Centrum Wymiany i Analizy Informacji
podsektora transportu kolejowego
„ISAC – Kolej”

Wytyczne dotyczące cyberbezpieczeństwa pasażerskiego taboru kolejowego

wersja 1.0

Warszawa, 31 lipca 2023

Wersjonowanie dokumentu:

Wersja	Zmiany
1.0	Pierwsza kompletna wersja dokumentu.
	Przyjęta przez ISAC-Kolej w dniu: 31 lipca 2023 r.
---	
	przyjęta przez ISAC-Kolej w dniu:

==========

Jednocześnie informuje się, że:

- Zgodnie z ustaleniami ze spotkania ISAC-Kolej w dniu 31 lipca 2023 dokument „Wytyczne dotyczące cyberbezpieczeństwa pasażerskiego taboru kolejowego” zostanie przekazany producentom taboru z sugestią podjęcia próby zastosowania dokumentu do wybranych typów pasażerskiego taboru kolejowego w celu uzyskania pierwszych doświadczeń i sformułowania ewentualnych uwag do wytycznych;
- Intencją autorów dokumentu jest nie tylko udostępnienie go przemysłowi oraz polskim przewoźnikom i zarządcom kolejowym; ale także
- Przetłumaczenie dokumentu na język angielski i przekazanie Agencji Unii Europejskiej ds. Cyberbezpieczeństwa ENISA wraz ze zgodą na upowszechnianie.

==========

Spis treści

strona

1. Wprowadzenie

W grudniu 2022 roku Parlament Europejski i Rada UE przyjęły Dyrektywę w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii Europejskiej [3]. Dokument ten (dyrektywa NIS 2) definiuje wymagania co do dbałości o zabezpieczenia przed cyberzagrożeniami między innymi dla przewoźników kolejowych. Wcześniejsza dyrektywa (dyrektywa NIS) [2] od przewoźników kolejowych wymagała działań związanych z cyberzagrożeniami wyłącznie jeśli zostali wskazani stosownymi decyzjami administracyjnymi przez właściwy organ krajowy. Dyrektywa NIS 2 wymaga stosownych działań między innymi od przewoźników kolejowych, z wyłączeniem tych, którzy zatrudniają nie więcej niż 49 osób oraz jednocześnie posiadają obroty roczne mniejsze niż 10 000,- euro. Dyrektywa NIS 2 narzuca więc nowe obowiązki w zakresie cyberbezpieczeństwa transportu na niemal wszystkich przewoźników kolejowych.

Niezależnie od zmiany prawa europejskiego, która musi być jeszcze wprowadzona do prawa krajowego, aktualna sytuacja międzynarodowa spowodowała w Polsce lawinowy wzrost cyberzagrożeń dla transportu od lutego 2022 r. Szczególnie narażony jest transport kolejowy jako intensywnie wykorzystywany dla wsparcia działań militarnych i dyplomatycznych za wschodnią granicą Polski.

Opracowane na podstawie „Transport Cybersecurity Toolkit" i przyjęte przez ISAC-Kolej w 2021 r. „Wytyczne dotyczące cyberbezpieczeństwa dla pracowników podmiotów kolejowych" stały się niewystarczające, mimo że od 2022 r. członkowie ISAC-Kolej drogą elektroniczną regularnie otrzymują:

- codzienne raporty krajowe dotyczące złośliwego ruchu sieciowego (rekomendacje dotyczące blokowania konkretnych IP),
- tygodniowe raporty krajowe zawierające informacje na temat wykrytych podatności w produktach IT (rekomendacje dotyczące aktualizacji systemów i oprogramowania),
- dwutygodniowy biuletyn informacyjny SOC PKP Informatyka dotyczący cyberbezpieczeństwa w transporcie kolejowym,

oraz w przypadkach wykrycia zagrożeń:

- informacje o nowych kampaniach phishingowych,
- informacje o zarejestrowaniu domen, które mogą być wykorzystane do ataków phishingowych (rekomendacje blokowania złośliwych domen na urządzeniach brzegowych, stosowania odpowiednich filtrów antyspamowych, czujności przy wysyłaniu/odbieraniu wiadomości przesyłanych drogą elektroniczną przez pracowników),
- informacje o wykryciu podatności zero-day, możliwości ich wykorzystania oraz IoC (rekomendacje – rożne, w zależności od typu podatności),
- informacje o kampaniach phishingowych dystrybuujących złośliwe oprogramowanie oraz IoC złośliwej kampanii (rekomendacje - wdrożenie stosownych reguł na urządzeniach filtrujących pocztę elektroniczną),
- w przypadku stwierdzenia – informacje o atakach DDoS, w tym o możliwych atakach na strony internetowe i serwisy (rekomendacje – ochrona antyDDoS, monitorowanie infrastruktury, przygotowanie się na ograniczenia ruchu przy eskalacji), oraz
- w razie konieczności – przydatne informacje, np. dotyczące działalności grup APT, Killnet, itp.

Dyrektywa NIS 2 wymaga od przewoźników kolejowych identyfikowania zagrożeń i przeciwdziałania zagrożeniom oraz raportowania cyberataków i incydentów. Mimo, że dyrektywa NIS 2 nie została jeszcze wprowadzona do prawa krajowego część przewoźników kolejowych przygotowując przetargi na zakup taboru kolejowego uznała za konieczne uwzględnienie wymagań z zakresu cyberbezpieczeństwa w dokumentacji przetargowej między innymi ze względu obecnie występujące cyberzagrożenia oraz fakt, że dostawy taboru przewidziane są po wejściu w życie dyrektywy NIS 2.

1.1. Regulacje prawne dotyczące cyberbezpieczeństwa transportu kolejowego

Kolejne dyrektywy UE w sprawie interoperacyjności kolei od roku 1996 w odniesieniu do kolei dużych prędkości, a od roku 2001 w odniesieniu do kolei konwencjonalnych, w załączniku III definiują wymagania zasadnicze, w tym wymaganie zasadnicze 'bezpieczeństwo'. Część zapisów definiujących wymaganie zasadnicze 'bezpieczeństwo' w obowiązującej dyrektywie (UE) 2016/797 w sprawie

interoperacyjności kolei [1] ma zastosowanie do rozwiązań elektronicznych i programowalnych między innymi w odniesieniu do zapewniania odpowiedniego poziomu bezpieczeństwa awarii np. systemów sterowania czy poziomu uczciwości i niezawodności w zakresie gromadzenia i przekazywania informacji dotyczących bezpieczeństwa np. w ramach aplikacji telematycznych. Wymagania wprost dedykowane do cyberbezpieczeństwa nie są jednak doprecyzowane ani w ramach dyrektywy ani w ramach Technicznych Specyfikacji Interoperacyjności przyjętych w formie rozporządzeń Komisji Europejskiej uzupełniających dyrektywę w sprawie interoperacyjności kolei.

Agencja Unii Europejskiej do spraw cyberbezpieczeństwa (ENISA) powołana została w roku 2004. W roku 2016 przyjęta została obecnie obowiązująca dyrektywa (UE) 2016/1148 w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych (dyrektywa NIS) [2], która swoim zakresem objęła między innymi transport kolejowy. Dyrektywa ta, w roku 2022, została zastąpiona dyrektywą (UE) 2022/2555 w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa (dyrektywą NIS 2) [3], która, jak wspomniano we wstępie, nakłada szereg obowiązków na przewoźników kolejowych w zakresie zapewnienia odpowiedniego poziomu cyberbezpieczeństwa. Dyrektywa NIS 2 zastąpi dyrektywę NIS po wdrożeniu do prawa krajowego państw UE, przy czym zgodnie z wiążącymi przepisami musi to nastąpić najpóźniej do października 2024 r. Równolegle Parlament Europejski przyjął dyrektywę (UE) 2022/2557 w sprawie odporności podmiotów krytycznych [4], w którym przewoźnicy kolejowi uznani zostali za podmioty krytyczne zobowiązane do prowadzenia ocen ryzyka obejmujących wszystkie istotne naturalne i spowodowane przez człowieka czynniki ryzyka oraz do podejmowania działań koniecznych dla minimalizacji zagrożeń. Treść tej dyrektywy nie odnosi się wprost do cyberbezpieczeństwa. Dyrektywa koncentruje się w szczególności na ochronie fizycznej oraz zarządzaniu kryzysowym, czyli kwestiach komplementarnych do cyberzagrożeń, które przy analizach ryzyka nie mogą być pomijane. Zapisy dyrektywy 2022/2557 wymagają aby ze względu na powiązanie między fizycznym bezpieczeństwem a cyberbezpieczeństwem podmiotów krytycznych wdrażanie dyrektyw 2022/2555 oraz 2022/2557 było skoordynowane.

Ze względu na przedmiot niniejszych wytycznych nie sposób pominąć rozporządzenia (UE) 2021/782 w sprawie praw i obowiązków pasażerów w transporcie kolejowym [5]. Rozporządzenie to wymaga, aby przewoźnicy kolejowi w porozumieniu z organami publicznymi oraz zarządcami infrastruktury i zarządcami stacji podejmowali odpowiednie działania w celu zapewnienia bezpieczeństwa osobistego pasażerów na stacjach kolejowych i w pociągach oraz w celu kontroli ryzyka. Tym samym przewoźnicy zobowiązani są do uwzględniania cyberbezpieczeństwa nie tylko cyfrowych systemów wpływających na bezpieczeństwo ruchu, ale także systemów wspomagających bezpieczeństwo osobiste pasażerów np. systemów informacji dla podróżnych, systemów rozgłoszeniowych, systemów wspomagających wzywanie pomocy.

1.2. Wyzwania dotyczące cyberbezpieczeństwa pasażerskiego taboru kolejowego

W przypadku nowoczesnego pasażerskiego taboru kolejowego zarówno odpowiedni poziom bezpieczeństwa ruchu kolejowego, jak i odpowiedni poziom ochrony transportu, zapewniający w szczególności bezpieczeństwo osobiste pasażerów, zapewniane są z wykorzystaniem rozwiązań cyfrowych, które powinny być odpowiednio chronione przed cyberzagrożeniami. Stosowne zabezpieczenia powinny zapewniać wysoki i jednocześnie podobny poziom ochrony w różnych obszarach, tak aby nie pozostawiać obszarów niezabezpieczonych lub wyraźnie słabiej zabezpieczonych, które mogłyby zostać wykorzystane do cyberataku. Wymagane i opcjonalne zabezpieczenia przed cyberatakami, przy uwzględnieniu zasady równomiernego zabezpieczania się przed zagrożeniami bezpieczeństwa ruchu, ochrony transportu i cyberzagrożeniami, oraz sposób ich dokumentowania i weryfikowania dla konkretnych nowych typów pasażerskiego taboru kolejowego przedstawiono w rozdziale 4.

Rozdział ten definiuje zasady dokumentowania i weryfikowania spójności bezpieczeństwa, ochrony i cyberbezpieczeństwa dla nowego pasażerskiego taboru kolejowego. Wyzwaniem dla każdego nowego typu pozostaje dobór i zabudowa zabezpieczeń w taborze przy uwzględnieniu różnych ryzyk wynikających z cyberzagrożeń, w tym ewentualnego wykorzystywania nieuprawnionego dostępu do systemów i/lub urządzeń.

Długi, kilkudziesięcioletni, okres eksploatacji pasażerskiego taboru kolejowego wymaga uwzględniania cyberzagrożeń podczas eksploatacji taboru ze szczególnym uwzględnieniem z jednej strony ryzyk związanych ze zmianami otoczenia, np. rozwojem narzędzi do łamania zabezpieczeń, a z drugiej ryzyk związanych z dostępem personelu utrzymaniowego do wszelkich zastosowanych rozwiązań cyfrowych realizujących funkcje wykorzystywane dla zapewniania bezpieczeństwa ruchu, ochrony transportu czy ochrony rozwiązań cyfrowych przed cyberzagrożeniami. Sugestie w tym zakresie zebrano i omówiono w rozdziale 5. Wyzwanie to dotyczy zarówno taboru, który będzie budowany i akceptowany zgodnie z niniejszymi wytycznymi jak i taboru, który już jest w eksploatacji bądź zostanie do niej przekazany bez wykorzystania niniejszych wytycznych.

Utrzymywanie wysokiego i zrównoważonego pomiędzy różnymi obszarami poziomu zabezpieczeń przed zagrożeniami bezpieczeństwa ruchu, ochrony transportu i cyberzagrożeniami nabiera nowego wymiaru w przypadku wprowadzania modyfikacji w istniejącym taborze. Dotycz to zarówno taboru projektowanego i budowanego zgodnie z niniejszymi wytycznymi jak i istniejącego zaprojektowanego i zbudowanego bez ich bezpośredniego uwzględnienia. Sugestie w tym zakresie zebrano i omówiono w rozdziale 6.

1.3. Jak należy rozumieć cyberbezpieczeństwo

„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]*

Natomiast „cyberbezpieczeństwo” i „cyberzagrożenia” definiuje „akt o cyberbezpieczeństwie”, czyli Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2019/881 z dnia 17 kwietnia 2019 r. w sprawie ENISA (Agencji Unii Europejskiej ds. Cyberbezpieczeństwa) oraz certyfikacji cyberbezpieczeństwa w zakresie technologii informacyjno-komunikacyjnych oraz uchylenia rozporządzenia (UE) nr 526/2013.

> *„cyberbezpieczeństwo” oznacza działania niezbędne do ochrony sieci i systemów informatycznych, użytkowników takich systemów oraz innych osób przed cyberzagrożeniami;*
>
> *„cyberzagrożenie” oznacza wszelkie potencjalne okoliczności, zdarzenie lub działanie, które mogą wyrządzić szkodę, spowodować zakłócenia lub w inny sposób niekorzystnie wpłynąć w przypadku sieci i systemów informatycznych, użytkowników takich systemów oraz innych osób;*
>
> *[zgodnie z art. 2 Rozporządzenia 2019/881]*

Rozporządzenie 2019/881 nie ma zastosowania do przewoźników kolejowych, więc zostało pominięte w zestawieniu dokumentów referencyjnych (rozdział 7.). Zawiera jednak obowiązującą definicję cyberbezpieczeństwa, która została przywołana powyżej.

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 zarządców i przewoźników kolejowych 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 czy sprzedaży biletów). 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.

Równolegle dyrektywa w sprawie odporności podmiotów krytycznych [4] określa „środki w zakresie odporności” wprowadzane przez podmioty krytyczne jako:

… odpowiednie i proporcjonalne środki techniczne, środki bezpieczeństwa i środki organizacyjne służące zapewnieniu odporności tych podmiotów, w oparciu o oceny ryzyka przeprowadzane przez państwa członkowskie oraz przeprowadzane przez podmioty krytyczne, obejmujące środki niezbędne w celu:

a) zapobiegania incydentom, z należytym uwzględnieniem środków zmniejszania ryzyka związanego z katastrofami i przystosowania się do zmiany klimatu;

b) zapewnienia odpowiedniej fizycznej ochrony ich budynków i terenów oraz infrastruktury krytycznej, z należytym uwzględnieniem na przykład zainstalowania ogrodzeń, budowy barier, narzędzi i procedur monitorowania terenu podlegającego ochronie, sprzętu do wykrywania i kontroli dostępu;

c) odpowiedzi na incydenty, stawiania im oporu i łagodzenia ich skutków, z należytym uwzględnieniem wdrażania procedur i protokołów zarządzania ryzykiem i zarządzania kryzysowego, a także procedur ostrzegawczych;

d) odtworzenia po incydentach, z należytym uwzględnieniem środków na rzecz ciągłości działania oraz identyfikacji alternatywnych łańcuchów dostaw w celu przywrócenia świadczenia usługi kluczowej;

e) zapewnienia odpowiedniego zarządzania bezpieczeństwem pracowników, z należytym uwzględnieniem środków takich jak ustanowienie kategorii personelu wykonującego funkcje krytyczne, ustanowienie praw dostępu do budynków i terenów, infrastruktury krytycznej i informacji szczególnie chronionych, ustanowienie procedur sprawdzenia przeszłości zgodnie z art. 14, wyznaczenie kategorii osób podlegających takim procedurom sprawdzenia przeszłości oraz określenie odpowiednich wymogów szkoleniowych i kwalifikacji;

f) zwiększania świadomości odpowiedniego personelu na temat środków, o których mowa w lit. a)–e), z należytym uwzględnieniem szkoleń, materiałów informacyjnych i ćwiczeń.

[zgodnie z art. 13 Dyrektywy 2022/2557]

Pociąga to za sobą konieczność co najmniej zapewniania odpowiedniej ochrony fizycznej, właściwego zabezpieczenia przed nieuprawnionym dostępem w odniesieniu do cyfrowych systemów i urządzeń, jako że dostęp taki może być wykorzystywany do przeprowadzania cyberataków.

2. Definicje

Bezpieczeństwo, ochronę i cyberbezpieczeństwo w kontekście regulacji prawnych UE należy rozumieć zgodnie z doprecyzowaniem odpowiednio w podrozdziałach 2.1., 2.2. i 2.3. Zawarte w tych podrozdziałach szerokie postrzeganie bezpieczeństwa transportu kolejowego nie ograniczające się do bezpieczeństwa ruchu kolejowego powinno być uwzględniane podczas opracowywania dokumentów, których charakter, zawartość i struktura zostały zdefiniowane w rozdziale 4.

