze zapewniona jest informacja pasażerska o pociągach i zakłóceniach w ruchu pociągów? TAK = 1, NIE = 0 2. Czy w pociągach dostępna jest dla pasażerów informacja pasażerska o opóźnieniach, następnej stacji oraz skomunikowaniach? TAK = 1, NIE = 0	Iloczyn odpowiedzi: 0 lub 1
RMF-o02 1. Czy w obszarach dostępnych dla pasażerów w infrastrukturze, a także w obszarach i pomieszczeniach wykorzystywanych przez personel kolejowy oraz na potrzeby systemów i urządzeń technicznych, zapewniona jest ochrona przeciwpożarowa? TAK = 1, NIE = 0 2. Czy w pociągach zapewniona jest ochrona przeciwpożarowa? TAK = 1, NIE = 0	Iloczyn odpowiedzi: 0 lub 1
RMF-o03 1. Czy w obszarach dostępnych dla pasażerów w infrastrukturze, a także w obszarach i pomieszczeniach wykorzystywanych przez personel kolejowy oraz na potrzeby systemów i urządzeń technicznych zapewniona jest ochrona przeciwporażeniowa? TAK = 1, NIE = 0 2. Czy w pociągach zapewniona jest ochrona przeciwporażeniowa? TAK = 1, NIE = 0	Iloczyn odpowiedzi: 0 lub 1
RMF-o04 1. Czy zapewniona jest ochrona przed spadającymi obiektami w infrastrukturze, w szczególności w obszarach dostępnych dla pasażerów, jeśli jest konieczna? TAK = 1, NIE = 0	0 lub 1
Zbiorcza wartość referencyjna dla grupy RMF-GO-01 iloczyn wartości referencyjnych RMF-o01 ÷ RMF-o04	0 lub 1
Korekta do RMF-GO-01 Brak	

--- --- ---

Karta kontrolna ochrony RMF-GO-02 funkcjonalności dedykowane dla wspierania zdrowia oraz osób o ograniczonych możliwościach ruchowych i osób na wózkach inwalidzkich (RMF-o05 ÷ RMF-o06)
Założenia: 1. Należy zapewnić wsparcie osób o ograniczonej sprawności ruchowej oraz osób na wózkach inwalidzkich.

Pytania kontrolne	Wartości ref.
RMF-o05 1. Czy osoby o ograniczonych możliwościach ruchowych i poruszające się na wózkach inwalidzkich mają zapewniony dostęp w obszarach dostępnych dla pasażerów w infrastrukturze do informacji, zakupu biletu oraz na perony? TAK = 1, NIE = 0 2. Czy osoby poruszające się na wózkach inwalidzkich mają zapewnione wsparcie przy wsiadaniu i wysiadaniu z pociągów, jeśli jest konieczne? TAK = 1, NIE = 0 3. Czy osoby o ograniczonych możliwościach ruchowych i poruszające się na wózkach inwalidzkich mają zapewniony dostęp w pociągach do miejsc siedzących, do informacji oraz toalet? TAK = 1, NIE = 0 4. Czy w obszarach dostępnych dla pasażerów w infrastrukturze udostępniony jest interwencyjny sprzęt medyczny, w szczególności defibrylatory, oraz czy zapewniono znaki informacyjne oraz instrukcje? TAK = 2, NIE = 1	Iloczyn odpowiedzi: 0 lub 1 lub 2
RMF-o06 1. Czy w obszarach dostępnych dla pasażerów w infrastrukturze zapewniona jest możliwość wezwania pomocy? TAK = 1, NIE = 0 2. Czy w pociągach pasażerom zapewniona jest możliwość wezwania pomocy? TAK = 1, NIE = 0	Iloczyn odpowiedzi: 0 lub 1
Zbiorcza wartość referencyjna dla grupy RMF-GO-02 iloczyn wartości referencyjnych RMF-o05 ÷ RMF-o06	0 lub 1 lub 2
Korekta do RMF-GO-02 Brak	

--- --- ---

Karta kontrolna ochrony RMF-GO-03 funkcjonalności dedykowane dla ochrony przed złodziejami i osobami agresywnymi oraz przed wandalizmem, a także współpracy kolejowych służb ochrony z innymi służbami ochrony (RMF-o07 ÷ RMF-o08)
Założenia: 1. Należy zapewnić możliwości pracy dla służb ochrony oraz współpracy własnych służb ochrony i służb współpracujących.

Pytania kontrolne	Wartości ref.
RMF-o07 1. Czy obszary dostępne dla pasażerów w infrastrukturze objęte są monitoringiem wizyjnym? TAK = 1, NIE = 0 2. Czy obszary dostępne dla pasażerów w pociągach objęte są monitoringiem wizyjnym? TAK = 1, NIE = 0	Iloczyn odpowiedzi: 0 lub 1
RMF-o08 1. Czy obszary dostępne dla pasażerów w infrastrukturze są dostępne dla własnych i współpracujących służb ochrony? TAK = 1, NIE = 0 2. Czy własne i współpracujące służby ochrony wyposażone są w środki łączności zapewniające łączność pomiędzy pracownikami ochrony oraz pracownikami odpowiedzialnymi za sterowanie i zarządzanie ruchem? TAK = 1, NIE = 0 3. Czy personel pokładowy może wezwać służby ochrony? TAK = 1, NIE = 0	Iloczyn odpowiedzi: 0 lub 1
Zbiorcza wartość referencyjna dla grupy RMF-GO-03 iloczyn wartości referencyjnych RMF-o07 ÷ RMF-o08	0 lub 1
Korekta do RMF-GO-03 Brak	

--- --- ---

Karta kontrolna ochrony RMF-GO-04 funkcjonalności dedykowane dla ochrony przed terroryzmem oraz współpracy ze służbami antyterrorystycznymi (RMF-o09 ÷ RMF-o12)
Założenia: 1. Należy zapewnić monitorowanie włamań i wtargnięć do obszarów niedostępnych dla osób nieupoważnionych. 2. Należy zapewnić możliwość współpracy ze służbami antyterrorystycznymi.

Pytania kontrolne	Wartości ref.
RMF-o09 1. Czy pomieszczenia techniczne, kontenery oraz szafy z urządzeniami zasilania, sterowania lub łączności są wyposażone w urządzenia wykrywające próby włamania? TAK = 1, NIE = 0 2. Czy pomieszczenia, gdzie pracują osoby odpowiedzialne za sterowanie i zarządzanie ruchem kolejowym oraz zaplecza techniczne, są chronione przed wtargnięciem przez osoby nieupoważnione? TAK = 1, NIE = 0	Iloczyn odpowiedzi: 0 lub 1
RMF-o10 1. Czy służby ochrony są wspomagane przez bieżącą analizę strumieni wideo z systemów monitoringu wizyjnego? TAK = 2, NIE = 1	1 lub 2
RMF-o11 1. Czy bagaże przed wniesieniem do pociągu są prześwietlane? TAK = 2, NIE = 1	1 lub 2
RMF-o12 1. Czy służby antyterrorystyczne mają dostęp do systemów monitoringu wizyjnego oraz analizy strumieni wideo z monitoringu wizyjnego (jeśli odp. RMF-o10 = 2) ? TAK = 1, NIE = 0 2. Czy służby antyterrorystyczne mają zapewnioną łączność z pracownikami ochrony oraz odpowiedzialnymi za sterowanie i zarządzanie ruchem? TAK = 1, NIE = 0	Iloczyn odpowiedzi: 0 lub 1
Zbiorcza wartość referencyjna dla grupy RMF-GO-04 iloczyn wartości referencyjnych RMF-o09 ÷ RMF-o12	0 lub 1 lub 2 lub 4
Korekta do RMF-GO-04 Brak	

--- --- ---

Karta kontrolna ochrony RMF-GO-05 funkcjonalności dedykowane dla ochrony przed katastrofami oraz współpracy ze służbami ratunkowymi (RMF-o13 ÷ RMF-o16)
Założenia: 1. Należy zapewnić ochronę przed ekstremalnymi warunkami atmosferycznymi. 2. Należy zapewnić możliwości współpracy ze służbami ratunkowymi.

Pytania kontrolne	Wartości ref.
RMF-o13 1. Czy zapewniona jest ochrona przed ekstremalnymi warunkami pogodowymi, które mogą wystąpić w okresie eksploatacji wydzielonego systemu kolejowego? TAK = 1, NIE = 0	0 lub 1
RMF-o14 1. Czy zapewniona jest ochrona przed możliwymi katastrofami naturalnymi? TAK = 2, NIE = 1	1 lub 2
RMF-o15 1. Czy zapewnione jest śledzenie ładunków niebezpiecznych oraz przewozów z przekroczoną skrajnią, jeśli takie przewozy są dozwolone? TAK = 2, NIE = 1	1 lub 2
RMF-o16 1. Czy służby ratunkowe mają zapewniony pełny dostęp do informacji w tym do informacji o ładunkach, które były przewożone? TAK = 1, NIE = 0 2. Czy służby ratunkowe mają zapewnioną łączność z pracownikami odpowiedzialnymi za sterowanie i zarządzanie ruchem oraz pracownikami ochrony? TAK = 1, NIE = 0 3. Czy służby ratunkowe mają zapewniony odpowiedni dojazd? TAK = 1, NIE = 0 4. Czy w miejscach dedykowanych do prowadzenia akcji ratunkowych zapewniony jest dostęp do zasilania i środków gaśniczych? TAK = 1, NIE = 0	Iloczyn odpowiedzi: 0 lub 1
Zbiorcza wartość referencyjna dla grupy RMF-GO-05 iloczyn wartości referencyjnych RMF-o13 ÷ RMF-o16	0 lub 1 lub 2 lub 4
Korekta do RMF-GO-05 Brak	

--- --- ---

Karta kontrolna ochrony RMF-CB funkcjonalności dedykowane ochronie przed cyberatakami
Założenia: 1. Należy zapewnić ochronę przed cyberatakami wszystkim przewodowym i bezprzewodowym systemom transmisji danych, które są wykorzystywane na potrzeby bezpieczeństwa ruchu kolejowego. 2. Należy rozważyć zapewnienie ochrony przed cyberatakami wszystkim przewodowym i bezprzewodowym systemom transmisji danych, które są wykorzystywane na potrzeby ochrony transportu kolejowego.