2.1. Bezpieczeństwo z punktu widzenia interoperacyjności systemu kolei

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 poniżej w ramce za dyrektywą bez rozróżniania wymagań dla systemu kolei i wymagań dla poszczególnych podsystemów współtworzących system kolei. Jednocześnie pod ramką dodano dwa wymagania ogólne związane z koniecznością zapewnienia odpowiedniego poziomu ochrony transportu.

1.1. *Bezpieczeństwo*

1.1.1.	*Projektowanie, budowa lub montaż, utrzymywanie i monitorowanie składników kluczowych dla bezpieczeństwa, a zwłaszcza składników dotyczących ruchu pociągów, muszą gwarantować bezpieczeństwo na poziomie odpowiadającym celom określonym dla sieci, w tym w szczególnie trudnych warunkach.*
1.1.2.	*Parametry dotyczące styku koło/szyna muszą spełniać wymogi w zakresie stabilności wymagane celem zagwarantowania bezpiecznego przejazdu przy maksymalnej dozwolonej prędkości. Parametry układu hamulcowego muszą gwarantować, że możliwe jest zatrzymanie pociągu na danej drodze hamowania przy maksymalnej dozwolonej prędkości.*
1.1.3.	*Stosowane składniki muszą być odporne na wszelkie normalne i nadzwyczajne obciążenia, jakie zostały określone w okresie ich użytkowania. Wpływ wszelkich przypadkowych awarii na bezpieczeństwo musi zostać ograniczony przy użyciu właściwych środków.*
1.1.4.	*Projekt instalacji stałych i taboru oraz wybór użytych materiałów muszą być skoncentrowane na ograniczeniu wywoływania, rozprzestrzeniania oraz skutków ognia i dymu w przypadku pożaru.*
1.1.5.	*Wszelkie urządzenia przeznaczone do obsługi przez użytkowników muszą być tak zaprojektowane, aby nie szkodzić bezpiecznemu funkcjonowaniu urządzeń lub zdrowiu bądź bezpieczeństwu użytkowników przy ich przewidywanym użyciu, jednakże nie w sposób niezgodny z zamieszczonymi na nich instrukcjami.*
1.1.6.	*Należy podjąć odpowiednie kroki celem zapobieżenia dostępowi lub niepożądanym włamaniom do instalacji. Należy podjąć kroki w celu ograniczenia zagrożenia dla osób narażonych, w szczególności w chwili przejazdu pociągu przez stację. Infrastruktura ogólnie dostępna musi być zaprojektowana i wykonana w taki sposób, aby ograniczyć wszelkie ryzyko związane z bezpieczeństwem ludzi (stabilność, pożar, dostęp, ewakuacja, perony itd.). Należy ustanowić właściwe przepisy celem uwzględnienia szczególnych warunków bezpieczeństwa w bardzo długich tunelach i na wiaduktach.*
1.1.7.	*Funkcjonowanie systemów dostaw energii nie może szkodzić bezpieczeństwu pociągów lub ludzi (użytkowników, obsługi, osób mieszkających w pobliżu torowiska oraz osób trzecich).*
1.1.8.	*Instalacje oraz procedury wykorzystywane w zakresie sterowania muszą umożliwiać przejazd pociągów na poziomie bezpieczeństwa odpowiadającym założeniom określonym dla sieci. Systemy sterowania muszą w sposób ciągły zapewniać bezpieczny przejazd pociągów posiadających zezwolenie na jazdę również w przypadkach awarii.*
1.1.9.	*Dostosowanie zasad eksploatacji sieci i kwalifikacji maszynistów oraz personelu pokładowego i personelu w centrach kontrolnych musi zapewniać bezpieczne funkcjonowanie sieci, przy uwzględnieniu różnych wymogów dla usług transgranicznych i krajowych. Działania i przerwy związane z utrzymaniem, wyszkolenie i kwalifikacje personelu odpowiedzialnego za utrzymanie i centrum kontrolnego oraz system zapewnienia jakości stworzony przez zainteresowanych operatorów w centrach kontroli i utrzymania muszą gwarantować wysoki*

poziom bezpieczeństwa.

1.1.10. Zapewniony zostać musi odpowiedni poziom uczciwości i niezawodności w zakresie gromadzenia i przekazywania informacji dotyczących bezpieczeństwa.

1.1.11. Instalacje techniczne oraz procedury używane w centrach utrzymania muszą zapewniać bezpieczne funkcjonowanie podsystemu i nie stanowić zagrożenia dla bezpieczeństwa.

[zgodnie z Załącznikiem III do Dyrektywy 2016/797]

1.1.12. Monitorowanie stref dostępnych dla pasażerów i osób postronnych (np. odprowadzających podróżnych) musi gwarantować odpowiednie wykrywanie sytuacji niebezpiecznych i umożliwiać podejmowanie stosownych działań.

1.1.13. Monitorowanie stref, pomieszczeń, kontenerów i szaf niedostępnych dla osób nieupoważnionych musi gwarantować właściwy poziom zabezpieczeń przed wandalami, złodziejami oraz osobami nieupoważnionymi posiadającymi inne złe zamiary oraz uruchamianie właściwych systemów i procedur.

Spełnianie **wymagania zasadniczego 'bezpieczeństwo'** rozumianego jako ogół wymagań zacytowanych powyżej za załącznikiem III do dyrektywy 2016/797, przez poszczególne podsystemy systemu kolejowego, w tym pasażerski tabor kolejowy, podlega weryfikacji WE. Stosowane w tym zakresie zasady krótko omówiono w rozdziale 3.1. Zapewnienie spełnienia wymagań ogólnych zdefiniowanych w punktach 1.1.12. oraz 1.1.13. powyżej wykracza poza wymagania dyrektywy w sprawie interoperacyjności kolei. Stosowne zasady są jednak uwzględnione w niniejszych wytycznych, w szczególności w rozdziale 4.1., ze względu na konieczność zapewnienia odpowiedniego poziomu zabezpieczeń systemów zapewniających ochronę transportu.

2.2. Ochrona

Jak już wspomniano w poprzednim rozdziale, 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, w tym w szczególności dla zapewnienia bezpieczeństwa osobistego pasażerów o którym mówi rozporządzenie w sprawie praw i obowiązków pasażerów [5], stosuje się:

a) monitorowanie stref dostępnych publicznie (patrz 1.1.12.) oraz
b) monitorowanie stref niedostępnych publicznie (patrz 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. Definiowanie i analizowanie środków ochrony powinno uwzględniać także kontekst dyrektywy w sprawie odporności podmiotów krytycznych [4].

2.3. Cyberbezpieczeństwo

Cyberbezpieczeństwo, zgodnie z zapisami rozdziału 1.3. niniejszych wytycznych, obejmuje zarówno bezpieczeństwo systemów IT jak i bezpieczeństwo systemów OT. Zwrócić przy tym należy uwagę na fakt, że 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 [6] 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.

Wytyczne dotyczące cyberbezpieczeństwa pasażerskiego taboru kolejowego ze względu na ich zakres i przeznaczenie obejmują wymagania dla systemów OT zarówno zapewniających bezpieczeństwo ruchu kolejowego jak i wspomagających ochronę transportu.

UWAGA: Zarządzanie bezpieczeństwem informacji i ochrona systemów IT będą musiały być wdrożone przez przewoźników kolejowych zgodnie z normami serii PN-EN ISO/IEC 27000, w tym w szczególności zgodnie z normą PN-EN ISO/IEC 27001 [8] 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. Pewne wytyczne w tym zakresie podano w rozdziale 5. Niniejszych wytycznych.

2.4. Definicje poszczególnych określeń przyjęte dla potrzeb wytycznych

1) **Bezpieczeństwo** – brak niedopuszczalnego ryzyka [9].
2) **Cyberbezpieczeństwo** – działania niezbędne do ochrony sieci i systemów informatycznych, użytkowników takich systemów oraz innych osób przed cyberzagrożeniami [2019/881].
3) **Cyberzagrożenie** – wszelkie potencjalne okoliczności, zdarzenie lub działanie, które mogą wyrządzić szkodę, spowodować zakłócenia lub w inny sposób niekorzystnie wpłynąć w przypadku sieci i systemów informatycznych, użytkowników takich systemów oraz innych osób [2019/881].
4) **Bezpieczeństwo sieci i systemów informatycznych** – 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].
5) **Dowód bezpieczeństwa** – udokumentowane wykazanie, że wyrób (np. system, podsystem lub urządzenie) jest zgodny z wyspecyfikowanymi wymaganiami bezpieczeństwa [9].
6) **Dowód spójności bezpieczeństwa, ochrony i cyberbezpieczeństwa** – dokument opracowany przez **wykonawcę** dla koncepcji, projektu lub realizacji, zgodny z wymaganiami rozdziału 4.1. niniejszego dokumentu, podlegający ocenie zgodnie z wymaganiami rozdziału 4.2. niniejszego dokumentu.
7) **Wewnętrzny zespół odpowiedzialny za bezpieczeństwo** – część struktury wewnętrznej, która koordynuje wewnętrzne procesy przewoźnika kolejowego w odniesieniu do bezpieczeństwa.
8) **Kompetentna niezależna jednostka inspekcyjna** – jednostka posiadającą akredytację Polskiego Centrum Akredytacji dla jednostki oceniającej analizy i wyceny ryzyka realizowane zgodnie z rozporządzeniem w sprawie oceny i wyceny ryzyka [6, 7] dla pięciu podsystemów strukturalnych – podsystemów „Infrastruktura", „Energia", „Sterowanie – urządzenia przytorowe" oraz „Tabor" i „Sterowanie – urządzenia pokładowe" prowadząca weryfikację '**dowodu spójności bezpieczeństwa, ochrony i cyberbezpieczeństwa**'.
9) **Ryzyko** – kombinacja oczekiwanej częstotliwości występowania szkody oraz oczekiwanej dotkliwości takiej szkody [9].
10) **Wykonawca** – podmiot opracowujący koncepcję lub projekt względnie budujący pasażerski tabor kolejowy lub zabudowujący urządzenia w takim taborze lub wprowadzający zmiany w koncepcji, projekcie lub budowie pasażerskiego taboru kolejowego lub jego wyposażeniu.
11) **Wymagania ogólne w zakresie ochrony** – wymagania 1.1.12 i 1.1.13. podane w rozdziale 2.1. niniejszych wytycznych (zdefiniowane jako wymagania ogólne dla potrzeb ochrony transportu).
12) **Wymaganie zasadnicze 'bezpieczeństwo'** – wymagania od 1.1.1. do 1.1.11. podane w rozdziale 2.1. niniejszych wytycznych (za załącznikiem III do dyrektywy w sprawie interoperacyjności [1]).

3. Interoperacyjność i cyberbezpieczeństwo

Konieczność zapewnienia interoperacyjności systemu kolei wynika z dyrektywy 2016/797 [1], a konieczność zapewnienia cyberbezpieczeństwa transportu kolejowego z dyrektywy 2016/1148 [2] zastąpionej dyrektyą 2022/2555 [3]. Dyrektywy te, a także dokumenty szczegółowe wydawane na ich podstawie nie zawierają zapisów pozwalających na prześledzenie relacji między wymaganiami formalnymi w zakresie interoperacyjności i wymaganiami formalnymi w zakresie cyberbezpieczeństwa. Niezależnie od tego wymagania z obu obszarów będą, w wielu przypadkach, jednocześnie miały zastosowanie do tych samych cyfrowych rozwiązań technicznych stosowanych np. w pasażerskim taborze kolejowym.

3.1. Interoperacyjność

Zgodnie z zapisami dyrektywy 2016/797 [1] interoperacyjność to *„zdolność systemu kolei do zapewnienia bezpiecznego i nieprzerwanego ruchu pociągów o charakterystykach odpowiednich dla danych linii kolejowych, zależna od wszystkich warunków technicznych, prawnych i eksploatacyjnych, których zachowanie zapewnia dotrzymanie zasadniczych wymagań”*. Wśród sześciu wymagań zasadniczych zdefiniowanych w dyrektywie jedno, wymaganie zasadnicze ‘bezpieczeństwo’, powiązane jest bezpośrednio z wymaganiami cyberbezpieczeństwa w odniesieniu do rozwiązań technicznych, które mają charakter cyfrowy.

Jednoczesne stosowanie wymagań interoperacyjności i cyberbezpieczeństwa ma więc zastosowanie np. do pokładowych systemów zapewniających łączność pomiędzy maszynistą a dyżurnymi ruchu, czy pokładowych instalacji Europejskiego Systemu Sterowania Pociągiem, systemu ETCS.

3.2. Ochrona

Zgodnie z zapisami rozporządzenia 2021/782 [5] przewoźnicy kolejowi w porozumieniu z organami publicznymi oraz zarządcami infrastruktury i zarządcami stacji zobowiązani są podejmować odpowiednie działania w celu zapewnienia bezpieczeństwa osobistego pasażerów na stacjach kolejowych i w pociągach. Działania takie powinny wynikać z procesów kontroli ryzyka rozpoczynających się od identyfikacji zagrożeń, w tym identyfikacji cyberzagrożeń w pasażerskim taborze kolejowym. Działań takich od przewoźników kolejowych wymaga także dyrektywa w sprawie odporności podmiotów krytycznych [4].

Systemy cyfrowe wykorzystywane dla zapewnienia bezpieczeństwa osobistego pasażerów w pociągach takie jak systemy monitoringu wizyjnego, informacji pasażerskiej, czy hamulca pasażera powinny być uwzględniane przy rozpatrywaniu cyberbezpieczeństwa pasażerskiego taboru kolejowego.

3.3. Cyberbezpieczeństwo

Główne zagrożenia dla cyberbezpieczeństwa w transporcie opisano w rozdziale 3.3.1. W rozdziale 3.3.2. przedstawiono przyjętą klasyfikację funkcjonalności pasażerskiego taboru kolejowego. Zidentyfikowane w toku prac nad wytycznymi typy nieuprawnionej ingerencji w cyberbezpieczeństwo taboru przedstawiono w rozdziale 3.3.3. Przegląd środków wykorzystywanych dla zapewnienia cyberbezpieczeństwa w transporcie kolejowym opisano w rozdziale 3.3.4., natomiast środki cyberbezpieczeństwa dla pasażerskiego taboru kolejowego w rozdziale 3.3.5.

3.3.1. Główne zagrożenia dla cyberbezpieczeństwa w transporcie kolejowym

Wstępne wskazanie głównych zagrożeń oparto na dokumencie „Transport cybersecurity toolkit” opracowanym i udostępnionym w roku 2020 przez Komisję Europejską. Zgodnie z zapisami tego dokumentu zarówno osoby fizyczne jak i organizacje mogą umyślnie lub nieumyślnie ujawniać i wykorzystywać podatności, które mogą potencjalnie powodować incydenty i wpływać na usługi transportowe, w tym na ich bezpieczeństwo, ochronę, działanie, finanse i reputację. Aktorzy zagrożeń to między innymi grupy sponsorowane przez organy państwowe, cyberprzestępcy, cyberterroryści,

haktywiści[1], hakerzy (w tym skrypt krakerzy[2]) oraz osoby legalnie posiadające dostęp do wewnętrznych informacji (w tym uprzywilejowane osoby posiadające legalny dostęp do takich informacji).

Najważniejszymi destrukcyjnymi aktorami celowo atakującymi organizacje transportowe są cyberprzestępcy, osoby legalnie posiadające dostęp do wewnętrznych informacji, państwa narodowe i grupy sponsorowane przez organy państwowe. Przeciwnicy, tacy jak cyberprzestępcy, przeprowadzają zmasowane kampanie cyberataków i często starają się uzyskiwać pieniężne profity.

Legalnie posiadający dostęp do wewnętrznych informacji znają specyfikę organizacji, dla których pracują, i często doskonale zdają sobie sprawę z subtelnych luk w zabezpieczeniach. Wewnętrzni aktorzy zagrożeń to między innymi niezadowoleni pracownicy, dostawcy i indywidualni wykonawcy. W miarę wzrostu globalnych napięć geopolitycznych, państwa narodowe i grupy sponsorowane przez organy państwowe stawiają sobie długoterminowe cele strategiczne. Często próbują one ukryć się w głębi struktury organizacji i gromadzić wrażliwe informacje. Po zdobyciu przyczółków w systemach cyfrowych, napastnicy sponsorowani przez organy państwowe starają się zająć pozycje, które zagwarantują spowodowanie jak największych szkód. Na przykład, mogą zaatakować systemy innych organizacji, wykorzystując połączenia sieciowe zinfiltrowanej organizacji.

Do aktorów zagrożeń zalicza się także osoby posiadające dostęp do wewnętrznych informacji, które mogą nieumyślnie lub przypadkowo podejmować działania skutkujące zdarzeniami związanymi z cyberbezpieczeństwem, a w najgorszych przypadkach incydentami cybernetycznymi mającymi wpływ na bezpieczeństwo i ochronę usług transportowych.

Zgodnie z informacjami zawartymi –w dokumencie „Transport cybersecurity toolkit" istnieje wiele cyber-zagrożeń ukierunkowanych na transport: rozproszone blokowania usług (DDoS), blokowania usługi (DoS), kradzieże danych, rozpowszechnianie złośliwego oprogramowania (malwaru), phishing, manipulacje oprogramowaniem, nieuprawniony dostęp, ataki destrukcyjne, fałszowanie lub obchodzenie procesów decyzyjnych angażujących operatorów cyberbezpieczeństwa, maskarady tożsamości, nadużywanie przywilejów dostępu, inżynieria społeczna, niszczenie wizerunku, podsłuchy, niewłaściwe wykorzystywanie aktywów, czy manipulacje sprzętem.