Pytania kontrolne	Wartości ref.
RMF-cb01 – przewodowa i bezprzewodowa transmisja danych w systemach i urządzeniach sterowania ruchem kolejowym 1. Czy wszystkie systemy transmisyjne wykorzystywane przez systemy sterowania ruchem kolejowym są uwzględnione w dowodach bezpieczeństwa potwierdzających stosowanie zasady SIL-4? (Czy dostępne są wiarygodne dowody bezpieczeństwa określonego zastosowania potwierdzające SIL-4, zweryfikowane przez niezależnego audytora?) TAK = 1, NIE = 0 2. Czy w przypadku wykrycia uszkodzenia transmisji podejmowana jest próba automatycznej rekonfiguracji transmisji dla zachowania prowadzenia ruchu z wykorzystaniem środków technicznych, a nie wyłącznie proceduralnych? TAK = 2, NIE = 1	Iloczyn odpowiedzi: 0 lub 1 lub 2
RMF-cb02 – przewodowa i bezprzewodowa transmisja danych w systemach zapewniających łączność głosową 1. Czy w łączność głosową może włączyć się osoba nieuprawniona? TAK = 0, NIE = 1 2. Czy osoba nieuprawniona może uniemożliwić pracownikom służby ruchu oraz służb ochrony i/lub ratunkowych korzystanie z łączności głosowej? TAK = 0, NIE = 1 3. Czy kluczowi dla bezpieczeństwa pracownicy są wyposażeni w niezależną łączność awaryjną? TAK = 2, NIE = 1	Iloczyn odpowiedzi: 0 lub 1 lub 2
RMF-cb03 – przewodowa i bezprzewodowa transmisja danych w systemach bezpiecznej kontroli jazy pociągu 1. Czy wszystkie systemy transmisyjne wykorzystywane przez systemy bezpiecznej kontroli jazdy pociągu (z wyłączeniem radiowej transmisji ZnJ) są uwzględnione w dowodach bezpieczeństwa potwierdzających stosowanie zasady SIL-4? (Czy dostępne są wiarygodne dowody bezpieczeństwa określonego zastosowania potwierdzające SIL-4, zweryfikowane przez niezależnego audytora?) TAK = 1, NIE = 0 2. Czy system radiowej transmisji ZnJ jest zgodny z dokumentami narzuconymi prawem w zakresie zabezpieczenia przed zakłóceniami i atakami? TAK = 1, NIE = 0 3. Czy w przypadku wykrycia uszkodzenia transmisji podejmowana jest próba automatycznej rekonfiguracji transmisji dla zachowania nadzoru systemów bezpiecznej kontroli jazdy nad prowadzeniem pojazdów przez maszynistów? TAK = 2, NIE = 1 **4.** Czy w przypadku uszkodzenia transmisji koniecznej dla systemów bezpiecznej kontroli jazdy ruch może być prowadzony w oparciu o obrazy sygnałowe na sygnalizatorach świetlnych, a nie wyłącznie w oparciu o procedury, połączenia głosowe i sygnały alarmowe? TAK = 2, NIE = 1	Iloczyn odpowiedzi: 0 lub 1 lub 2 lub 4
RMF-cb04 – przewodowa i bezprzewodowa transmisja danych w systemach wspierających ochronę transport szynowego 1. Czy systemy transmisyjne wykorzystywane przez rozwiązania techniczne wspierające ochronę mogą zostać wyłączone przez osoby nieuprawnione? TAK = 0, NIE = 1 **2.** Czy systemy transmisyjne (np. wideomonitoring wraz z gromadzeniem i analizą strumienia wideo) są wyposażone w zasilanie awaryjne zapewniające pracę przez minimum cztery godziny od wyłączenia zasilania? TAK = 2, NIE = 1	Iloczyn odpowiedzi: 0 lub 1 lub 2
Zbiorcza wartość referencyjna dla grupy RMF-CB iloczyn wartości referencyjnych RMF-cb01÷ RMF-cb04	0 lub 1 lub 2 lub 4 lub 8 lub 16 lub 32
Korekta do RMF-CB Brak	

--- --- ---

Wyróżniając poprzez pytania kwestie, w odniesieniu do których jest możliwe przypisanie wartości „2”, wybrano de facto rozwiązania techniczne, których zastosowanie w istotny sposób podnosi bezpieczeństwo lub ochronę bądź cyberbezpieczeństwo. Liczbę pytań, którym można przypisać wartość „2”, dobrano w taki sposób, aby maksymalne skumulowane wartości referencyjne dla bezpieczeństwa, ochrony oraz cyberbezpieczeństwa były takie same. Przy zaproponowanych pytaniach maksymalne skumulowane wartości referencyjne dla bezpieczeństwa, ochrony i cyberbezpieczeństwa wynoszą „32”, przy czym w przypadku bezpieczeństwa skumulowana wartość referencyjna dla systemów kolejowych, w których pociągi prowadzą maszyniści, obejmuje funkcjonalności RMF-GB-01, -02, -03 oraz -04, a dla systemów kolejowych, w których pociągi poruszają się bez maszynistów pod nadzorem systemów automatycznego prowadzenia ruchu (systemów klasy ATO – ang. Automatic Train Operation), funkcjonalności RMF-GB-01, -02, -03 oraz -05. Natomiast skumulowana wartość referencyjna dla ochrony obejmuje funkcjonalności RMF-GO-01, -02, -03, -04 oraz -05.

Dopuszcza się stosowanie przez **wykonawców** koncepcji i projektów oraz **wykonawców** realizujących budowę lub przebudowę infrastruktury innych pytań różnicujących. Zastosowanie innego pytania różnicującego wymaga każdorazowo uzyskania formalnej zgody spółki CPK. W tym celu **wykonawca** powinien zwrócić się do **wewnętrznego zespołu odpowiedzialnego za bezpieczeństwo**. Jednocześnie nie dopuszcza się wprowadzania zmian w odniesieniu do pytań dyskwalifikujących.

Dla pytań różnicujących dopuszcza się stosowanie odpowiedzi częściowo twierdzących z przypisaniem wartości z przedziału otwartego (1, 2), czyli wartości większych od 1 i jednocześnie mniejszych od 2.

3.1.6. Określenie poziomu bezpieczeństwa, ochrony i cyberbezpieczeństwa i poziomu ich spójności

Zbiorcze wartości referencyjne dla grup funkcjonalności pozwalają na określenie skumulowanych wartości referencyjnych dla bezpieczeństwa, ochrony i cyberbezpieczeństwa. Jak już podano powyżej, każda z wartości skumulowanych może maksymalnie osiągnąć wartość „32”. Mogą one jednakże przyjmować wyłącznie wartości „0”, „1”, „2”, „4”, „8”, „16” i „32”. Określone w taki sposób skumulowane wartości referencyjne mogą być przedstawiane w postaci wektorowej jako:

$$[bezpieczeństwo\,,ochrona\,,cyberbezpieczeństwo] \tag{6.1}$$

czyli

$$[GB\,,GO\,,CB] \tag{6.2}$$

gdzie:
GB – skumulowana wartość referencyjna dla bezpieczeństwa,
GO – skumulowana wartość referencyjna dla ochrony,
CB – skumulowana (zbiorcza) wartość referencyjna dla cyberbezpieczeństwa.

Dla systemów, w których pociągi prowadzą maszyniści, wektor przyjmuje postać:

$$[GB_1 \times GB_2 \times GB_3 \times GB_4\,, GO_1 \times GO_2 \times GO_3 \times GO_4 \times GO_5\,, CB] \tag{6.3}$$

Dla systemów, w których pociągi poruszają się bez maszynistów, z wykorzystaniem systemów klasy ATO, wektor przyjmuje postać:

$$[GB_1 \times GB_2 \times GB_3 \times GB_5\,, GO_1 \times GO_2 \times GO_3 \times GO_4 \times GO_5\,, CB] \tag{6.4}$$

gdzie:
GB_x – zbiorcza wartość referencyjna dla funkcjonalności bezpieczeństwa RMF-GB-0x,
GO_x – zbiorcza wartość referencyjna dla funkcjonalności ochrony RMF-GO-0x,
CB – zbiorcza wartość referencyjna dla cyberbezpieczeństwa.

W obu przypadkach (6.3) i (6.4) maksymalną długość osiągamy dla wektora:

$$[32, 32, 32] \tag{6.5}$$

Dla infrastruktury kolejowej CPK wymaga się, aby poziomy bezpieczeństwa, ochrony i cyberbezpieczeństwa wynosiły co najmniej 4. Oznacza to, że zarówno dla bezpieczeństwa, jak i dla ochrony i dla cyberbezpieczeństwa należy wykazać co najmniej dwie pozytywne odpowiedzi na pytania różnicujące. Jednocześnie wymaga się, aby ilość pozytywnych odpowiedzi dla dwóch elementów wektora [GB, GO, CB] była równa, a dla trzeciego nie różniła się więcej niż o jedną.

Wektorowa reprezentacja skumulowanych wartości (6.3) i (6.4) pozwala na szacunkowe określanie poziomu spójności funkcjonalnej skumulowanych wartości referencyjnych bezpieczeństwa i ochrony oraz skumulowanej (zbiorczej) wartości referencyjnej cyberbezpieczeństwa. Jeśli wartości referencyjne są takie same, to ich spójność funkcjonalną określa się jako 1.

Jeśli pomiędzy tymi wartościami pojawiają się różnice, to spójność maleje nieliniowo, najpierw delikatnie, a następnie szybciej, ale nie spada do zera. W tym celu zdefiniowano płaszczyznę odniesienia, dla której wektor (6.5) jest tzw. wektorem normalnym, tzn. prostopadłym do tej płaszczyzny, oraz jako miarę spójności funkcjonalnej bezpieczeństwa, ochrony i cyberbezpieczeństwa przyjęto sinus kąta pomiędzy tą płaszczyzną i wektorem (6.3) lub (6.4).

Każdą płaszczyznę w trójwymiarowej przestrzeni definiują trzy punkty. Jako płaszczyznę odniesienia przyjęto płaszczyznę Π_{odn} zdefiniowaną następującą macierzą:

$$\Pi_{odn} = \begin{matrix} 32 & 0 & 0 \\ 0 & 32 & 0 \\ 0 & 0 & 32 \end{matrix} \tag{6.6}$$

w której wiersze reprezentują punkty, a kolumny ich współrzędne w przestrzeni trójwymiarowej i dla której wektor (6.5) jest wektorem normalnym.

Spójność funkcjonalna bezpieczeństwa, ochrony i cyberbezpieczeństwa będzie wówczas obliczana z następującego wzoru:

$$FIL_{SF,\,SC,\,CS} = sin\,\langle \left(\begin{matrix} 32 & 0 & 0 \\ 0 & 32 & 0 \\ 0 & 0 & 32 \end{matrix}, [\,SF, SC, CS\,] \right) \left| \begin{matrix} SF \neq 0 \\ SC \neq 0 \\ CS \neq 0 \end{matrix} \right. \tag{6.7}$$

gdzie:
$FIL_{GB,\,GO,\,CB}$ – spójność funkcjonalna bezpieczeństwa, ochrony i cyberbezpieczeństwa.

Przyjęcie określenia FIL w założeniu ma korespondować z poziomami nienaruszalności bezpieczeństwa SIL (ang. *Safety Integrity Level*) i powinno być rozumiane jako poziom spójności funkcjonalnej bezpieczeństwa, ochrony i cyberbezpieczeństwa $FIL_{SS\&C}$ (ang. *Functional Integrity Level for safety, security and cybersecurity*).

UWAGA: Możliwe jest opracowanie tabeli wartości FIL, jako że liczba przypadków wektorów z wartościami GB, GO oraz CB jest ograniczona, szczególnie że możliwych jest tylko siedem wartości GB, siedem GO oraz siedem CB, a wartości kąta będą się powtarzały dla różnych wartości wektora, np. dla [4, 8, 4], [4, 4, 8] i [8, 4, 4]. Należy jednak zauważyć, że taka tabela finalnie zamykałaby dopuszczalną liczbę wartości FIL, natomiast określanie wartości FIL poprzez sinus konta pozwala na przypisywanie odpowiedziom na pytania różnicujące wartości odpowiedzi z przedziału $\langle 1, 2\rangle$ przy pozostawieniu odpowiedzi „0" oraz „1" dla pytań dyskwalifikujących. Zakres wartości FIL nadal zawierałby się w przedziale $\langle 0, 1\rangle$, przy czym zasada pięciu pytań różnicujących powinna zostać zachowana. Niezachowanie z góry zdefiniowanej i równej dla bezpieczeństwa, ochrony i cyberbezpieczeństwa liczby pytań różnicujących mogłoby prowadzić do manipulowania wartościami przy opracowywaniu dowodów spójności funkcjonalnej bezpieczeństwa, ochrony i cyberbezpieczeństwa.