Dokument ten podaje, że w oparciu o obszerne badania literaturowe publicznie dostępnych dokumentów oraz wywiady z ekspertami uznano, że do najpilniejszych pojawiających się cyber-zagrożeń mających wpływ na transport należą następujące cztery zagrożenia:

1. **złośliwe oprogramowanie (malware)**
   (złośliwe oprogramowanie, które może mieć potencjalny wpływ na osoby lub organizacje w różnych rodzajach transportu)
2. **(rozproszone) blokowania usług (DDoS & DoS)**
   (ataki cybernetyczne uniemożliwiające osobom fizycznym lub organizacjom dostęp do odpowiednich usług i zasobów transportowych)
3. **nieuprawnione uzyskiwanie dostępu i kradzieże**
   (nieuprawniony dostęp, przywłaszczenie i wykorzystanie krytycznych zasobów)
4. **manipulacje oprogramowaniem**
   (ataki cybernetyczne na oprogramowanie w celu zmiany jego działania i przeprowadzania specyficznych ataków)

Te cztery zagrożenia w wyniku wojny za wschodnią granicą Polski uzupełnić należy o:

5. **zdalne (uprawnione) wyłączenie (remote authorized shutdown R(A)S)**
   (realizowane na odległość wyłączenie systemu przez osobę/podmiot, uznającą(-y) się za uprawnioną(-y), a nawet zobowiązaną(-y) do wyłączenia systemu)

Poszczególne cyberzagrożenia należy rozumieć następująco:

[1] Haktywiści to osoby, które używają komputerów i sieci do promowania celów społecznych i politycznych, zwłaszcza wolności słowa, praw człowieka i dostępu do informacji.

[2] Skrypt krakerzy to osoby które używają programów i skryptów napisanych przez innych bez dogłębnej znajomości zasad ich działania, jedynie po to, aby uzyskać nieuprawniony dostęp do komputerowych kont użytkowników lub plików lub żeby przeprowadzać ataki na systemy komputerowe.

Ad. 1. złośliwe oprogramowanie (Malware)
Złośliwe oprogramowanie (Malware) obejmuje szkodliwe programy, które mogą obejmować różne rodzaje aplikacji, takie jak wirusy, trojany, robaki, ransomware, cryptocurrency-miners oraz wszelkie aplikacje, które mogą potencjalnie mieć negatywny wpływ na organizacje lub osoby prywatne w różnych rodzajach transportu.

Ograniczanie rozprzestrzeniania się złośliwego oprogramowania przeznaczonego do celowego uszkadzania komputerów, serwerów, klientów, sieci lub wszystkich tych elementów jest jednym z głównych priorytetów cyberbezpieczeństwa we wszystkich rodzajach transportu. Typowy wektor ataku może obejmować wiadomości e-mail typu phishing skierowane do pracowników. Inne wektory ataku mogą obejmować różne i wyrafinowane strategie inżynierii społecznej, takie jak podłączenie klucza USB do wolnego portu (np. w celu naładowania telefonu komórkowego).

Klikając hiperłącza w podejrzanych wiadomościach e-mail lub otwierając załączniki z plikami, użytkownik może nieświadomie instalować oprogramowanie lub świadomie narażać usługi i zasoby transportowe na niebezpieczeństwo.

Na przykład, cyberatak ransomware WannaCry dotknął ponad 150 krajów i zainfekował ponad 230 000 systemów. Chodziło o oprogramowanie ransomware, które zwykle rozprzestrzenia się za pośrednictwem wiadomości e-mail typu phishing zawierających złośliwe załączniki lub hiperłącza. Ten rodzaj ataku wykorzystuje socjotechnikę w celu wprowadzenia w błąd użytkowników systemu, aby zainstalowali (lub aktywowali) określone złośliwe oprogramowanie.

Ad. 2. (rozproszone) blokowania usług (DDoS & DoS)
Ataki typu rozproszone blokowanie usługi (DDoS – ang. Distributed Denial of Service) oraz blokowanie usługi (DoS – ang. Denial of Service) wpływają na dostępność i osiągalność danych, usług, systemów i innych zasobów.

Tego typu ataki mogą trwać przez różny czas i mogą być skierowane na więcej niż jedną usługę lub system jednocześnie. Ataki DDoS wykorzystują wiele systemów (lub kanałów ataku) w celu przeciążenia docelowych usług lub systemów żądaniami. Udane ataki wpływają na zdolności usług i możliwości systemów w zakresie obsługi niespodziewanej liczby żądań. Skutkuje to blokowaniem dostępu do usług i zasobów.

Należy zauważyć, że dotknięte usługi i systemy należące do organizacji transportowych mogą być wykorzystywane do przeprowadzania ataków DDoS i DoS, których celem są określone systemy eksploatacyjne lub inne organizacje. Zaatakowane mogą zostać na przykład, korporacyjne systemy informacyjne (takie jak komputery osobiste i specjalizowane urządzenia) w celu uzyskania dostępu do technologicznych rozwiązań eksploatacyjnych, które mogą być podłączone do internetu lub do sieci dostępowej w celu przesyłania danych eksploatacyjnych. Połączenia między różnymi systemami i sieciami (takimi jak sieci korporacyjne, technologiczne rozwiązania eksploatacyjne i zdalny dostęp serwisowy) mogą stanowić podatności na ataki DDoS lub DoS na krytyczne usługi i systemy transportowe. Przykładowo, ataki DDoS i DoS mogą wykorzystywać powszechnie stosowane protokoły sieciowe i komunikacyjne, takie jak Web Services Dynamic Discovery (WS Discovery), które urządzenia IoT mogą wykorzystywać do automatycznego wykrywania każdego węzła w sieciach lokalnych (LAN). Jeśli urządzenia IoT posiadają podatności na ataki, osoby atakujące mogą je wykorzystać do wykrycia innych podłączonych urządzeń i przeprowadzenia ataków DDoS lub DoS.

Ad. 3. nieuprawniony dostęp i kradzież
Aktorzy zagrożeń mogą chcieć uzyskać logiczny lub fizyczny dostęp bez zezwolenia do sieci, systemu, aplikacji, danych lub innego zasobu w celu przeprowadzenia destrukcyjnych działań, w tym kradzieży wrażliwych danych lub zasobów (w tym zasobów fizycznych). Za działania destrukcyjne uznaje się zarówno ingerencje w programy i dane jak i fizyczną utratę programów i/lub danych.

Zagrożenia związane z nieuprawnionym dostępem i kradzieżą dotyczą aktywów poufnych i zastrzeżonych (w tym identyfikatorów osobistych, danych uwierzytelniających do kont uprzywilejowanych czy systemów oraz różnego typu poufnych i zastrzeżonych informacji). Zagrożenia te mogą wykorzystywać luki w systemach, jak również nieświadome osoby ujawniające dane wrażliwe, takie jak dane uwierzytelniające (login, hasło itp.) lub dane osobowe (e-mail, osobisty numer identyfikacyjny itp.).

W odniesieniu do nieuprawnionego dostępu kradzież tożsamości polega na bezprawnym wykorzystaniu danych osobowych lub niepowtarzalnych identyfikatorów w celu podszywania się pod osoby lub pod usługi czy systemy, w celu uzyskania dostępu do zasobów prywatnych lub zastrzeżonych (w tym np. zasobów finansowych i fizycznych). Takie cyberzagrożenia mogą być również skierowane przeciwko aktywom fizycznym we wszystkich rodzajach transportu.

Ad.4. manipulacja oprogramowaniem
Nieprawidłowe konfiguracje i manipulacje oprogramowaniem oraz powiązanymi z nim systemami lub składnikami mogą mieć bezpośredni wpływ na stan bezpieczeństwa usług i systemów transportowych. Ataki cybernetyczne wykorzystujące manipulacje oprogramowaniem modyfikują ustawienia oprogramowania lub wpływają na integralność danych w celu zmiany zachowania systemów i usług.

Atakujący mogą celowo manipulować oprogramowaniem (lub jego częścią) w celu uzyskania korzyści z dostępu do wrażliwych zasobów (np. uzyskania nieuprawnionego dostępu, uniemożliwienia uprawnionym osobom lub systemom dostępu do niezbędnych zasobów, gromadzenia poufnych informacji, wprowadzania zmian w sposobie realizacji funkcji itp.).

Na przykład atakujący mogą celować w kanały komunikacyjne producentów w celu przesyłania destrukcyjnych aktualizacji oprogramowania usług i systemów (w tym technologii eksploatacyjnych) w czasie eksploatacji. Atakujący wykorzystują naruszone poświadczenia autoryzacji, aby uzyskać dostęp do zabezpieczonego interfejsu sieciowego zdalnego serwisu w celu zainstalowania zmanipulowanego oprogramowania i dalszego narażania na utratę bezpieczeństwa innych dostępnych usług i systemów. Następnie instalują zmanipulowane oprogramowanie, które narusza bezpieczeństwo docelowych usług i systemów lub atakują inne podłączone usługi i/lub systemy, lub wprowadzają zmiany oprogramowania, których celem jest umożliwienie cyberataku.

Ad. 5. zdalne (uprawnione) wyłączenie R(A)S
Lawinowy wzrost cyberataków od początku roku 2022 w związku z wojną za wschodnią granicą Polski pokazał, że poważnie potraktować należy także możliwość zdalnego wyłączenia różnego rodzaju systemów i urządzeń przez osoby względnie podmioty, które je wyprodukowały, konfigurowały, lub utrzymują, a które w świetle sytuacji prawnej lub militarnej uznają za konieczne skorzystanie z możliwości zdalnego wyłączenia systemu lub urządzenia oraz zdalnego usunięcia lub takiego zmodyfikowania ich oprogramowania, które uniemożliwi ich ponowne włączenie bez udziału producenta czy autoryzowanego serwisu.

W marcu 2023 roku Agencja Unii Europejskiej do spraw Cyberbezpieczeństwa ENISA udostępniła Threat Landscape dla Transport Sector za okres styczneń 2021 – październik 2022. Dokument ten zawiera analizę dla całego sektora transportu oraz wydzielone analizy dla transportu lotniczego, wodnego, kolejowego, drogowego, i dla „cross sector attacks”. Uwzględniono następujące typy ataków:

Ransomware (ransomware)
Ransomware definiuje się jako rodzaj ataku, w którym aktorzy zagrożeń przejmują kontrolę nad zasobami atakowanego i żądają okupu w zamian za przywrócenie dostępności zasobu.

Threats against data (zagrożenia dla danych)
Źródła danych są atakowane w celu uzyskania nieautoryzowanego dostępu i ujawnienia oraz manipulowania danymi w celu ingerencji w zachowanie systemów. Zagrożenia te są również podstawą wielu innych zagrożeń. Na przykład ataków ransomware lub DDoS, które mają na celu uniemożliwienie dostępu do danych i ewentualne pobranie okupu za przywrócenie dostępu. Technicznie rzecz biorąc, zagrożenia dla danych można sklasyfikować głównie jako naruszenia danych i wycieki danych. Naruszenie danych to celowy atak przeprowadzony przez cyberprzestępcę w celu uzyskania nieautoryzowanego dostępu i ujawnienia wrażliwych, poufnych lub chronionych danych. Wyciek danych to zdarzenie, które może spowodować niezamierzone ujawnienie wrażliwych, poufnych lub chronionych danych, na przykład z powodu błędnej konfiguracji, luk w zabezpieczeniach lub błędów ludzkich.

Malware (złośliwe oprogramowanie)
Złośliwe oprogramowanie to nadrzędny termin używany do opisania dowolnego oprogramowania (software) lub oprogramowania układowego (firmware) przeznaczonego do wykonywania nieautoryzowanego procesu, który będzie miał negatywny wpływ na poufność, integralność lub dostępność systemu. Tradycyjnie przykłady typów złośliwego kodu obejmują wirusy (viruses), robaki

(worms), trojany (trojan horses), oprogramowanie szpiegujące (spyware), oprogramowanie reklamowe (adware) oraz inne rozwiązania oparte na kodzie, które infekują hosta.

Denial of service (ataki DDoS)
Dostępność jest celem wielu zagrożeń i ataków, wśród których wyróżnia się DDoS. Ataki DDoS są ukierunkowane na dostępność systemów i danych i choć nie są nowym zagrożeniem, odgrywają znaczącą rolę w krajobrazie zagrożeń cyberbezpieczeństwa w sektorze transportu. Ataki mają miejsce, gdy użytkownicy systemu lub usługi nie są w stanie uzyskać dostępu do odpowiednich danych, usług lub innych zasobów. Brak dostępu może być skutkiem wyczerpania usługi i jej zasobów lub przeciążenia komponentów infrastruktury sieciowej. Obecne wydarzenia geopolityczne i aktywność haktywistów zwiększają liczbę ataków DDoS na organizacje transportowe.

Vulnerability exploitation (wykorzystywanie podatności)
Wykorzystywanie podatności odnosi się do wykorzystywania znanych podatności, w tym podatności typu zero-day.

Social engineering (inżynieria społeczna)
Inżynieria społeczna obejmuje szeroki zakres działań, które próbują wykorzystać ludzki błąd lub ludzkie zachowanie w celu uzyskania dostępu do informacji lub usług. Wykorzystuje się różne formy manipulacji, aby nakłonić ofiary do popełnienia błędów lub przekazania poufnych lub tajnych informacji. W cyberbezpieczeństwie inżynieria społeczna wykorzystywana jest do nakłaniania użytkowników do otwierania dokumentów, plików lub wiadomości e-mail, odwiedzania stron internetowych lub przyznawania nieupoważnionym osobom dostępu do systemów lub usług. Ten obszar zagrożeń obejmuje głównie następujące wektory: phishing, spear-phishing, whaling, smishing, vishing, kompromitacja służbowej poczty e-mail (business email compromise), oszustwa (fraud), podszywanie się (impersonation) i fałszerstwa (counterfeiting). Obecnie obserwowane są głównie ataki typu phishing i spear phishing wymierzone w użytkowników transportu oraz oszustwa, podszywanie się i fałszerstwa.

Attacks to suppliers and supply-chain attacks (ataki na dostawców i na łańcuchy dostaw)
Atak na łańcuch dostaw (supply-chain attack) jest wymierzony w relacje między organizacjami a ich dostawcami. Dokument *ENISA Threat Landscape for Supply Chain*, uznaje że atak jest atakiem tego typu jeśli składa się z kombinacji co najmniej dwóch ataków. Aby atak został sklasyfikowany jako atak na łańcuch dostaw, zarówno dostawca, jak i klient muszą być celami. Aktorzy zagrożeń korzystają z takich ataków, aby zdobywać przyczółki w organizacjach a następnie wykorzystywać możliwość szerokiego oddziaływania oraz bazy potencjalnych ofiar dalszych ataków. Obecnie obserwowane są zarówno ataki na łańcuch dostaw, jak i ataki na dostawców powodujące zakłócenia lub straty dla podmiotów w sektorze transportu.

Breach/intrusion (naruszenie/włamanie)
Naruszenie/włamanie odnosi się do incydentów, w których atak na system został potwierdzony lub upubliczniony, a atakujący uzyskali dostęp do systemów, ale szczegóły dotyczące sposobu naruszenia lub włamania nie są jasne.

Inne zagrożenia obejmują przypadki zbierania danych uwierzytelniających (**credential harvesting**) oraz fałszowania geolokalizacji (**spoofing of geolocation**) w sektorze morskim.

Istnieje także niewielki odsetek incydentów, w przypadku których nawet jeśli doszło do cyberataku, nie ma wystarczających informacji, aby można było je sklasyfikować. Są one określane jako incydenty niewyjaśnione (**unknowns**).

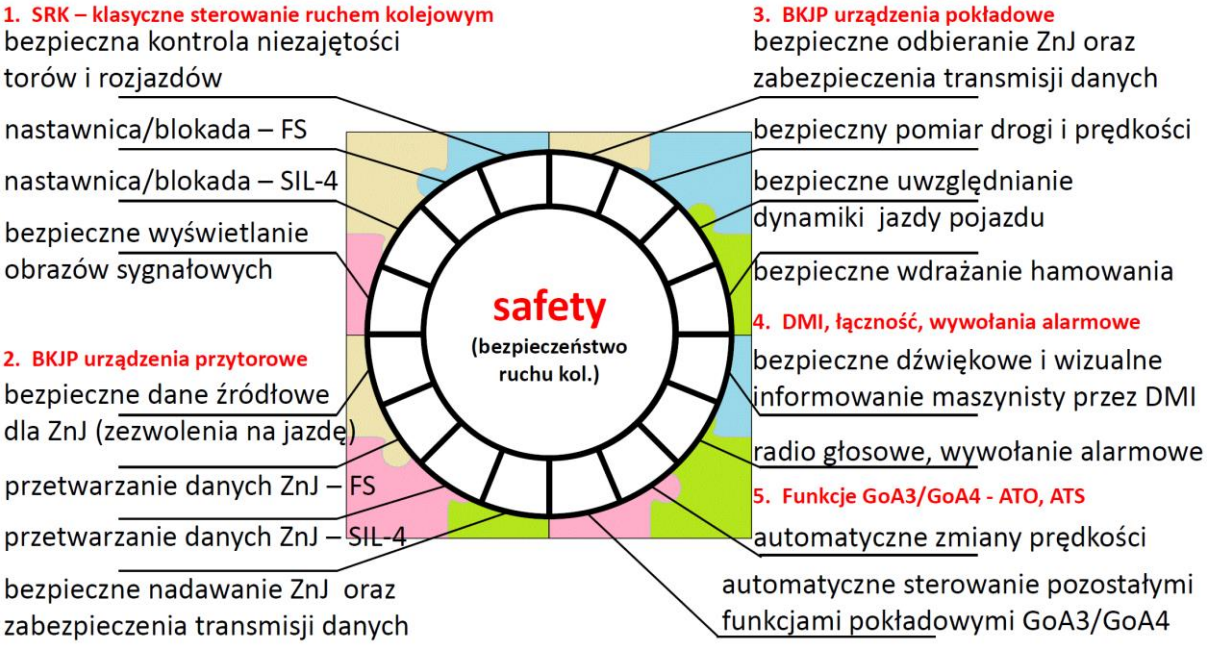
[ENISA Threat Landscape: Transport Sector, marzec 2023]

Analiza cyberataków z lat 2021 i 2022 wskazuje, że w transporcie kolejowym należy zabezpieczać się w szczególności przed:

a) ransomware,
b) zagrożeniami dla danych,
c) atakami DoS, DDoS, RDoS,
d) naruszeniami/włamaniami, oraz
e) wykorzystywaniem podatności.