3.1.7. Podsumowanie dowodu spójności bezpieczeństwa, ochrony i cyberbezpieczeństwa

Każdy '**dowód spójności bezpieczeństwa, ochrony i cyberbezpieczeństwa**' powinien zawierać osobny dedykowany rozdział, w którym wykonawca podaje zakres ocenianego systemu, uproszczenia dla potrzeb analiz, jeśli zostały zastosowane oraz wynikowe poziomy bezpieczeństwa, ochrony i cyberbezpieczeństwa oraz wynikowy poziom spójności bezpieczeństwa, ochrony i cyberbezpieczeństwa.

3.1.8. Upraszczanie systemów dla potrzeb oceny

Określenie poziomu spójności bezpieczeństwa, ochrony i cyberbezpieczeństwa uwzględnia zarówno charakterystykę infrastruktury kolejowej, jak i charakterystykę taboru w odniesieniu do systemów z transmisją danych wspierających bezpieczeństwo ruchu i/lub ochronę transportu. Prostej ocenie nie może więc być poddany na przykład cały system kolei w Polsce, ponieważ różne stacje i szlaki, podobnie jak pociągi i pojazdy, są w różny sposób wyposażone w systemy wykorzystujące transmisję danych na potrzeby bezpieczeństwa ruchu kolejowego, ochrony transportu kolejowego i cyberbezpieczeństwa. Podobne wyzwanie dotyczyć będzie także systemu kolejowego bazującego na infrastrukturze kolejowej CPK. Z tego względu dopuszcza się przyjmowanie założeń upraszczających analizy zawarte w **dowodzie spójności bezpieczeństwa, ochrony i cyberbezpieczeństwa**. Sposób postępowania podano poniżej w postaci kolejnych dwunastu kroków, wraz z pytaniami, które pozwalają na pominięcie części kroków.

Krok 1. Opis systemu transportowego, który ma być poddany ocenie.

Dowód spójności bezpieczeństwa, ochrony i cyberbezpieczeństwa powinien rozpoczynać się od opisu ocenianego systemu zawartego w rozdziałach dedykowanych zabezpieczeniom technicznym bezpieczeństwa ruchu i zabezpieczeniom technicznym ochrony transportu.
Przejdź do kroku 2.

Krok 2. Czy system jest jednolity technicznie?

Opracowane pierwsze dwa rozdziały **dowodu spójności bezpieczeństwa, ochrony i cyberbezpieczeństwa** mogą wskazywać na brak jednolitości systemu w odniesieniu do ocenianych cech charakterystycznych.
Jeśli oceniany system jest jednolity, technicznie przejdź do kroku 5.
Jeśli oceniany system nie jest jednolity technicznie, przejdź do kroku 3.

Krok 3. Czy system jest jednolity funkcjonalnie?

Techniczna jednolitość ocenianego systemu nie musi być zapewniona. Na potrzeby zastosowania modelu RMF wystarczy jednolitość funkcjonalności powiązanych ze wspieraniem bezpieczeństwa i ochrony przez systemy z transmisją danych oraz jednolitość sposobów zabezpieczenia tych systemów przed cyberatakami.
Jeśli oceniany system jest jednolity funkcjonalnie, przejdź do kroku 5.
Jeśli oceniany system nie jest jednolity funkcjonalnie, przejdź do kroku 4.

Krok 4. Upraszczanie ocenianego systemu transportowego:

a) wydzielenia obszarowe.

Jednolitość funkcjonalna na potrzeby wiarygodnego zastosowania modelu RMF może zostać osiągnięta poprzez wyłączenie z oceny części infrastruktury, na przykład stacji granicznych. Należy przy tym zaznaczyć, że ocena może być prowadzona zarówno dla systemu spójnego, czyli takiego, w ramach którego pojazdy mogą przejeżdżać między każdymi dwiema częściami infrastruktury pod nadzorem czy z wykorzystaniem analizowanych systemów z transmisją danych, jak i dla systemów, które w odniesieniu do tych systemów należy uznać za niespójne, czyli posiadające luki obszarowe.

Wymaga się odnotowania uproszczeń przyjętych dla przeprowadzenia oceny.

Jeśli uproszczony system jest jednolity funkcjonalnie, przejdź do kroku 5.
Jeśli uproszczony system nie jest jednolity funkcjonalnie, przejdź do kroku 4b.

b) wydzielenia funkcjonalne.

Jednolitość funkcjonalna na potrzeby wiarygodnego zastosowania modelu RMF może zostać osiągnięta poprzez wyłączenie z oceny części czynników wpływających na ocenę w modelu RMF. Może to dotyczyć pojedynczych czynników lub nawet wyłączenia oceny w zakresie ochrony dla przeprowadzenia oceny wyłącznie w odniesieniu do bezpieczeństwa ruchu. Takie wyłączenie będzie wymagało dla uzyskania wartości poziomu *FIL* przyjęcia fałszywych wartości referencyjnych „1” dla odpowiedzi na pytania kontrolne odnoszące się do obszaru/ów wyłączenia. Tak uzyskaną wartość poziomu *FIL* można określić jako zafałszowany poziom *FIL*.
Wymaga się odnotowania uproszczeń przyjętych dla przeprowadzenia oceny.