3.3.2. Identyfikacja cyfrowych funkcjonalności, systemów i urządzeń taboru pasażerskiego

W taborze pasażerskim uwzględniając pociągi zespołowe oraz pociągi złożone z lokomotyw i wagonów wyróżniono dwa obszary funkcjonalności bezpieczeństwa ruchu „safety" oraz cztery obszary funkcjonalności bezpieczeństwa transportu „security". Obszary „safety" przedstawiono na Rysunku 1. Razem z dwoma komplementarnymi obszarami safety, które pozostają po stronie infrastruktury, natomiast obszary „security" przedstawiono na Rysunku 2.



Rysunek 1. Obszary funkcjonalności bezpieczeństwa ruchu kolejowego – safety
(źródło: opracowanie własne)

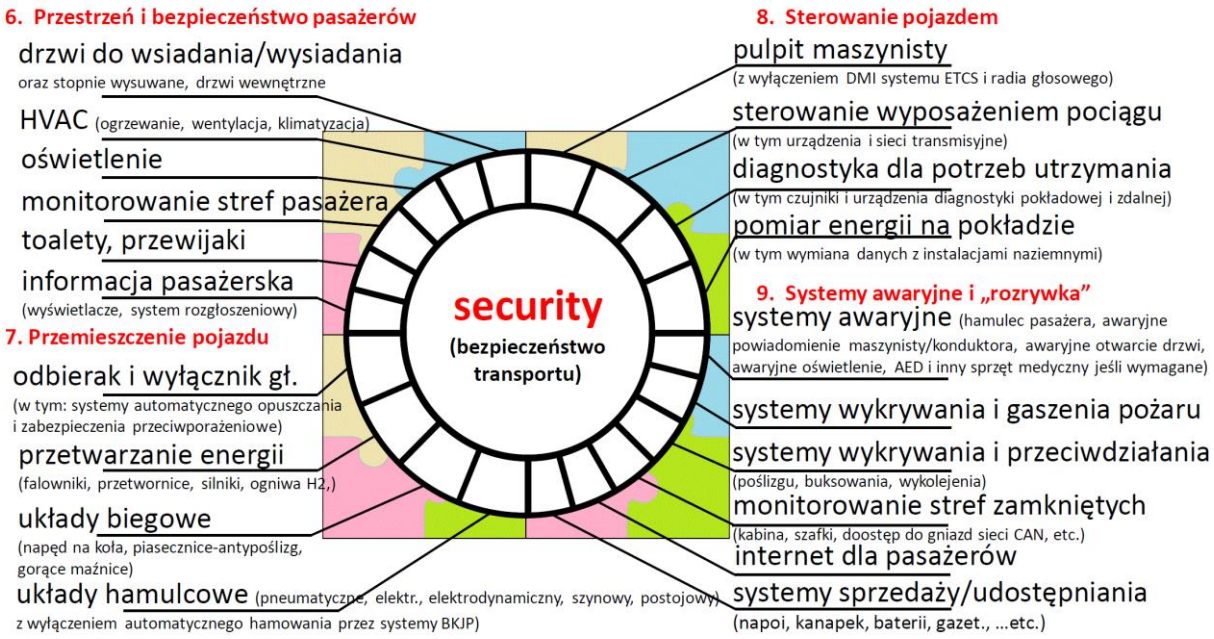
Poszczególnym obszarom od 1 do 4 odpowiadają karty kontrolne podane w rozdziale 4. Zaznaczyć przy tym należy, że karty kontrolne „1. SRK – klasyczne sterowanie ruchem kolejowym" oraz „2. BKJP urządzenia przytorowe" zawierają wartości referencyjne odpowiedzi na pytania kontrolne, opisujące charakterystykę wyposażenia infrastruktury torowej w systemy sterowania i systemy bezpiecznej kontroli jazdy, w odniesieniu do której oceniane jest bezpieczeństwo nadzoru nad prowadzeniem pojazdu przez maszynistę i/lub bezpieczeństwo automatycznego prowadzenia pojazdu dla pojazdów wyposażonych w automatyczną realizację funkcji wskazanych jako realizowane przez system dla poziomów automatyzacji GoA3 oraz GoA4 w normie IEC 62267:2009-07. Norma ta definiuje poziomy automatyzacji zgodnie z tabelą poniżej. Karty „3. BKJP – urządzenia pokładowe" oraz „4. DMI, łączność, wywołania alarmowe" oraz „5. Funkcje GoA3/GoA4 - ATO, ATS" zawierają pytania kontrolne wykorzystywane do oceny taboru pod kątem bezpieczeństwa ruchu kolejowego.

Tabela 1. Poziomy automatyzacji prowadzenia ruchu - GoA

poziomy automatyzacji ➔ / podstawowe funkcje w eksploatacji pociągu		Jazda na widoczność	Jazda nie automatyczna	ETCS wzorzec 2.3.0.d 3.4.0/3.6.0	Jazda półautomatyczna	ETCS wzorzec 4.0.0 TSI 2023	Jazda bez maszynisty	Jazda bez personelu	ETCS wzorzec 5.0.0 (?) TSI 2025
		TOS	NTO	NTO	STO	STO	DTO	UTO	UTO
		GoA0	GoA1	GoA1	GoA2	GoA2	GoA3	GoA4	GoA4
Zapewnienie bezpiecznego ruchu pociągów	Zagwarantowanie bezpiecznej drogi przebiegu dla pociągu	X (sterowanie napędami rozjazdów)	S	S	S	S	S	S	S
	Zapewnienie bezpiecznej separacji pociągów	X	S	S	S	S	S	S	S
	Zapewnienie bezpiecznej prędkości	X	X (częściowo nadzorowane przez system)	S	S	S	S	S	S
Prowadzenie pociągu	Kontrolowanie hamowania i przyspieszania	X	X	hamowanie - S przyspieszanie - X	S	S	S	S	S
Nadzór drogi przebiegu	Zapobieganie kolizji z obiektami	X	X	X	X	X	S	S	S
	Zapobieganie kolizji z osobami	X	X	X	X	X	S	S	S
Nadzór ruchu pasażerów	Sterowanie drzwiami dla pasażerów	X	X	X	X	X	X lub S	S	S
	Zapobieganie urazom pasażerów w przejściach między-wagonowych i przy wsiadaniu/wysiadaniu	X	X	X	X	X	X lub S	S	S
	Zapewnienie bezpiecznych warunków ruszania	X	X	X	X	X	X lub S	S	S
Obsługa pociągu	Włączanie i wyłączanie z ruchu	X	X	X	X	X	X	S	S
	Nadzór stanu pociągu	X	X	X	X	X	X	S	S
Wykrywanie i obsługa sytuacji awaryjnych	Realizacja diagnostyki pociągu, wykrywanie pożaru/dymu i wykolejenia, obsługa sytuacji awaryjnych (wywołania alarmowe/ewakuacje, nadzór)	X	X	X	X	X	X	S i/lub personel OCC	S i/lub personel OCC

X = odpowiedzialność personelu S = realizowane przez system techniczny

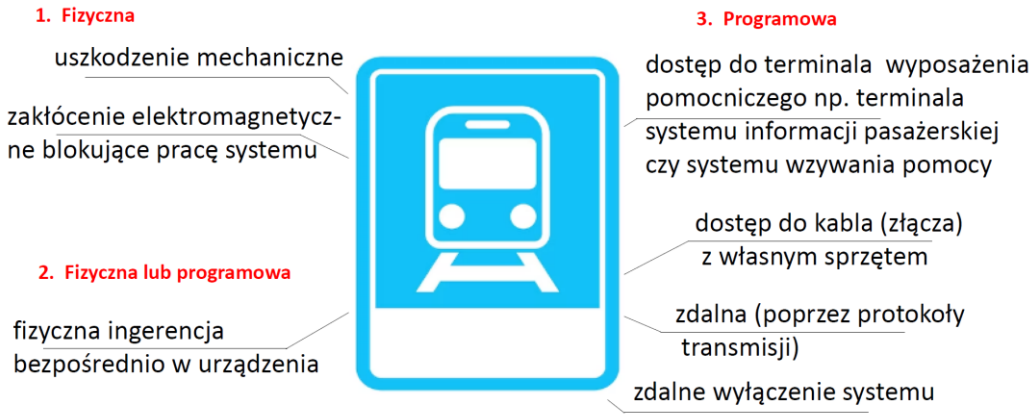
Rysunek 2. przedstawia obszary funkcjonalności od 6. do 9., którym odpowiadają karty kontrolne „6. Przestrzeń i bezpieczeństwo pasażerów", „7. Przemieszczanie pojazdu", 8. Sterowanie pojazdem" oraz 9. Systemy awaryjne i „rozrywka"" podane w rozdziale 4. zawierają pytania kontrolne wykorzystywane do oceny taboru pod kątem bezpieczeństwa transportu.



Rysunek 2. Obszary funkcjonalności bezpieczeństwa transportu - security
(źródło: opracowanie własne)

3.3.3. Typy nieuprawnionej ingerencji w tabor pasażerski i jego wyposażenie

Ingerencja w systemy pokładowe taboru kolejowego może się odbywać na wielu poziomach dostępu, od ingerencji mechanicznej, poprzez nieuprawnione podłączenie do sieci/systemu, aż po ingerencję zdalną, nie wymagającą obecności atakującego na pokładzie, bądź nawet w pobliżu pojazdu. Różne poziomy i przypadki ingerencji w tabor i jego wyposażenie przedstawia Rysunek 3.



Rysunek 3. Poziomy ingerencji w systemy pokładowe taboru

Ingerencja fizyczna polega na możliwości manipulacji bezpośrednio w miejscu lokalizacji urządzenia. Manipulacja ta może być mechaniczna, np. poprzez zmianę położeń przełączników, rozłączenie kabli, czy programowa – poprzez zmianę ustawień programowych urządzenia za pomocą dostępnego interfejsu człowiek-maszyna. Jej efektem może być np. wyłączenie urządzenia, aktywacja lub dezaktywacja jego funkcji, czy wreszcie zmiana w oprogramowaniu układowym (firmware) poprzez podmianę plików czy uruchomienie procedury aktualizacji z nośnika zewnętrznego bezpośrednio wpiętego fizycznie do portu atakowanego urządzenia.

Poprzez **dostęp do terminala** możliwe jest działanie w ramach oprogramowania urządzenia, a więc złośliwa aktywacja lub dezaktywacja jego funkcji, zmiana ustawień, parametrów pracy, czy wręcz przejście w tryb serwisowy, za pomocą którego można aktualizować lub zdezaktywować oprogramowanie.

Wykorzystując **dostęp do kabla** (do złącza lub portu wewnętrznego np. złącza USB) z własnym sprzętem, można podsłuchiwać transmisję, zakłócać ją, a także, w większości przypadków podłączyć się do sieci wewnętrznej własnym terminalem. Co umożliwia dalsze działanie w systemie na poziomie programowym. W najgorszym przypadku, dostęp do kabla daje takie same możliwości jak fizyczny dostęp do urządzenia czy do jego terminala z możliwością modyfikacji i/lub usuwania danych.
Ingerencja zdalna wykorzystuje dostępne protokoły transmisji zdalnej (jak bluetooh, wi-fi) wraz z otwartymi portami komunikacji, w celu połączenia się z systemem pokładowym pojazdu i wprowadzenia w nim modyfikacji.

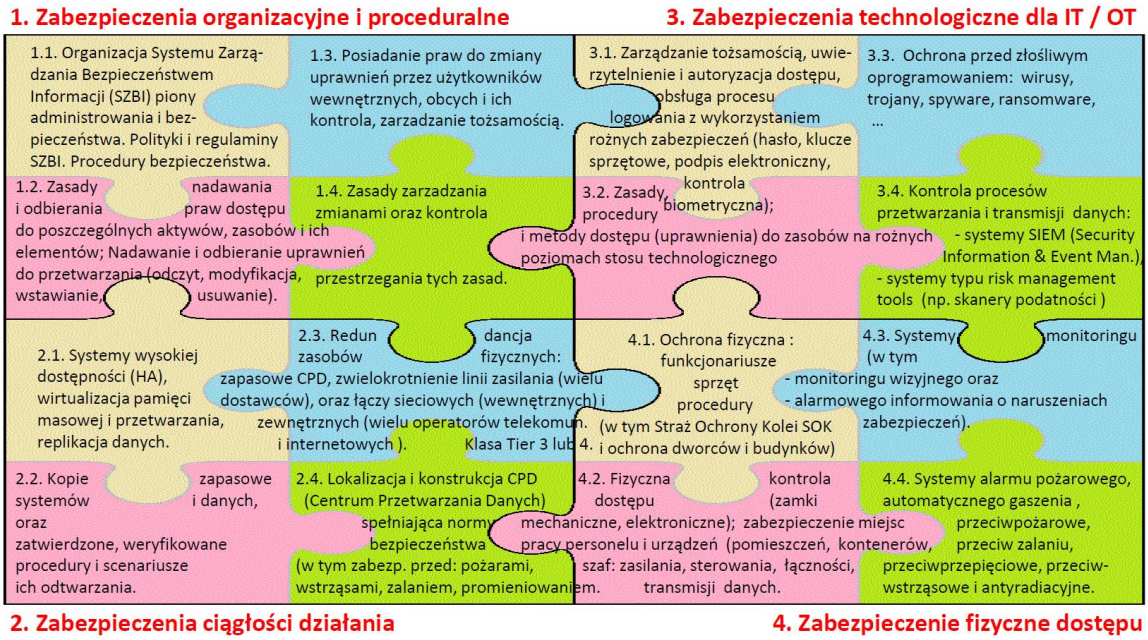
Poprzez **uszkodzenie mechaniczne** można doprowadzić systemy do dezaktywacji, zerwania transmisji pomiędzy systemami, bądź wymuszenie zadziałania/niezadziałania systemu w określonych warunkach.

Wytworzone intencjonalnie silne **zakłócenie elektromagnetyczne** może dezaktywować nie tylko systemy transmisji bezprzewodowej, ale również doprowadzić do resetu lub zawieszenia systemów komputerowych. Znane są na przykład stosunkowo prostej konstrukcji systemy do dezaktywacji dronów, oparte o emisję kierunkową silnego zakłócenia elektromagnetycznego.

Zdalne wyłączenie systemu jest najczęściej funkcją implementowaną w oprogramowaniu systemowym urządzeń przez producentów, np. na wypadek kradzieży urządzeń. Teoretycznie do tej funkcji nikt nie powinien mieć dostępu, a jej uruchomienie powinno być możliwe tylko w ściśle określonych warunkach. Nieautoryzowana aktywacja tej funkcji powoduje wyłączenie systemu i często brak możliwości jego ponownego uruchomienia bez udziału producenta lub jego autoryzowanego serwisu.

3.3.4. Środki cyberbezpieczeństwa w transporcie kolejowym

Wyróżnia się cztery grupy środków cyberbezpieczeństwa zapewniających zabezpieczenia dla różnych systemów IT i różnych systemów OT. Przyjęty podział środków cyberbezpieczeństwa przedstawiono schematycznie na Rysunku 4. w postaci, która wykorzystywana jest jako tło, na którym prezentowane są właściwe funkcjonalności systemów IT oraz OT.



Rysunek 4. Środki cyberbezpieczeństwa w transporcie kolejowym
(źródło: opracowanie własne)

Środki cyberbezpieczeństwa dzieli się na:

1. Zabezpieczenia organizacyjne i proceduralne

Zabezpieczenia organizacyjne i proceduralne powinny być uporządkowane i precyzyjnie opisane w ramach wdrożenia Systemu Zarządzania Bezpieczeństwem Informacji (SZBI) przez przewoźników kolejowych i zarządców infrastruktury kolejowej. W tym zakresie wyróżniono:

1.1. Organizację Systemu Zarządzania Bezpieczeństwem Informacji (SZBI) z uwzględnieniem zakresów odpowiedzialności i działań pionów administrowania i bezpieczeństwa oraz polityk i regulaminów SZBI oraz procedur bezpieczeństwa;

1.2. Zasady nadawania i odbierania praw dostępu do poszczególnych aktywów, zasobów i ich elementów. Nadawanie i odbieranie uprawnień do przetwarzania danych z rozbiciem na uprawnienia do odczytu, modyfikowania, wstawiania i usuwania danych;

1.3. Udostępnianie praw do zmiany uprawnień przez użytkowników wewnętrznych oraz obcych, a także ich kontrola, wraz z innymi zagadnieniami zarządzania tożsamością;

1.4. Zasady zarządzania zmianami w obrębie zabezpieczeń organizacyjnych i proceduralnych włącznie z kontrolą stosowania przyjętych zasad.

2. Zabezpieczenia ciągłości działania

Opracowywanie i stosowanie Planów Ciągłości Działania, czyli planów PCD, z uwzględnieniem wymagań normy ISO 22301 oraz dobrych praktyk. W tym zakresie wyróżniono:

2.1. Systemy wysokiej dostępności (HA), wirtualizacja pamięci masowej i wirtualizacji przetwarzania danych oraz replikacji danych;
2.2. Tworzenie i wykorzystywanie kopii zapasowych systemów (oprogramowania) oraz danych, w tym zatwierdzone i weryfikowane procedury i scenariusze odtwarzania systemów i danych w przypadku ich utraty bądź uszkodzenia;
2.3. Stosowanie redundancji zasobów fizycznych, w tym zapasowych Centrów Przetwarzania Danych, czyli centrów CPD, zwielokrotnienia linii zasilania elektrycznego (z uwzględnieniem opcji zasilania od wielu dostawców), zwielokrotniania łączy sieciowych (wewnętrznych) oraz łączy sieciowych zewnętrznych (z uwzględnieniem opcji korzystania z łączy od wielu operatorów telekomunikacyjnych i/lub internetowych). Klasa Tier 3 lub 4;
2.4. Zasady ustalania i akceptacji lokalizacji i konstrukcji centrów CPD z uwzględnieniem norm bezpieczeństwa, w tym między innymi zabezpieczeń przed: pożarami, wstrząsami, zalaniem, promieniowaniem.

3. Zabezpieczenia technologiczne dla systemów IT/OT

W zakresie stosowanych i możliwych do zastosowania zabezpieczeń technologicznych i procesowych wyróżniono następujące zabezpieczenia technologiczne (3.1., 3.2., 3.3.) oraz procesowe (3.4.):

3.1. Zarządzanie tożsamością, w tym uwierzytelnienie i autoryzacja dostępu oraz obsługa procesu logowania z wykorzystaniem rożnych stosowanych i możliwych do zastosowania zabezpieczeń (hasła, klucze sprzętowe, podpisy elektroniczne, kontrola biometryczna);
3.2. Definiowanie i stosowanie zasad, procedur i metod dostępu (uzyskiwania uprawnienia i korzystania z uprawnienia) do zasobów na rożnych poziomach stosu technologicznego;
3.3. Ochrona przed złośliwym oprogramowaniem, w tym między innymi przed wirusami, trojanami, oprogramowaniem szpiegującym (spyware), oprogramowaniem służącym do wymuszania okupów (ransomware);
3.4. Kontrola procesów przetwarzania i transmisji danych, w tym systemy typu SIEM (ang. *Security Information & Event Management*) oraz systemy i narzędzia zarządzania ryzykiem (ang. *risk management tools*), na przykład skanery podatności.

4. Zabezpieczenie fizyczne dostępu

Bezwzględnie koniecznym komplementarnym obszarem jest ochrona fizyczna. W tym zakresie wyróżniono:

4.1. Ochronę fizyczną infrastruktury, w tym w szczególności ochronę fizyczną budynków i pomieszczeń, w których znajdują się systemy i urządzenia z poziomu których możliwy mógłby być nieuprawniony dostęp do systemów informacyjnych IT lub eksploatacyjnych OT. Ochrona fizyczna obejmuje w szczególności funkcjonariuszy, sprzęt i procedury Straży Ochrony Kolei a także wymagania narzucane innym podmiotom zapewniającym ochronę fizyczną takich lokalizacji;
4.2. Mechaniczne i elektroniczne zamki oraz inne zabezpieczenia miejsc pracy personelu i miejsc działania systemów i urządzeń (pomieszczenia pracy dyżurnych ruchu, kabiny maszynistów, stanowiska pracy służb utrzymania, kontenery i szafy z urządzeniami: zasilania, sterowania, łączności, transmisji danych, itp. zarówno po stronie infrastruktury jak i taboru);
4.3. Systemy monitoringu obejmujące zarówno systemy monitoringu wizyjnego, jak i systemy alarmowe informujące o naruszeniach zabezpieczeń; oraz
4.4. Systemy zabezpieczeń przed katastrofami naturalnymi i budowlanymi w tym przeciwpożarowe takie jak systemy wykrywania pożarów, wykrywania dymu, automatycznego gaszenia pożarów, a także przeciwpowodziowe, chroniące przed zalaniem, przeciwprzepięciowe, przeciwwstrząsowe, czy antyradiacyjne.

3.3.5. Środki cyberbezpieczeństwa dla pasażerskiego taboru kolejowego

Z punktu widzenia oceny bezpieczeństwa, ochrony i cyberbezpieczeństwa oraz ich spójności funkcjonalnej dla danego typu pojazdu/pociągu pasażerskiego zastosowania nie będą miały zabezpieczenia typu 1. czyli organizacyjne i proceduralne stosowane przez przewoźnika kolejowego. Nie oznacza to, że producenci pojazdów nie potrzebują takich zabezpieczeń, ale tego typu zabezpieczenia stosowane przez producentów nie zabezpieczają wprost przewoźników podczas eksploatacji taboru. Jednocześnie zastrzec należy, że przewoźnicy i podmioty odpowiedzialne za

utrzymanie w sferze nadzoru nad utrzymaniem oraz rejestracji i obsługi zdarzeń eksploatacyjnych potrzebują zabezpieczeń typu 1.

Natomiast zabezpieczenia typu 2. zapewniające ciągłość działania rozwiązań technicznych oraz zabezpieczenia typu 3 czyli zabezpieczenia technologiczne oraz typu 4. czyli fizyczne zabezpieczenie dostępu do taboru powinny być stosowane w pasażerskim taborze kolejowym.

Pytania kontrolne wskazane w kartach kontrolnych 3. oraz 4. w zakresie bezpieczeństwa ruchu kolejowego – safety, oraz 5., 6., 7., 8. w zakresie bezpieczeństwa transportu czyli szeroko rozumianej ochrony – security, a także pytania kontrolne wskazane w karcie kontrolnej 9. Dedykowanej wprost do cyberbezpieczeństwa wskazują wymagane i opcjonalne zakresy zastosowania poszczególnych środków cyberbezpieczeństwa dla wybranych funkcjonalności taboru i jego wyposażenia.

3.4. Interoperacyjność a cyberbezpieczeństwo rozumiane jako odpowiedni poziom spójności 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 taborze posiadały certyfikaty zgodności WE wydane przez właściwe jednostki notyfikowane dla poszczególnych rozwiązań technicznych.
b) aby wszystkie składniki interoperacyjności zabudowywane w taborze 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 urządzeń podlegające pod wymóg uzyskania świadectwa typu przewidziane do zabudowy w taborze posiadały świadectwa typu wydane przez Prezesa UTK dla poszczególnych rozwiązań technicznych.
d) aby wszystkie urządzenia podlegające pod wymóg uzyskania świadectwa typu zabudowywane w taborze 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 podsystemy strukturalne (podsystemy „Tabor” oraz „Sterowanie – urządzenia pokładowe”) współtworzące tabor posiadały certyfikaty weryfikacji WE wydane przez właściwe jednostki notyfikowane dla poszczególnych podsystemów.
f) aby wszystkie podsystemy strukturalne (podsystemy „Tabor” oraz „Sterowanie – urządzenia pokładowe”) współtworzące tabor posiadały deklaracje weryfikacji WE wydane przez wykonawców poszczególnych podsystemów.
g) aby tabor tworzony przez podsystemy strukturalne (podsystemy „Tabor” oraz „Sterowanie – urządzenia pokładowe”) przed rozpoczęciem eksploatacji uzyskał zezwolenie na przekazanie do eksploatacji wydane przez Prezesa UTK.

Przywołane powyżej wymagania wynikają z przepisów prawa. Certyfikaty i deklaracje zgodności WE oraz świadectwa typu i deklaracje zgodności z typem a także 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 ponieważ wymaganie zasadnicze ‘bezpieczeństwo’ nie ma zastosowania do części rozwiązań wspierających ochronę (wymagań ogólnych w zakresie ochrony 1.1.12. i 1.1.13.) oraz do rozwiązań wspierających cyberbezpieczeństwo. W szczególności pomijają zespoły i podzespoły nie będące składnikami interoperacyjności a zawierające oprogramowanie układowe (firmware) i połączone z siecią pokładową WTB i/lub TCN.

4. Szczegółowe wymagania w zakresie dokumentowania i weryfikowania spójności bezpieczeństwa, ochrony i cyberbezpieczeństwa dla nowego pasażerskiego taboru kolejowego

Zasady dokumentowania i weryfikowania spójności bezpieczeństwa, ochrony i cyberbezpieczeństwa zdefiniowane w rozdziale 4 niniejszego dokumentu łącznie stanowią przyjętą metodę weryfikowania funkcjonalnej kompletności i adekwatności bezpieczeństwa, ochrony oraz cyberbezpieczeństwa taboru pasażerskiego.

Rozdział 4.1. definiuje zasady dokumentowania spójności bezpieczeństwa, ochrony i cyberbezpieczeństwa przez producentów taboru kolejowego opracowujących koncepcje/projekty nowego typu taboru a następnie produkujących pasażerski tabor kolejowy oraz przez podmioty wprowadzające zmiany techniczne mające wpływ na bezpieczeństwo, ochronę lub cyberbezpieczeństwo eksploatowanego taboru.

Rozdział 4.2. definiuje zasady weryfikowania spójności bezpieczeństwa, ochrony i cyberbezpieczeństwa przez **kompetentną niezależną jednostkę inspekcyjną**.

4.1. Dowody spójności bezpieczeństwa, ochrony i cyberbezpieczeństwa

4.1.1. Wymagania ogólne dla dowodów spójności bezpieczeństwa, ochrony i cyberbezpieczeństwa w taborze kolejowym

Dla koncepcji, projektów oraz zamówień nowego taboru kolejowego, wymaga się opracowania przez **wykonawcę** *„dowodu spójności bezpieczeństwa, ochrony i cyberbezpieczeństwa w taborze”* 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 [9÷13] jako właściwe dla poziomów nienaruszalności bezpieczeństwa przypisanych poszczególnym rozwiązaniom technicznym zgodnie z zasadami wskazanymi w tych normach i przepisach;
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 taboru, udokumentowaną zgodnie z wymaganiami zawartymi w rozdziale 4.1.2, oraz analizę zabezpieczeń technicznych związanych z zapewnieniem odpowiedniego poziomu bezpieczeństwa osób i mienia, udokumentowaną zgodnie z wymaganiami zawartymi w rozdziale 4.1.3.;
d) uwzględniał zarówno dla zabezpieczeń technicznych związanych z zapewnieniem bezpieczeństwa ruchu pojazdów jak i zabezpieczeń technicznych związanych z zapewnieniem ochrony taboru przed cyberberzagrożeniami i dokumentował je zgodnie z wymaganiami zawartymi w rozdziale 4.1.4.;
e) określał poziom spójności bezpieczeństwa, ochrony i cyberbezpieczeństwa zgodnie z wymaganiami zawartymi w rozdziale 4.1.5.;
f) określał indeks cyfrowego bezpieczeństwa dla pasażerskiego taboru kolejowego zgodnie z wymaganiami zawartymi w rozdziale 4.1.6.4.

Konstruktorzy, zamawiający i wykonawcy nowych projektów taboru kolejowego, powinni wraz z projektem, przedłożyć **dowód spójności bezpieczeństwa, ochrony i cyberbezpieczeństwa**,

zgodny z proponowaną koncepcją, chyba że zapisy umowy, ze względu na charakter koncepcji, wprost przesądzają, że opracowanie *„dowodu spójności bezpieczeństwa, ochrony i cyberbezpieczeństwa w taborze”* nie jest wymagane.

Dowód spójności bezpieczeństwa, ochrony i cyberbezpieczeństwa dla koncepcji/projektu lub realizacji lub zmiany nowego taboru, powinien obejmować pięć następujących rozdziałów:

1. Rozdział 1 - Wstęp wraz z określeniem systemu podlegającego ocenie
2. Rozdział 2 - Analiza zabezpieczeń technicznych związanych z zapewnieniem bezpieczeństwa taboru (patrz podrozdział 4.1.2.)
3. Rozdział 3 - Analiza zabezpieczeń technicznych związanych z zapewnieniem ochrony pasażerów (patrz podrozdział 4.1.3.)
4. Rozdział 4 - Analiza zabezpieczeń przed cyberzagrożeniami (patrz podrozdział 4.1.4.)
5. Rozdział 5 - Określenie poziomu bezpieczeństwa, ochrony i cyberbezpieczeństwa i poziomu ich spójności (patrz podrozdziały 4.1.5. i 4.1.6.)
6. Rozdział 6 - Podsumowanie dowodu spójności bezpieczeństwa, ochrony i cyberbezpieczeństwa (patrz podrozdział 4.1.7.)

Należy zdefiniować system podlegający ocenie, czyli nowy pojazd kolejowy, którego dotyczy **dowód spójności bezpieczeństwa, ochrony i cyberbezpieczeństwa** oraz zdefiniować funkcje, granice i interfejsy zewnętrzne analizowanego systemu. Granice i interfejsy systemu należy uwzględnić przy opracowywaniu kolejnych rozdziałów.

Dla każdego **dowodu spójności bezpieczeństwa, ochrony i cyberbezpieczeństwa** - dla dowodu dla określonego typu pasażerskiego taboru kolejowego producent lub przewoźnik jako przyszły użytkownik taboru powinien uzyskać pozytywną niezależną ocenę od **kompetentnej niezależnej jednostki inspekcyjnej** (patrz rozdział 4.2. niniejszego dokumentu).

4.1.2. Analiza zabezpieczeń technicznych związanych z zapewnieniem bezpieczeństwa ruchu (Safety)

Analiza zabezpieczeń technicznych związanych wpływem taboru na bezpieczeństwo ruchu kolejowego (Rozdział 2 *„dowodu spójności bezpieczeństwa, ochrony i cyberbezpieczeństwa w taborze”*) powinna opierać się na **referencyjnym modelu funkcjonalnym** (dalej **RMF**) przedstawionym w części safety na Rysunku 1.

W modelu RMF wyróżnionych zostało osiem funkcjonalności pokładowych wpływających na bezpieczeństwo ruchu kolejowego realizowanego z wykorzystaniem danego typu taboru. Jednocześnie referencyjną charakterystykę zdefiniowano dla ośmiu komplementarnych funkcjonalności realizowanych po stronie infrastruktury przez klasyczne systemy sterowania ruchem kolejowym oraz przytorowe systemy i urządzenia bezpiecznej kontroli jazdy BKJP. 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. Przywołują one zasady FS oraz SIL-4, a także funkcjonalności systemów sterowania i bezpiecznej kontroli jazdy kluczowe z punktu widzenia cyberbezpieczeństwa taboru.

Funkcjonalności te połączono w pięć następujących grup:

RMF-G01 – SRK – klasyczne sterowanie ruchem kolejowym (RMF-1.1 ÷ RMF-1.4),
RMF-G02 – BKJP urządzenia przytorowe (RMF-2.1 ÷ RMF-2.4),
RMF-G03 – BKJP urządzenia pokładowe (RMF-3.1 ÷ RMF-3.4),
RMF-G04 – DMI, łączność głosowa, wywołania alarmowe (RMF-4.1 ÷ RMF-4.2),
RMF-G05 – Funkcje GoA3/GoA4 - ATO, ATS (RMF-5.1 ÷ RMF-5.2).

Między innymi następujące kwestie zostały odwzorowane w pytaniach w kartach kontrolnych:

01 – odseparowanie pokładowej wymiany danych istotnych dla bezpieczeństwa od innych pokładowych sieci i systemów,
02 – fizyczne zabezpieczenie miejsc, gdzie zlokalizowane są punkty dostępu do systemu (zabezpieczenie najniższej – fizycznej warstwy dostępu),
03 – cyfrowe zabezpieczenie sieci LAN - odseparowanie systemów sterowania pojazdem od systemów komfortu (system informacji pasażerów, monitoring, sprzedaż biletów, ładowania telefonów, etc.),
04 – autoryzacja dla pracowników (serwis) mających dostęp do wrażliwych danych,
05 - prowadzenie dziennika logowania serwisu do systemu,
06 – zabezpieczenie sieci WiFi dostępnych w pojeździe, przed ingerencją z zewnątrz (zabezpieczenia typu WPA, dostęp jednokierunkowy),
07 – zabezpieczenie przed nieuprawnioną ingerencją w działanie układów napędowego oraz hamulcowego,
08 – zabezpieczenie przed nieuprawnionym generowaniem sygnałów dźwiękowych i wizualnych w kabinie maszynisty oraz informowanie maszynisty poprzez sygnalizację kabinową,
09 – zapewnienie głosowego połączenia radiowego, pomiędzy służbą ruchu i personelem pokładowym, w szczególności pomiędzy dyżurnym ruchu i maszynistą, oraz możliwości bezpiecznego generowania wywołań alarmowych,
10 – zapewnienie głosowego (analogowego połączenia fonicznego), pomiędzy maszynistą i personelem pokładowym, oraz pomiędzy maszynistą i pasażerem używającym HBP (Hamulec Bezpieczeństwa Pasażera), oraz możliwości bezpiecznego generowania wywołań alarmowych w pojeździe (informacje głosowe i wyświetlane na monitorach),
11 – bezpieczne automatyczne sterowanie pozostałymi systemami pokładowymi

Rozdział 2 *„dowodu spójności bezpieczeństwa, ochrony i cyberbezpieczeństwa w taborze”* dedykowany analizie zabezpieczeń technicznych związanych z zapewnieniem bezpieczeństwa ruchu kolejowego tj. właściwej konstrukcji taboru w odniesieniu do obszaru „safety” powinien być podzielony na osiem podrozdziałów dedykowanych funkcjonalnościom 3.1 ÷ 3.4 oraz 4.1 ÷ 4.2 oraz 5.1 ÷ 5.2, tak aby pola modelu RMF mogły zostać wykorzystane do przedstawienia poziomu zabezpieczenia np. przy wykorzystaniu odcieni szarości lub kolorów.