Jeśli uproszczony system jest jednolity funkcjonalnie, przejdź do kroku 5.
Jeśli uproszczony system nie jest jednolity funkcjonalnie, przejdź do kroku 4c.

c) wydzielenie części cyberzabezpieczeń.

Jednolitość funkcjonalna na potrzeby wiarygodnego zastosowania odwzorowania systemów transmisji w modelu RMF może zostać osiągnięta poprzez wyłączenie z oceny cyberbezpieczeństwa części procesów nadawania, transmisji i odbierania danych wpływających na ocenę. Transmisje wyłączone z oceny na wizualizacji nie mogą być pomijane. Wymaga się aby były one przedstawiane strzałkami z konturem zaznaczonym linią przerywaną oraz białym wypełnieniem. Ciemne wypełnienie wskazuje na potwierdzenie bezpieczeństwa transmisji, a białe na brak takiego potwierdzenia, więc zgodnie z zasadą fail-safe w tym przypadku wypełnienia strzałek powinny być białe.

Wymaga się odnotowania uproszczeń przyjętych dla przeprowadzenia oceny.

Jeśli uproszczony system jest jednolity funkcjonalnie, przejdź do kroku 5.
Jeśli uproszczony system nadal nie jest jednolity, należy rozważyć zastosowanie dodatkowych uproszczeń zgodnych z opisem w punktach a, b lub c.

Krok 5. Opracowanie wizualizacji w modelu RMF bez wizualizacji transmisji.

Wizualizacja w modelu RMF powinna obejmować stosowny opis poparty danymi potwierdzającymi stosowanie poszczególnych funkcjonalności. Może zawierać odwołania do innych dostępnych dokumentów, opisy funkcjonalności, zdjęcia itp. Sama wizualizacja w modelu RMF może być przedstawiona na początku (wówczas opis będzie niejako dowodem, że wizualizacja została przedstawiona w sposób właściwy) lub na końcu (jako wynik analizy opartej na opisie funkcjonalności).

Po opracowaniu wizualizacji w modelu RMF, przejdź do kroku 6.

Krok 6. Opracowanie wizualizacji w modelu RMF z wizualizacją transmisji.

Zestawienie informacji o wszystkich procesach nadawania, transmisji i odbierania danych wykorzystywanych przez systemy wspierające bezpieczeństwo ruchu i ochronę transportu powinno zawierać informacje o ich zabezpieczeniach przed wpływem warunków zewnętrznych, uszkodzeniami współpracujących systemów oraz cyberzagrożeniami. Zebrane informacje powinny być poparte dowodami, np. odwołaniami do innych dokumentów. Wizualizacja w modelu RMF może wrysowywać poszczególne procesy przekazywania danych zarówno wewnątrz, jak i na zewnątrz modelu RMF. Dla funkcjonalności, w zakresie których mają miejsce osobne transmisje po stronie infrastrukturalnej i osobne po stronie taborowej, stosuje się wizualizację transmisji odpowiednio wewnątrz i na zewnątrz modelu RMF.

Po opracowaniu wizualizacji transmisji w modelu RMF przejdź do kroku 7.

Krok 7. Określenie poziomu funkcjonalnej spójności bezpieczeństwa ochrony i cyberbezpieczeństwa ocenianego systemu transportowego.

Oceniany system transportowy przedstawiony wizualnie w modelu RMF może być systemem technicznie jednolitym lub jednolitym funkcjonalnie w zakresie ocenianych czynników lub systemem uproszczonym na potrzeby zastosowania modelu. W przypadku uproszczeń dla określenia poziomu *FIL* w zakresie uproszczeń należy przyjmować fałszywe wartości referencyjne „1”. Wartości takie należy podawać czerwoną czcionką. Zastosowanie wartości fałszywych pozwala na określenie poziomu FIL dla uproszczonego systemu, ale uzyskany poziom FIL będzie poziomem zafałszowanym. Taki poziom FIL należy podawać czerwoną czcionką.

Konieczne jest zastosowanie wszystkich pytań dyskwalifikujących. W odniesieniu do pytań różnicujących należy zweryfikować ich adekwatność w przypadku ocenianego systemu. Pytania różnicujące można skorygować lub nawet sformułować na potrzeby danego **dowodu spójności bezpieczeństwa, ochrony i cyberbezpieczeństwa**. Powinna być jednak zachowana liczba pytań różnicujących.

Przejdź do kroku 8.

Krok 8. Wnioskowanie o bezpieczeństwie, ochronie i cyberbezpieczeństwie rzeczywistego lub uproszczonego systemu w oparciu o wizualizację w modelu RMF oraz poziom *FIL*.

Uzyskana wartość poziomu FIL (rzeczywista lub zafałszowana) może przyjmować różne wartości, przy czym uzyskiwane wartości *GB*, *GO* oraz *CB*, będące krotnościami wartości „2”, mogą być wynikiem różnych zabezpieczeń. Podobnie takie same wartości poziomu FIL mogą być uzyskane dla różnych wartości *GB*, *GO* oraz *CB*, na przykład dla wektorów [4, 4, 2] oraz [4, 2, 4]. Dlatego wymaga się przedstawiania wniosków dotyczących spójności bezpieczeństwa, ochrony i cyberbezpieczeństwa z zaznaczeniem, które z nich zostały uzyskane dzięki zastosowaniu uproszczeń.

Jeśli na potrzeby oceny system nie był upraszczany, to przejdź do kroku 11.
Jeśli system był upraszczany na potrzeby oceny, przejdź do kroku 9.

Krok 9. Wnioskowanie o bezpieczeństwie nieuproszczonego systemu transportowego w oparciu o wizualizację uproszczonego systemu transportowego w modelu RMF i zafałszowany poziom *FIL*.