4.1.3. Analiza zabezpieczeń technicznych związanych z zapewnieniem ochrony w taborze (Security)

Analiza zabezpieczeń technicznych związanych z zapewnieniem bezpieczeństwa transportu czyli właściwej ochrony transportu (Rozdział 3 *„dowodu spójności bezpieczeństwa, ochrony i cyberbezpieczeństwa w taborze”*) powinna opierać się na **referencyjnym modelu funkcjonalnym RMF** przedstawionym w części security na Rysunku 2.

W modelu RMF wyróżnionych zostało dwadzieścia funkcjonalności pokładowych wpływających na bezpieczeństwo życia, zdrowia i mienia. Uwzględniają one zarówno wsparcie udzielania pomocy 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.

Funkcjonalności te połączono w cztery następujące grupy:

RMF-G06 – Przestrzeń i bezpieczeństwo pasażerów (RMF-6.1 ÷ RMF-6.6),
RMF-G07 – Przemieszczanie pojazdu (RMF-7.1 ÷ RMF-7.4),
RMF-G08 – Sterowanie pojazdem (RMF-8.1 ÷ RMF-8.4),
RMF-G09 – Systemy awaryjne i „rozrywka” (RMF-9.1 ÷ RMF-9.6).

Między innymi następujące kwestie zostały odwzorowane w pytaniach w kartach kontrolnych:

01 – zapewnienie informacji pasażerskiej w taborze,

02 – zapewnienie ochrony przeciwpożarowej w taborze,
03 – zapewnienie ochrony przed uruchomieniem awaryjnym drzwi,
04 – zapewnienie interwencyjnego sprzętu medycznego oraz urządzeń i systemów wspierających dostępność transportu kolejowego dla osób o ograniczonej sprawności ruchowej oraz osób na wózkach inwalidzkich,
05 – zapewnienie możliwości wzywania pomocy poprzez udostępnianie instalacji alarmowych i/lub wdrożenia hamowania przez pasażera (HBP),
06 – monitorowanie obszarów stacji i wnętrz pojazdów systemami wizyjnymi zainstalowanymi w taborze,
07 – ochrona pomieszczeń zamkniętych przed osobami nieupoważnionymi, w tym w szczególności dostępu do miejsc pracy osób odpowiedzialnych za bezpieczeństwo i prowadzenie pojazdu.

Rozdział 3 *„dowodu spójności bezpieczeństwa, ochrony i cyberbezpieczeństwa w taborze”* dedykowany analizie zabezpieczeń technicznych związanych z zapewnieniem ochrony transportu tj. właściwej konstrukcji taboru w odniesieniu do obszaru „security” powinien być podzielony na dwadzieścia podrozdziałów dedykowanych funkcjonalnościom 6.1 ÷ 6.6 oraz 7.1 ÷ 7.4 oraz 8.1 ÷ 8.4 oraz 9.1 ÷ 9.6, tak aby pola modelu RMF mogły zostać wykorzystane do przedstawienia poziomu zabezpieczenia np. przy wykorzystaniu odcieni szarości lub kolorów.

4.1.4. Analiza zabezpieczeń przed cyberzagrożeniami

Zarówno zabezpieczenia techniczne związane z zapewnieniem bezpieczeństwa taboru jak i zabezpieczenia techniczne związane z zapewnieniem ochrony pasażerów, korzystają z przechowywania, przekazywania i przetwarzania danych realizowanego przez systemy, podsystemy i/lub komponenty cyfrowe, które łącznie dalej określane są jako systemy/podsystemy/komponenty z oprogramowaniem oraz systemy transmisyjne zapewniające wymianę informacji pomiędzy tymi systemami/podsystemami/komponentami.

Rozdział 4 *„dowodu spójności bezpieczeństwa, ochrony i cyberbezpieczeństwa w taborze”* dedykowany analizie zabezpieczeń przed cyberzagrożeniami’ powinien być podzielony na sześć następujących podrozdziałów:

4.1 Opis pokładowej struktury systemów/podsystemów/komponentów z oprogramowaniem
4.2 Przechowywanie i przetwarzanie danych dla zapewnienia bezpieczeństwo ruchu,
4.3. Przechowywanie i przetwarzanie danych dla zapewnienia ochrony transportu,
4.4. Przekazywanie danych związanych z bezpieczeństwem ruchu,
4.5. Przekazywanie danych związanych z ochroną transportu,
4.6. Powiązanie systemów bezpieczeństwa ruchu i systemów ochrony transportu z mechanizmami podnoszenia bezpieczeństwa sieci i systemów informatycznych.

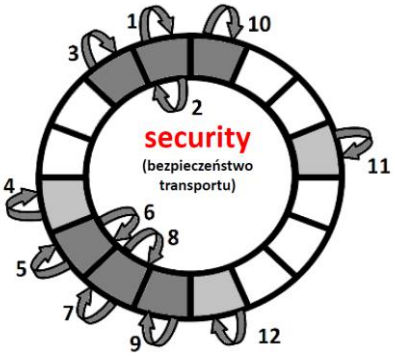
Podrozdział 4.1 powinien zawierać i omawiać schemat pokazujący wszystkie pokładowe systemy/ podsystemy/komponenty z oprogramowaniem oraz systemy transmisyjne do wymiany danych pomiędzy nimi oraz powiązania z bezprzewodowymi systemami transmisyjnymi, przeznaczonymi do wymiany danych z systemami przytorowymi/infrastrukturalnymi/naziemnymi. Właściwa identyfikacja systemów/podsystemów/komponentów z oprogramowaniem oraz systemów transmisyjnych są kluczowe dla właściwego zastosowania kart kontrolnych związanych z cyberbezpieczeństwem.

Podrozdziały dedykowane przechowywaniu i przetwarzaniu danych, podrozdziały 4.2. i 4.3., powinny obejmować precyzyjne odwołania do opisów rozwiązań technicznych. W przypadku zabezpieczeń technicznych związanych z zapewnieniem bezpieczeństwa ruchu (podrozdział 4.2.) 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 4.3.) 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 pasażerów, podrozdziały 4.4. i 4.5. '**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 4.4. powinien odwoływać się do dokumentów potwierdzających właściwe zastosowanie normy PN EN 50159 [13], lub wprost obejmować stosowne dowody.

Systemy transmisji opisane w podrozdziałach 4.4. oraz 4.5. '**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 5.



Rysunek 5. Przykład zobrazowania systemów transmisji
z wykorzystaniem referencyjnego modelu funkcjonalnego
dla zabezpieczeń technicznych związanych z ochroną transportu
(źródło: opracowanie własne)

Podrozdział 4.6. '**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 przewoźnika kolejowego zgodnie z normą PN-EN ISO/IEC 27001 [8].[3]

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.

4.1.5. 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

[3] Dyrektywa UE 2022/2555 (NIS2) zobowiązuje między innymi przewoźników kolejowych do wdrożenia Systemów Zarządzania Bezpieczeństwem Informacji (SZBI), dla których wymagania zdefiniowano w normie PN-EN ISO/IEC 27001.

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 czternastu kartach kontrolnych – dwóch referencyjnych, trzech dotyczących bezpieczeństwa, czterech ochrony i pięciu cyberbezpieczeństwa to jest dwóch referencyjnych i dwunastu służących do oceny bezpieczeństwa, ochrony i cyberbezpieczeństwa danego typu taboru kolejowego oraz ich spójności funkcjonalnej.

UWAGA: Karty kontrolne nie służą do weryfikowania wszystkich wymagań stawianych nowemu taborowi kolejowemu. Zgodnie z zapisami w rozdziale 1.2. oraz zgodnie z obowiązującymi przepisami prawa wymagania zasadnicze w całości potwierdzane są na poziomie podsystemów „Tabor" oraz „Sterowanie – urządzenia pokładowe" 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 wyposażenie taboru kolejowego. Jednocześnie zaznaczyć należy, że ocena spójności bezpieczeństwa, ochrony i cyberbezpieczeństwa nowego taboru pasażerskiego, która zgodnie z zapisami niniejszego dokumentu ma być realizowana z uwzględnieniem wymagań rozporządzenia w sprawie oceny i wyceny ryzyka [6, 7], nie wyczerpuje zakresu stosowania oceny i wyceny ryzyka dla nowego taboru pasażerskiego, bo ta zgodnie z obowiązującym prawem powinna być stosowana do wszelkich zmian technicznych, eksploatacyjnych i organizacyjnych wpływających na bezpieczeństwo.

4.1.5.1. Referencyjne karty kontrolne infrastrukturalne

Niniejsze karty kontrolne posiadają przypisane wartości odpowiedzi, które reprezentują referencyjną infrastrukturę w zakresie jej wyposażenia w urządzenia i systemy zapewniające bezpieczeństwo ruchu kolejowego. Przypisane referencyjne wartości „1" gwarantują, że producenci/dostawcy taboru kolejowego nie odpowiadają za stan i wyposażenie infrastruktury na której eksploatowany będzie pasażerski tabor kolejowy.

Referencyjna karta kontrolna bezpieczeństwa RMF-G01 funkcjonalności przytorowych systemów sterowania od kontroli niezajętości do wyświetlania obrazów sygnałowych na sygnalizatorach świetlnych (RMF-1.1 ÷ RMF-1.4)
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 i/lub blokady i/lub systemu sterowania rozrządem).

Pytania kontrolne	Wartości ref.
RMF-1.1	
1. Czy wszystkie tory na całej długości objęte są kontrolą niezajętości? TAK = 1, NIE = 0	Ad. 1 ➔ 1
2. Czy wszystkie zastosowane rozwiązania techniczne stosują zasadę FS? (Czy możliwe uszkodzenia modułów prowadzą do zgłaszania zajętości?) TAK = 1, NIE = 0	Ad. 2 ➔ 1
3. Czy wszystkie zastosowane rozwiązania techniczne stosują zasadę SIL-4? (Czy dostępne są wiarygodne dowody bezpieczeństwa dla aplikacji potwierdzające SIL-4, zweryfikowane przez niezależnego audytora?) TAK = 1, NIE = 0, NIE, ale system jest w pełni analogowy = 1	Ad. 3 ➔ 1 Iloczyn odpowiedzi ➔ 1
RMF-1.2	
1. Czy wszystkie zastosowane rozwiązania techniczne stosują zasadę FS? (Czy możliwe uszkodzenia modułów prowadzą do stanów bezpiecznych?) TAK = 1, NIE = 0	Ad. 1 ➔ 1
RMF-1.3	
1. Czy wszystkie zastosowane rozwiązania techniczne stosują zasadę SIL-4? (Czy dostępne są wiarygodne dowody bezpieczeństwa dla aplikacji potwierdzające SIL-4, zweryfikowane przez niezależnego audytora?) TAK = 1, NIE = 0	Ad. 1. ➔ 1
RMF-1.4	
1. Czy wszystkie odstępy (ew. grupy odstępów) są osłonięte sygnalizatorami? TAK = 1, NIE = 0, NIE, ale zastosowano system BKJP = 1	Ad. 1 ➔ 1
2. Czy wszystkie zastosowane rozwiązania techniczne stosują zasadę FS? (Czy możliwe uszkodzenia modułów prowadzą do stanów bezpiecznych?) TAK = 1, NIE = 0	Ad. 2. ➔ 1
3. Czy wszystkie zastosowane rozwiązania techniczne stosują zasadę SIL-4? (Czy dostępne są wiarygodne dowody bezpieczeństwa dla aplikacji potwierdzające SIL-4, zweryfikowane przez niezależnego audytora?) TAK = 1, NIE = 0, NIE, ale system jest w pełni analogowy = 1	Ad. 3. ➔ 1 Iloczyn odpowiedzi: ➔ 1
Zbiorcza wartość referencyjna dla grupy RMF-G01 iloczyn wartości referencyjnych RMF-1.1 ÷ RMF-1.4	**1**

UWAGA: w przypadku pojazdów przeznaczonych do jazdy pod nadzorem systemu bezpiecznej kontroli jazdy w trybie opartym na zasadzie ruchomego odstępu blokowego nie wymaga się, aby tory na których realizowane są/będą jazdy w takim trybie były objęte kontrolą niezajętości w postaci obwodów torowych i/lub liczników osi. W takim przypadku kontrola niezajętości odbywa się w ramach systemu zarządzania następstwem pociągów wykorzystującego dane o położeniu i ewentualnie prędkości poszczególnych pociągów. W istniejących systemach funkcja taka realizowana jest po stronie infrastrukturalnej.

--- --- ---

Referencyjna karta kontrolna bezpieczeństwa RMF-G02 funkcjonalności przytorowych urządzeń systemów bezpiecznej kontroli jazdy pociągu od obrazów sygnałowych do wysyłania elektronicznych zezwoleń ZnJ (RMF-2.1 ÷ RMF-2.4)
Założenia: 1. Bezpieczna kontrola jazdy pociągu wykorzystuje system klasy ATP lub ATC.

Pytania kontrolne	Wartości ref.
RMF-2.1	
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	Ad. 1 ➔ 1
2. Czy wszystkie zastosowane rozwiązania techniczne stosują zasadę FS? (Czy możliwe uszkodzenia modułów prowadzą do stanów bezpiecznych?) TAK = 1, NIE = 0	Ad. 2 ➔ 1
3. Czy wszystkie zastosowane rozwiązania techniczne stosują zasadę SIL-4? (Czy dostępne są wiarygodne dowody bezpieczeństwa dla aplikacji potwierdzające SIL-4, zweryfikowane przez niezależnego audytora?) TAK = 1, NIE = 0, NIE, ale system jest w pełni analogowy = 1	Ad. 3 ➔ 1 Iloczyn odpowiedzi ➔ 1
RMF-2.2	
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	Ad. 1 ➔ 1
RMF-2.3	
1. Czy wszystkie systemy przetwarzania danych źródłowych definiujące ZnJ w pełnym zakresie stosują zasadę SIL-4? (Czy dostępne są wiarygodne dowody bezpieczeństwa dla aplikacji potwierdzające SIL-4, zweryfikowane przez niezależnego audytora?) TAK = 1, NIE = 0	Ad. 1 ➔ 1
RMF-2.4	
1. Czy wysyłane ZnJ zawierają dane pozwalające na identyfikację nadawcy i identyfikację odbiorcy – czy system transmisji jest systemem zamkniętym? TAK = 1, NIE = 0	Ad. 1 ➔ 1
2. Czy wysyłane ZnJ zawierają dane pozwalające na weryfikację ważności (np. czas żądania i czas nadania lub stempel czasu wspólnego)? TAK = 1, NIE = 0	Ad. 2 ➔ 1
3. Czy wysyłane ZnJ zawierają dane pozwalające na weryfikację kompletności oraz spójności danych (np. sumy kontrolne, kody hamminga)? TAK = 1, NIE = 0	Ad. 3 ➔ 1 Iloczyn odpowiedzi ➔ 1
Zbiorcza wartość referencyjna dla grupy RMF-G02 iloczyn wartości referencyjnych RMF-2.1 ÷ RMF-2.4	**1**

UWAGA: Określenie ZnJ oznacza elektroniczne Zezwolenie na Jazdę czyli cyfrową informację przekazywaną poprzez bezprzewodową transmisję z toru do pojazdu w oparciu o którą po pierwsze wyświetlane są dane na pulpicie maszynisty przedstawiające ograniczenia jazdy a po drugie prowadzony jest elektroniczny nadzór nad zgodnością prowadzenia pojazdu z tymi ograniczeniami.

--- --- ---

4.1.5.2. Karty kontrolne dla oceny typu taboru w zakresie pokładowego wyposażenia w systemy zapewniające bezpieczeństwo ruchu kolejowego

Niniejsze karty należy wypełnić dla analizowanego typu taboru poprzez przypisanie odpowiedziom wartości wg wzoru. Zaznacza się, że w ramach dowodu spójności bezpieczeństwa, ochrony i cyberbezpieczeństwa należy uwzględnić informacje pozwalające na zweryfikowanie odpowiedzi. Stosowne dane mogą być zawarte w pełnym zakresie w dowodzie lub częściowo opierać się na przywoływanych dokumentach, które wówczas muszą być udostępnione jednostce oceniającej dowód.

Karta kontrolna bezpieczeństwa RMF-G03 funkcjonalności pokładowych urządzeń systemów bezpiecznej kontroli jazdy pociągu od odebrania zezwolenia ZnJ do interwencyjnego wdrażania hamowania (RMF-3.1 ÷ RMF-3.4)
Założenia: 1. Bezpieczna kontrola jazdy pociągu wykorzystuje system klasy ATP lub ATC.

Pytania kontrolne	Wartości ref.
RMF-3.1 1. Czy wszystkie człony trakcyjne pasażerskiego taboru trakcyjnego danego typu są wyposażone w system automatycznego sterowania pociągiem ATC? TAK = 1, NIE = 0 2. Czy pokładowe instalacje ATC stosują zasadę FS? (Czy możliwe uszkodzenia modułów prowadzą do stanów bezpiecznych?) TAK = 1, NIE = 0 3. Czy pokładowe instalacje ATC stosują zasadę SIL-4? (Czy dostępne są wiarygodne dowody bezpieczeństwa dla aplikacji potwierdzające SIL-4, zweryfikowane przez niezależnego audytora?) TAK = 1, NIE = 0 4. Czy odbierane ZnJ podlegają uwierzytelnieniu poprzez sprawdzenie identyfikatorów nadawcy/odbiorcy oraz weryfikację ważności ZnJ (np. czas żądania/czas nadania lub stempel czasu wspólnego)? TAK = 1, NIE = 0 5. Czy odbierane ZnJ zawierają dane pozwalające na weryfikację kompletności oraz spójności danych (np. sumy kontrolne, kody hamminga) i podlegają weryfikacji kompletności oraz spójności? TAK = 1, NIE = 0 6. Czy system transmisji ZnJ jest systemem zamkniętym zgodnie z definicją zawartą w normie PN-EN 50159:2011 względnie otwartym, ale zabezpieczonym zgodnie z wymaganiami tej normy? TAK = 1, NIE = 0 UWAGA: Właściwe zabezpieczenie systemu transmisji ZnJ powinno być ujęte i potwierdzone w dowodzie bezpieczeństwa dla pokładowego systemu bezpiecznej kontroli jazdy opracowanym i zaakceptowanym zgodnie z normami RAMS [9÷13] 7. Czy system radiowej transmisji ZnJ jest zgodny z dokumentami narzuconymi prawem w zakresie zabezpieczenia przed zakłóceniami i atakami? TAK = 1, NIE = 0	Iloczyn odpowiedzi: 0 lub 1
RMF-3.2 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-3.3 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 techniczne BKJP stosują zasadę SIL-4? (Czy dostępne są wiarygodne dowody bezpieczeństwa dla aplikacji 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-3.4 1. Czy systemy automatycznego wdrażania hamowania interwencyjnego w pełnym zakresie stosują zasadę SIL-4? (Czy dostępne są wiarygodne dowody bezpieczeństwa dla aplikacji potwierdzające SIL-4, zweryfikowane przez niezależnego audytora?) TAK = 1, NIE = 0 2. Czy automatyczne wdrażanie hamowania interwencyjnego uwzględnia więcej niż jeden tryb hamowania interwencyjnego (hamowanie służbowe i hamowanie nagłe)? TAK = 2, NIE = 1 3. Czy określana jest i sygnalizowana maszyniście lokalizacja, gdzie najpóźniej należy rozpocząć hamowanie dla odpowiedniego zmniejszenia prędkości przed ograniczeniem prędkości? TAK = 2, NIE = 1 4. Czy jest możliwe wykrycie dysfunkcji układu hamulcowego w trakcji ukrotnionej? TAK = 1, NIE = 0	Iloczyn odpowiedzi: 0 lub 1 lub 2 lub 4
Zbiorcza wartość referencyjna dla grupy RMF-G03 iloczyn wartości referencyjnych RMF-3.1 ÷ RMF-3.4	0 lub 1 lub 2 lub 4

--- --- ---

Karta kontrolna bezpieczeństwa RMF-G04 funkcjonalności wspierające manualne prowadzenie pociągów przez maszynistów w oparciu o obrazy sygnałowe na sygnalizatorach świetlnych przy wykorzystaniu radia (RMF-4.1 ÷ RMF-4.2)
Założenia: 1. Pociągi prowadzone są przez maszynistów. 2. Zapewniona jest łączność eksploatacyjna.

Pytania kontrolne	Wartości ref.
RMF-4.1 1. Czy wszystkie człony trakcyjne pasażerskiego taboru kolejowego danego typu wyposażone są we wszystkie systemy ostrzegawcze (klasy AWS) konieczne do ostrzegania maszynistów o zbliżaniu się do miejsc niebezpiecznych, dostosowane do współpracy z instalacjami przytorowymi stosowanymi na infrastrukturze po której w normalnych warunkach eksploatacyjnych na poruszać się tabor? TAK = 1, NIE = 0 2. Czy wszystkie systemy AWS generujące sygnały ostrzegawcze (dźwiękowe i/lub 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 ATC prezentuje ZnJ na pulpicie w kabinie maszynisty? TAK = 1, NIE = 0 UWAGA: jeśli brak jest systemu BKJP klasy ATC, należy przyjąć wartość „1”.	Iloczyn odpowiedzi: 0 lub 1
RMF-4.2 1. Czy zapewnione jest głosowe połączenie radiowe między maszynistą i dyżurnym ruchu (ew. dyspozytorem)? TAK = 1, NIE = 0 2. Czy zastosowano zabezpieczenia przed możliwością nieuprawnionej cyfrowej ingerencji (włączenia się) w łączność głosową między maszynistą i dyżurnym ruchu (ew. dyspozytorem)? TAK = 1, NIE = 0 UWAGA: Jeśli system łączności między maszynistą i dyżurnym ruchu jest systemem analogowym, należy przyjąć wartość „1” ze względu na brak możliwości przeprowadzenia cyberataku, co nie oznacza, że instalacji systemów łączności nie należy zabezpieczać przed innymi atakami np. fizycznymi. 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-G04 iloczyn wartości referencyjnych RMF-4.1 ÷ RMF-4.2	0 lub 1 lub 2

--- --- ---

Karta kontrolna bezpieczeństwa RMF-GB-05 funkcjonalności automatycznego prowadzenia pociągu zastępujące maszynistę w przyspieszaniu i hamowaniu oraz obsłudze innych urządzeń pokładowych i synchronizacji pracy drzwi pokładowych i peronowych (RMF-5.1 ÷ RMF-5.2)
Założenia: 1. Pociągi prowadzone są przez systemy klasy ATO. 2. Ruch pociągów jest nadzorowany przez systemy klasy ATS.

Pytania kontrolne	Wartości ref.
RMF-5.1 1. Czy wszystkie człony trakcyjne pasażerskiego taboru kolejowego ocenianego typu są wyposażone w systemy klasy ATO? TAK = 1, NIE = 0 2. Czy systemy ATO zapewniają bezpieczne automatyczne ograniczanie prędkości do zera oraz automatycznym ograniczaniem prędkości do wartości ograniczeń przed miejscami ograniczeń prędkości? TAK = 1, NIE = 0 3. Czy systemy ATO zapewniają bezpieczne automatyczne rozpoczynanie jazdy oraz automatyczne zwiększanie prędkości do wartości dopuszczalnej zgodnie z ograniczeniami infrastrukturalnymi? TAK = 1, NIE = 0 4. 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 dla aplikacji potwierdzające SIL-4, zweryfikowane przez niezależnego audytora?) TAK = 1, NIE = 0	Iloczyn odpowiedzi: 0 lub 1
RMF-5.2 1. Czy systemy ATO realizują wszystkie wymagane funkcje GoA3 (Grade of Automation GoA3 – poziomu automatyzacji dla jazdy bez maszynisty) wskazane w normie IEC 62267:2009-07, w tym automatyczne sterowanie pokładowymi urządzeniami pomocniczymi takimi jak np. systemy poboru prądu czy drzwi zewnętrzne? TAK = 1, NIE = 0 UWAGA: Norma definiuje także dodatkowe funkcje dla GoA4 (poziom automatyzacji wymagany dla jazdy bez personelu). Stosowne funkcje mogą być wymagane dla danego typu pasażerskiego taboru kolejowego. 2. Czy pokładowe systemy ATO zapewniają wymianę danych z przytorowym systemem ATS koniecznych dla zapewnienia nadzoru nad autonomiczną jazdą w zakresie właściwym dla poziomu automatyzacji (GoA3 lub GoA4)? TAK = 1, NIE = 0 UWAGA: Jazda autonomiczna odbywa się pod nadzorem systemu klasy ATS, który może być obsługiwany przez dyspozytora lub autonomiczny. System ATS pozostaje poza oceną taboru, ale wymiana danych pomiędzy autonomicznym pojazdem a systeme klasy ATS powinna być uwzględniona w ocenie bezpieczeństwa taboru. **3.** Czy zapewniona jest bezpieczna wymiana danych dla bezpiecznego automatycznego sterowania drzwiami peronowymi w synchronizacji z drzwiami pokładowymi? TAK = 1, NIE = 0	Iloczyn odpowiedzi: 0 lub 1
Zbiorcza wartość referencyjna dla grupy RMF-G5 iloczyn wartości referencyjnych RMF-5.1 ÷ RMF-5.2	0 lub 1

--- --- ---

4.1.5.3. Karty kontrolne dla oceny typu pasażerskiego taboru kolejowego w zakresie bezpieczeństwa transportu (ochrony - security)

Niniejsze karty należy wypełnić dla analizowanego typu taboru poprzez przypisanie odpowiedziom wartości wg wzoru. Zaznacza się, że w ramach dowodu spójności bezpieczeństwa, ochrony i cyberbezpieczeństwa należy uwzględnić informacje pozwalające na zweryfikowanie odpowiedzi. Stosowne dane mogą być zawarte w pełnym zakresie w dowodzie lub częściowo opierać się na przywoływanych dokumentach, które wówczas muszą być udostępnione jednostce oceniającej dowód.

Karta kontrolna ochrony RMF-G06 funkcjonalności dedykowane dla zapewnienia minimum bezpieczeństwa pasażerów (RMF-6.1 ÷ RMF-6.6)
Założenia: Należy zapewnić bezpieczeństwo w obszarach dostępnych dla pasażerów.

Pytania kontrolne	Wartości ref.
RMF-6.1 1. Czy zastosowane jest fizyczne zabezpieczenie przed możliwością ingerencji w sterowniki drzwi zewnętrznych (i stopni wysuwnych, jeśli są stosowane), oraz przed zakłóceniem przetwarzania sygnału postoju, co może skutkować samoczynnym otwarciem drzwi w trakcie jazdy pociągu, lub rozpoczęciem jazdy z otwartymi drzwiami? TAK = 1, NIE = 0 2. Czy drzwi zewnętrzne dla pasażerów w pojeździe objęte są monitoringiem wizyjnym? TAK = 1, NIE = 0 3. Czy zarówno drzwi zewnętrzne jak i drzwi wewnętrzne dla pasażerów objęte są systemem wykrywania obecności pasażera w drzwiach blokującym zamykanie drzwi przy obecności pasażera? TAK = 1, NIE = 0 4. Czy zastosowane jest fizyczne zabezpieczenie przed ingerencją w systemy sterowania drzwiami wewnętrznymi? TAK = 1, NIE = 0	Iloczyn odpowiedzi: 0 lub 1
RMF-6.2 1. Czy wszystkie przestrzenie, w których w normalnych warunkach eksploatacji mogą znajdować się pasażerowie wyposażone są w systemy ogrzewania, wentylacji i klimatyzacji? TAK = 1, NIE = 0 2. Czy zastosowane jest fizyczne zabezpieczenie przed możliwością ingerencji zewnętrznej w system ogrzewania? TAK = 1, NIE = 0 3. Czy zastosowane jest fizyczne zabezpieczenie przed możliwością ingerencji zewnętrznej w system wentylacji? TAK = 1, NIE = 0 4. Czy istnieje zabezpieczenie przed możliwością ingerencji zewnętrznej w system klimatyzacji? TAK = 1, NIE = 0	Iloczyn odpowiedzi: 0 lub 1
RMF-6.3 1. Czy wszystkie przestrzenie w których w normalnych warunkach eksploatacji mogą znajdować się pasażerowie wyposażone są w systemy oświetlenia? TAK = 1, NIE = 0 2. Czy wszystkie przestrzenie w których w normalnych warunkach eksploatacji mogą znajdować się pasażerowie wyposażone są w systemy oświetlenia awaryjnego jeśli pasażerski tabor danego typu przeznaczony jest do jazd w tunelach? TAK = 1, NIE = 0 3. Czy zastosowane jest fizyczne zabezpieczenie przed możliwością ingerencji zewnętrznej w system oświetlenia oraz system oświetlenia awaryjnego (jeśli został zastosowany)? TAK = 1, NIE = 0	Iloczyn odpowiedzi: 0 lub 1
RMF-6.4 1. Czy monitoring wizyjny obejmuje wszystkie obszary dostępne dla pasażerów w normalnych warunkach eksploatacyjnych? TAK = 1, NIE = 0 2. Czy zastosowane jest fizyczne zabezpieczenie przed możliwością ingerencji zewnętrznej w system monitoringu wizyjnego, w tym odłączenia nagrywania obrazu i dźwięku oraz usunięcia nagranego materiału? TAK = 1, NIE = 0 3. Czy system monitoringu wizyjnego wyposażony jest w funkcje analizy strumienia wideo pozwalające na identyfikowanie sytuacji niebezpiecznych i automatyczne informowanie personelu pokładowego np. kierownika pociągu i/lub służb ochrony? TAK = 2, NIE = 1	Iloczyn odpowiedzi: 0 lub 1 lub 2

RMF-6.5 1. Czy zastosowane jest fizyczne zabezpieczenie przed ingerencją w systemy sterowania drzwiami do toalet? TAK = 1, NIE = 0 2. Czy zastosowane jest fizyczne zabezpieczenie przed możliwością ingerencji w system alarmowy w toaletach w pojeździe? TAK = 1, NIE = 0	Iloczyn odpowiedzi: 0 lub 1
RMF-6.6 1. Czy w obszarach dostępnych dla pasażerów w pojeździe zapewniona jest wizualna informacja pasażerska? TAK = 1, NIE = 0 2. Czy w obszarach dostępnych dla pasażerów w pojeździe zapewniona jest głosowa informacja pasażerska? TAK = 1, NIE = 0 3. Czy istnieje fizyczne zabezpieczenie przed ingerencją w systemy informacji pasażerskiej w obszarach dostępnych w pojeździe dla pasażerów? TAK = 1, NIE = 0 4. Czy udostępniono urządzenia wspierające bezpieczeństwo pasażerów w typach, ilościach i miejscach właściwych dla przeznaczenia pojazdu? TAK = 1, NIE = 0 UWAGA: Należy uwzględnić co najmniej: systemy awaryjnego otwierania drzwi, systemy awaryjnego powiadamiana maszynisty/personelu pokładowego (wzywania pomocy) oraz systemy hamulca bezpieczeństwa pasażera. 5. Czy istnieje fizyczne zabezpieczenie przed ingerencją w systemy, o których mowa w punkcie 4. powyżej, zabezpieczająca przed wyłączeniem tych systemów oraz odłączeniem łączności z właściwym personelem? TAK = 1, NIE = 0	Iloczyn odpowiedzi: 0 lub 1
Zbiorcza wartość referencyjna dla grupy RMF-G06 iloczyn wartości referencyjnych RMF-6.1 ÷ RMF-6.6	0 lub 1 lub 2

--- --- ---

Karta kontrolna ochrony RMF-G07 przemieszczanie pojazdu (RMF-7.1 ÷ RMF-7.4)
Założenia: Należy zapewnić bezpieczeństwo przemieszczania pojazdu.

Pytania kontrolne	Wartości ref.
RMF-7.1 1. Czy zapewnione jest bezpieczne automatyczne sterowanie pokładowymi urządzeniami do poboru prądu (pantografami)? TAK = 1, NIE = 0 2. Czy zastosowane jest fizyczne zabezpieczenie przed możliwością ingerencji w sterownik pantografu, podczas postoju i jazdy, TAK = 1, NIE = 0 3. Czy zastosowane jest fizyczne zabezpieczenie przed możliwością ingerencji w wyłącznik główny, podczas postoju i jazdy, TAK = 1, NIE = 0 UWAGA: w przypadku pojazdów z silnikami spalinowymi, bateryjnych oraz wodorowych a także hybrydowych istnieje konieczność przeformułowania pytań 1.÷3, które podano powyżej. 4. Czy w obszarach dostępnych dla pasażerów w pojeździe zapewniona jest ochrona przeciwporażeniowa? TAK = 1, NIE = 0	Iloczyn odpowiedzi: 0 lub 1
RMF-7.2 1. Czy zapewnione jest bezpieczne automatyczne sterowanie pokładowymi urządzeniami przetwarzania energii takimi jak np.: falowniki, silniki, przekształtniki, ogniwa wodorowe, baterie akumulatorowe, …)? TAK = 1, NIE = 0 2. Czy istnieje fizyczne zabezpieczenie przed wyłączeniem zasilania pociągu przez osoby nieuprawnione? TAK = 1, NIE = 0 UWAGA: z wyłączeniem ingerencji po stronie infrastrukturalnej.	Iloczyn odpowiedzi: 0 lub 1

RMF-7.3 1. Czy zastosowane jest fizyczne zabezpieczenie przed ingerencją osób nieuprawnionych w system sterowania układem napędowym z zewnątrz pojazdu? TAK = 1, NIE = 0 2. Czy zastosowane jest fizyczne zabezpieczenie przed ingerencją osób nieuprawnionych w system sterowania układem napędowym z wewnątrz pojazdu? TAK = 1, NIE = 0	Iloczyn odpowiedzi: 0 lub 1
RMF-7.4 1. Czy zastosowane jest fizyczne zabezpieczenie przed ingerencją osób nieuprawnionych w system sterowania układem hamulcowym? TAK = 1, NIE = 0 2. Czy zastosowane jest fizyczne zabezpieczenie przed ingerencją osób nieuprawnionych w systemy antypoślizgowe, w tym dozujące piasek pod koła pojazdu? TAK = 1, NIE = 0	Iloczyn odpowiedzi: 0 lub 1
Zbiorcza wartość referencyjna dla grupy RMF-G07 iloczyn wartości referencyjnych RMF-7.1 ÷ RMF-7.4	0 lub 1

--- --- ---

Karta kontrolna ochrony RMF-G08 funkcjonalności dedykowane dla sterowania pojazdem (RMF-8.1 ÷ RMF-8.4)
Założenia: Należy zapewnić bezpieczeństwo sterowania pojazdem.