Wszystkie wprowadzone uproszczenia powinny być przeanalizowane pod kątem wpływu na ocenę końcową. Wnioski sformułowane dla systemu uproszczonego należy analizować w kontekście systemu rzeczywistego. W niektórych przypadkach analizy będą wskazywały, że zidentyfikowane braki zabezpieczeń są w rzeczywistości znacznie poważniejsze niż wynikałoby to z zafałszowanych wizualizacji i zafałszowanego poziomu *FIL*. W niektórych przypadkach analizy mogą sugerować przeniesienie uproszczeń z modelu do rzeczywistego systemu transportowego np. przez rezygnację z eksploatacji wybranych typów pociągów lub

pojazdów.
Przejdź do kroku 10.

Krok 10. Analiza wpływu poziomów SIL zastosowanych rozwiązań technicznych na zafałszowany poziomu spójności bezpieczeństwa, ochrony i cyberbezpieczeństwa *FIL*.

W pytaniach kontrolnych odwzorowano wymagany poziom integralności bezpieczeństwa SIL-4. Jednakże nie wszystkie stosowane rozwiązania techniczne gwarantują taki poziom SIL. Jeśli uproszczenia, względnie część uproszczeń, są spowodowane wartością poziomu SIL, konieczne jest przeprowadzenie analizy zasadności i możliwości podniesienia poziomu SIL.

Przejdź do kroku 11.

Krok 11. Analiza wrażliwości poziomu spójności bezpieczeństwa, ochrony i cyberbezpieczeństwa.

Jeśli w procesie określania wartości poziomu *FIL* zostały przypisane wartości „0", to maskują one ewentualne pozytywne odpowiedzi na pytania różnicujące. W takim przypadku należy przeanalizować i przedstawić zmiany poziomu *FIL*, jakie będą miały miejsce po wyeliminowaniu braków skutkujących zerowymi „0" wartościami referencyjnymi.

Przejdź do kroku 12.

Krok 12. Wnioski końcowe z analizy bezpieczeństwa, ochrony i cyberbezpieczeństwa.

Analiza prowadzona w modelu RMF oraz określenie poziomu *FIL* muszą kończyć się jasno sformułowanymi wnioskami końcowymi. Wnioski takie powinny zawierać rekomendacje ze wskazaniem obszarów, w których jest konieczne względnie możliwe wprowadzenie dodatkowych środków zabezpieczających.

Ostatni rozdział **dowodu spójności bezpieczeństwa, ochrony i cyberbezpieczeństwa** powinien zawierać zarówno wnioski, w tym wartości wynikowe wektora [GB, GO, C] oraz poziomu FIL, jak i zestawienie wszystkich uproszczeń, które zostały zastosowane w celu osiągnięcia wynikowej wartości poziomów bezpieczeństwa, ochrony i cyberbezpieczeństwa oraz ich spójności.

Stosowanie przedstawionych powyżej uproszczeń wymaga każdorazowo uzyskania formalnej zgody spółki CPK. W tym celu **wykonawca** powinien zwrócić się do **wewnętrznego zespołu odpowiedzialnego za bezpieczeństwo**. Nie ma jednakże wątpliwości, że uproszczenia takie będą niekiedy konieczne. Przykładowo jeśli po infrastrukturze kolejowej CPK będą poruszały się zarówno pociągi wyposażone jak i nie wyposażone w pokładowe systemy ETCS dla zapewnienia informacyjnego charakteru wyliczeń konieczne będzie wyłączenie z oceny pociągów niewyposażonych. Świadomość tego wyłączenia powinna wiązać się z dążeniem do doposażenia takich pojazdów we właściwe urządzenia pokładowe.

3.2 Zasady weryfikowania spójności bezpieczeństwa, ochrony i cyberbezpieczeństwa infrastruktury kolejowej CPK

Weryfikacja '**dowodu spójności bezpieczeństwa, ochrony i cyberbezpieczeństwa**' powinna być przeprowadzona przez **kompetentną niezależną jednostkę inspekcyjną** posiadającą akredytację Polskiego Centrum Akredytacji dla jednostki oceniającej ryzyko dla pięciu podsystemów strukturalnych – podsystemów „Infrastruktura", „Energia", „Sterowanie – urządzenia przytorowe" oraz „Tabor" i „Sterowanie – urządzenia pokładowe".

Kompetentna niezależna jednostka inspekcyjna opracowuje 'Raport z niezależnej oceny dowodu spójności bezpieczeństwa, ochrony i cyberbezpieczeństwa' respektując wymagania dla jednostek zdefiniowane w rozporządzeniu w sprawie wspólnej metody oceny bezpieczeństwa w zakresie

wyceny i oceny ryzyka [3, 4] oraz stosując wymagania dla raportu zdefiniowane w niniejszym rozdziale.

‘Raport z niezależnej oceny dowodu spójności bezpieczeństwa, ochrony i cyberbezpieczeństwa’ dla koncepcji lub projektu lub realizacji infrastruktury kolejowej CPK powinien obejmować pięć następujących rozdziałów:

1. Ocena analizy zabezpieczeń technicznych związanych z zapewnieniem bezpieczeństwa ruchu
2. Ocena analizy zabezpieczeń technicznych związanych z zapewnieniem ochrony transportu
3. Ocena analizy zabezpieczeń przed cyberzagrożeniami
4. Ocena sposobu określenia poziomu spójności bezpieczeństwa, ochrony i cyberbezpieczeństwa
5. Wnioski z oceny dowodu spójności bezpieczeństwa, ochrony i cyberbezpieczeństwa

Rozdział 1 powinien zawierać ocenę analizy zabezpieczeń technicznych związanych z zapewnieniem bezpieczeństwa ruchu, w tym odniesienie do następujących aspektów wymagania zasadniczego bezpieczeństwo: 1.1.1., 1.1.4., 1.1.5., 1.1.6., 1.1.7., 1.1.8., 1.1.10. oraz 1.1.11. Należy przy tym uwzględnić wszystkie wymagania szczegółowe Technicznych Specyfikacji Interoperacyjności powiązane z tymi aspektami wymagania zasadniczego bezpieczeństwo oraz wszystkie wymagania właściwych tomów Standardów kolejowych CPK, które z tymi aspektami są powiązane.

Rozdział 2 powinien zawierać ocenę analizy zabezpieczeń technicznych związanych z zapewnieniem ochrony transportu, w tym odniesienia do następujących aspektów wymagania zasadniczego bezpieczeństwo: 1.1.12. oraz 1.1.13 zdefiniowanych dla potrzeb infrastruktury kolejowej CPK. Należy przy tym uwzględnić wszystkie wymagania właściwych tomów Standardów kolejowych CPK, które z tymi aspektami są powiązane.

Rozdział 3 powinien zawierać ocenę analizy zabezpieczeń przed cyberzagrożeniami włącznie z analizą pełnego stosowania zasad systemu zarządzania bezpieczeństwem informacji przyjętych przez zarządcę infrastruktury zgodnie z normą PN-EN ISO/IEC 27001 [6].

Rozdział 4 powinien potwierdzać prawidłowe wyliczenie wartości wektora [GB, GO, CB] oraz poziomu FIL spójności bezpieczeństwa, ochrony i cyberbezpieczeństwa. Rozdział ten powinien odnosić się do wszystkich ewentualnych uproszczeń zastosowanych przy określaniu tych wartości.

Kompetentna niezależna jednostka inspekcyjna opracowująca ‘Raport z niezależnej oceny dowodu spójności bezpieczeństwa, ochrony i cyberbezpieczeństwa’ zobowiązana jest do umieszczenia na końcu raportu osobnego rozdziału zawierającego jednoznaczne podsumowanie ze wskazaniem pozytywnego lub negatywnego wyniku raportu.

Dla etapu realizacji prac ‘koncepcja’ weryfikacja ‘**dowodu spójności bezpieczeństwa, ochrony i cyberbezpieczeństwa**’ prowadzona może być przez spółkę CPK. W tym celu **wykonawca** powinien zwrócić się do wewnętrznego zespołu odpowiedzialnego za bezpieczeństwo.

‘Raport z oceny dowodu spójności bezpieczeństwa, ochrony i cyberbezpieczeństwa’ prowadzonej przez wewnętrzny zespół odpowiedzialny za bezpieczeństwo opracowywany jest zgodnie z zasadami określonymi przez CPK.

[pozostałą część strony intencjonalnie pozostawiono pustą]

4. Dokumenty referencyjne

Dla potrzeb opracowania Tomu XVIII wykorzystano następujące dokumenty referencyjne:

dokumenty prawne UE:

- dyrektywy:
  1. Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/797 z dnia 11 maja 2016 r. w sprawie interoperacyjności systemu kolei w Unii Europejskiej (Dz.U.UE L 138/44 z dnia 26.05.2016)
  2. Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/1148 z dnia 6 lipca 2016 r. w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii (Dz.U.UE L 194/1 z dnia 19.7.2016)

- rozporządzenia:
  3. Rozporządzenie Wykonawcze Komisji (UE) nr 402/2013 z dnia 30 kwietnia 2013 r. w sprawie wspólnej metody oceny bezpieczeństwa w zakresie wyceny i oceny ryzyka i uchylające rozporządzenie (WE) nr 352/2009 (Dz.U.UE L 121/8 z dnia 3.5.2013)
  4. Rozporządzenie Wykonawcze Komisji (UE) 2015/1136 z dnia 13 lipca 2015 r. zmieniające rozporządzenie wykonawcze (UE) nr 402/2013 w sprawie wspólnej metody oceny bezpieczeństwa w zakresie wyceny i oceny ryzyka (Dz.U.UE L 185/6 z dnia 14.7.2015)

dokumenty prawne RP:

- ustawy:
  5. Ustawa z dnia 5.07.2018 r. o krajowym systemie cyberbezpieczeństwa, Dz.U. 2018 poz. 1560

powołane normy i dokumenty normatywne:

- normy europejskie przejęte przez CEN, CENELEC, ETSI
  6. PN-EN ISO/IEC 27001:2017-06 Technika informatyczna -- Techniki bezpieczeństwa -- Systemy zarządzania bezpieczeństwem informacji -- Wymagania
  7. PN-EN 50126-1:2018-02 Zastosowania kolejowe -- Specyfikowanie i wykazywanie niezawodności, dostępności, podatności utrzymaniowej i bezpieczeństwa (RAMS) -- Część 1: Proces ogólny RAMS
  8. PN-EN 50126-2:2018-02 Zastosowania kolejowe -- Specyfikowanie i wykazywanie niezawodności, dostępności, podatności utrzymaniowej i bezpieczeństwa (RAMS) -- Część 2: Sposoby podejścia do bezpieczeństwa
  9. PN-EN 50128:2011 Zastosowania kolejowe -- Systemy łączności, przetwarzania danych i sterowania ruchem -- Oprogramowanie kolejowych systemów sterowania i zabezpieczenia
  10. PN-EN 50129:2019-01 Zastosowania kolejowe -- Systemy łączności, przetwarzania danych i sterowania ruchem -- Elektroniczne systemy sterowania ruchem związane z bezpieczeństwem
  11. PN-EN 50159:2011 Zastosowania kolejowe -- Systemy łączności, sterowania ruchem i przetwarzania danych -- Łączność bezpieczna w systemach transmisyjnych

--- ---