Pytania kontrolne	Wartości ref.
RMF-8.1 1. Czy zastosowane jest fizyczne zabezpieczenie kabiny maszynisty oraz innych pomieszczeń/przestrzeni zamkniętych przed dostępem osób nieupoważnionych? TAK = 1, NIE = 0 2. Czy zastosowane zabezpieczenie zapewniające ochronę, o której mowa powyżej, jest zabezpieczone przed możliwością ingerencji przez osoby nieupoważnione? TAK = 1, NIE = 0	Iloczyn odpowiedzi: 0 lub 1
RMF-8.2 1. Czy istnieje fizyczne zabezpieczenie przed dostępem osób nieupoważnionych do kabli i sieciowych urządzeń aktywnych wykorzystywanych do sterowania przez maszynistę systemami/podsystemami/komponentami z oprogramowaniem, które sterują np. drzwiami, ogrzewaniem, wentylacją, klimatyzacją, informacją pasażerską (głosową i wyświetlaną na monitorach)? TAK = 1, NIE = 0 2. Czy istnieje fizyczne zabezpieczenie przed dostępem osób nieupoważnionych do kabli i sieciowych urządzeń aktywnych wykorzystywanych przez system monitoringu wizyjnego? TAK = 1, NIE = 0 3. Czy istnieje fizyczne zabezpieczenie przed dostępem osób nieupoważnionych do kabli i sieciowych urządzeń aktywnych wykorzystywanych przez systemy hamowania? TAK = 1, NIE = 0 4. Czy połączenia (kable, urządzenia aktywne, złącza) wykorzystywane przez systemy hamowania są fizycznie odseparowane od pokładowych sieci wykorzystywanych dla wszelkich innych celów? TAK = 1, NIE = 0 5. Czy połączenia (kable, urządzenia aktywne, złącza) wykorzystywane do sterowania podnoszeniem prędkości pojazdu oraz obsługi drzwi zewnętrznych (w tym stopni wysuwnych jeśli są zastosowane) są fizycznie odseparowane od pokładowych sieci wykorzystywanych dla wszelkich innych celów? TAK = 2, NIE = 1	Iloczyn odpowiedzi: 0 lub 1 lub 2

RMF-8.3 1. Czy tabor wyposażony jest w systemy diagnostyczne? TAK = 1, NIE = 0 2. Czy zastosowane jest fizyczne zabezpieczenie przed dostępem osób nieupoważnionych do systemów/urządzeń/czujników diagnostycznych? TAK = 1, NIE = 0 3. Czy zastosowane jest fizyczne zabezpieczenie przed dostępem osób nieupoważnionych do kabli i sieciowych urządzeń aktywnych wykorzystywanych przez systemy/ urządzenia/czujniki diagnostyczne monitorujące bieżącą pracę taboru? TAK = 1, NIE = 0	Iloczyn odpowiedzi: 0 lub 1
RMF-8.4 1. Czy istnieje fizyczne zabezpieczenie przed dostępem osób nieupoważnionych do urządzeń współtworzących pokładowy system pomiaru energii pobieranej z sieci i oddanej do sieci trakcyjnej oraz połączeń pomiędzy tymi urządzeniami? TAK = 1, NIE = 0 UWAGA: Jeśli pasażerski tabor kolejowy danego typu nie jest wyposażony w pokładowy system pomiaru energii pobranej z sieci i oddanej do sieci trakcyjnej należy przypisać wartość „1”. 2. Czy istnieje fizyczne zabezpieczenie przed dostępem osób nieupoważnionych, po stronie taboru, do urządzeń łączności bezprzewodowej wykorzystywanych przez pokładowy system pomiaru energii pobieranej z sieci i oddanej do sieci trakcyjnej. TAK = 1, NIE = 0	Iloczyn odpowiedzi: 0 lub 1
Zbiorcza wartość referencyjna dla grupy RMF-G08 iloczyn wartości referencyjnych RMF-8.1 ÷ RMF-8.4	0 lub 1 lub 2

--- --- ---

Karta kontrolna ochrony RMF-G09 funkcjonalności dedykowane dla systemów umożliwiających podejmowanie działań w sytuacjach awaryjnych oraz oferowania „rozrywki” (RMF-9.1 ÷ RMF-9.6)
Założenia: 1. Należy zapewnić bezpieczeństwo w sytuacjach zagrożeń ruchowych i w nagłych wypadkach. 2. Należy zapewnić brak zagrożeń ze strony systemów poprawiających komfort podróży.

Pytania kontrolne	Wartości ref.
RMF-9.1 1. Czy istnieje fizyczne zabezpieczenie przed możliwością nieuprawnionej ingerencji w systemy alarmowe? TAK = 1, NIE = 0 2. Czy działa system awaryjnego otwierania drzwi? TAK = 1, NIE = 0 3. Czy istnieje zabezpieczenie przed możliwością nieuprawnionego awaryjnego otwarcia drzwi? TAK = 1, NIE = 0 4. Czy działa system hamowania awaryjnego (hamulec bezpieczeństwa)? TAK = 1, NIE = 0 5. Czy istnieje zabezpieczenie przed możliwością nieuprawnionej ingerencji zewnętrznej w system hamowania awaryjnego? TAK = 1, NIE = 0 6. Czy działa system łączności wewnętrznej (intercom)? TAK = 1, NIE = 0 7. Czy istnieje zabezpieczenie przed możliwością nieuprawnionej ingerencji zewnętrznej w system łączności wewnętrznej (intercom)? TAK = 1, NIE = 0 8. Czy pojazd wyposażony jest w urządzenia AED oraz system nadzoru nad ich udostępnianiem z łącznością z kabiną maszynisty lub personelem pokładowym? TAK = 2 NIE = 1	Iloczyn odpowiedzi: 0 lub 1 lub 2
RMF-9.2 1. Czy pojazd wyposażony jest w system wykrywania pożaru? TAK = 1, NIE = 0 2. Czy pojazd wyposażony jest w system gaszenia pożaru? TAK = 1, NIE = 0	Iloczyn odpowiedzi: 0 lub 1

RMF-9.3 1. Czy zastosowany jest system wykrywania poślizgu? TAK = 1, NIE = 0 2. Czy system wykrywania poślizgu ma zastosowane fizyczne zabezpieczenie przed dostępem osób nieupoważnionych? TAK = 1, NIE = 0	Iloczyn odpowiedzi: 0 lub 1
RMF-9.4 1. Czy przedziały techniczne i szafy aparaturowe są fizycznie zabezpieczone przed dostępem osób nieuprawnionych? TAK = 1, NIE = 0 2. Czy zastosowano zabezpieczenia fizyczne uniemożliwiające podłączenie się do magistrali CAN osobom nieupoważnionym, w tym maszynistom? TAK = 1, NIE = 0 3. Czy zastosowano zabezpieczenia fizyczne uniemożliwiające podłączenie się do sieci LAN osobom nieupoważnionym? TAK = 1, NIE = 0	Iloczyn odpowiedzi: 0 lub 1
RMF-9.5 1. Czy system udostępniania internetu pasażerom (w tym kable, urządzenia aktywne, złącza, bufory, itp.) jest fizycznie odseparowany od wszelkich systemów i sieci pokładowych z wyjątkiem systemów sprzedaży prasy, artykułów spożywczych i ewentualnie biletów? TAK = 1, NIE = 0 2. Czy istnieje zabezpieczenie przed możliwością nieuprawnionej ingerencji w pokładową sieć WiFi? TAK = 1, NIE = 0	Iloczyn odpowiedzi: 0 lub 1
RMF-9.6 1. Czy systemy sprzedaży prasy, artykułów spożywczych i ewentualnie biletów (w tym wykorzystywane kable, urządzenia aktywne, złącza, bufory, itp.) jest fizycznie odseparowany od wszelkich systemów i sieci pokładowych z wyjątkiem systemu udostępniania internetu? TAK = 1, NIE = 0	Odpowiedz: 0 lub 1
Zbiorcza wartość referencyjna dla grupy RMF-G09 iloczyn wartości referencyjnych RMF-9.1 ÷ RMF-9.6	0 lub 1 lub 2

--- --- ---

4.1.5.4. Ocena typu pasażerskiego taboru kolejowego w zakresie cyberbezpieczeństwa

Wszystkie systemy mikroprocesorowe i sprzęt pomocniczy, taki jak systemy diagnostyczne i cały sprzęt komunikacyjny, muszą być zaprojektowane, przetestowane i dostarczone z uwzględnieniem odpowiednich środków cyberbezpieczeństwa, aby zapobiec narażeniu na ryzyko związane z zagrożeniami zewnętrznymi.

Zagrożenia te należy identyfikować jako:
- zagrożenia dotyczące serwerów wewnętrznych odnoszące się do pojazdów znajdujących się w terenie
- zagrożenia dla pojazdów dotyczące kanałów komunikacyjnych
- zagrożenia dla pojazdów dotyczące ich procedur aktualizacji
- zagrożenia dla pojazdów związane z niezamierzonymi działaniami człowieka ułatwiającymi cyberataki
- zagrożenia dla pojazdów związane z ich zewnętrzną łącznością i połączeniami
- zagrożenia dla danych/kodów pojazdu
- potencjalne podatności, które mogą zostać wykorzystane, jeżeli nie będą wystarczająco chronione lub jeżeli stosowne mechanizmy zabezpieczające . nie zostaną wzmocnione

W analizie zagrożeń należy uwzględnić również możliwe skutki ataku. Mogą one pomóc w ustaleniu dotkliwości ryzyka i określeniu dodatkowych zagrożeń. Możliwe skutki ataku mogą obejmować:
- wpływ na bezpieczne działanie pojazdu;
- zatrzymanie funkcji pojazdu;
- modyfikację oprogramowania, zmianę działania;
- zmianę oprogramowania bez wpływu na działanie;
- naruszenie integralności danych;
- naruszenie poufności danych;

- utratę danych;
- inne skutki, w tym o charakterze kryminalnym.

Przyjmuje się, że oprogramowanie wykonane, skonfigurowane, wykorzystywane i aktualizowane zgodnie z normami określającymi wymagania dla bezpieczeństwa oprogramowania to jest normami PN EN 50128 oraz PN EN 50657 [11], które łącznie w roku 2023 zastępuje norma EN 50716, które jest instalowane, użytkowane, monitorowane i aktualizowane zgodnie z wymaganiami norm serii PN-EN ISO/IEC 62443 [14] dla systemów/podsystemów/komponentów z oprogramowaniem, które są przeznaczone dla wykorzystywania w systemach sterowania i automatyki przemysłowej, zapewnia odpowiedni poziom bezpieczeństwa funkcjonalnego. Jednocześnie uznaje się, że mimo to bezpieczeństwo funkcjonalne może być przedmiotem działań, prowadzących do jago zagrożenia. Dlatego konieczne jest przestrzeganie wymagań wskazanych poniżej, których weryfikowaniu służą karty kontrolne od G9 do G14.

Wymagania ogólne dotyczące cyberbezpieczeństwa pasażerskiego taboru kolejowego:

1. Należy przeprowadzić ocenę zagrożeń i podatności podsystemu Dostawcy poprzez określenie wpływu/prawdopodobieństwa dla następujących wektorów ataku w oparciu o szczegóły podsystemu:
    a. wandalizm;
    b. podsłuch;
    c. podszywanie się pod urządzenie/użytkownika;
    d. ataki słownikowe;
    e. modyfikacja wiadomości;
    f. przejęcie sesji;
    g. przepełnienie bufora;
    h. odmowa usługi;
    i. zagłuszanie (odmowa usługi w warstwie fizycznej);
    j. infekcja wirusem/robakiem;
    k. nieautoryzowana instalacja oprogramowania; oraz
    l. nieautoryzowany dostęp roota/administratora.
2. System powinien być zaprojektowany tak, aby był zasadniczo cyberbezpieczny zgodnie z najlepszymi praktykami. IEC 62443 dla ogólnego podejścia do cyberbezpieczeństwa.
3. Stosowane schematy szyfrowania i uwierzytelniania muszą być zatwierdzone do aktywnego użytku (np. nie mogą być zastąpione lub przestarzałe) przez odpowiednie organy zarządzające. Protokoły ze znanymi wadami lub złamanymi zabezpieczeniami (np. WEP) są zabronione.
4. Nieużywane funkcje, które nie są wymagane do działania lub konserwacji węzła sieci lub urządzenia końcowego, powinny zostać usunięte (np. biblioteki oprogramowania, porty komunikacyjne). Jeśli usunięcie nie jest technicznie wykonalne, należy je wyłączyć.

   Należy udokumentować funkcje, które nie są wymagane, w tym metodę ich usunięcia lub wyłączenia. Jeśli jakiekolwiek funkcje nie mogą zostać usunięte lub wyłączone, należy wyjaśnić przyczynę techniczną i oszacować wszelkie związane z tym ryzyko, a także sposób jego ograniczenia.
5. Systemy powinny stosować zasadę najmniejszych uprawnień w celu umożliwienia dostępu w przypadku zapewnienia hierarchii uprawnień konta użytkownika, aby umożliwić każdemu kontu użytkownika dostęp tylko do wymaganych funkcji. Zapewniają metodę ochrony przed nieautoryzowaną eskalacją uprawnień.
6. Systemy pojazdów powinny być zaprojektowane z uwzględnieniem planowanych przyszłych możliwości poprawy bezpieczeństwa, tak aby przez cały okres eksploatacji pojazdów wszelkie używane protokoły, które staną się przestarzałe, mogły zostać zaktualizowane lub zastąpione.

7. Należy zweryfikować i przedłożyć dokumentację systemu potwierdzającą, że nieautoryzowane urządzenia rejestrujące (np. rejestratory kluczy, kamery i mikrofony) nie zostały zainstalowane w systemie po jego dostarczeniu do Zamawiającego.
8. W razie potrzeby zastosować ograniczenie szybkości przychodzenia/wychodzenia na portach urządzeń końcowych.
9. Przed dostarczeniem oprogramowania należy monitorować listę Common Vulnerabilities and Exposures (CVE) pod kątem wszystkich odpowiednich wpisów.

   Wszelkie mające zastosowanie CVE z Common Vulnerability Scoring System (CVSS) o nasileniu średnim lub wyższym muszą zostać złagodzone przed akceptacją pojazdu.
10. Wszystkie logowania użytkowników muszą być uwierzytelnione i autoryzowane przez urządzenie końcowe przed zezwoleniem na dostęp do systemu. Zabronione są logowania weryfikowane wyłącznie na PTU.
11. Komunikacja wymagająca przesyłania haseł lub tokenów sesji przez sieć (np. logowanie do PTU lub przesyłanie plików) musi odbywać się przy użyciu szyfrowanego połączenia (np. HTTPS, FTPS, SFTP).
12. Hasła muszą być przechowywane w zatwierdzonym jednokierunkowym formacie hashowanym; hasła nie mogą być przechowywane w postaci zwykłego tekstu, rejestrowane ani zakodowane na stałe w oprogramowaniu lub skryptach. Przestarzałe protokoły haszujące są zabronione (np. SHA1).
13. Wszelkie hasła fabryczne, które mogą być publicznie dostępne, należy zastąpić hasłami spełniającymi wymagania określone powyżej.
14. Fizyczne porty i usługi węzła sieciowego nieużywane do obsługi lub konserwacji pojazdu muszą być wyłączone.
15. Systemy powinny wdrożyć podejście do gromadzenia i przechowywania plików dziennika bezpieczeństwa.
    a. Pliki dziennika bezpieczeństwa powinny zawierać zdarzenia ze znacznikami czasowymi, aby umożliwić audyty i dochodzenia, podobnie jak w przypadku dzienników syslog.
    b. Pliki dziennika zabezpieczeń powinny być tylko do odczytu dla wszystkich kont użytkowników, w tym kont administratorów, i zapewniać metodę sprawdzania integralności dziennika.
    c. Podejście to powinno obejmować co najmniej następujące zdarzenia (stosownie do ich funkcji):
        i. żądania informacji i odpowiedzi urządzeń
        ii. udane i nieudane próby uwierzytelnienia i dostępu
        iii. zmiany konta
        iv. uprzywilejowane użycia
        v. ścieżki audytu znaczników czasu i pliki dziennika w uniwersalnym czasie koordynowanym (UTC).
16. Systemy powinny zapewniać sposób dostępu do systemu, biorąc pod uwagę fizyczny dostęp do urządzenia, aby zapobiec zablokowaniu systemu w przypadku utraty haseł. Działanie to powinno być rejestrowane i możliwe do skontrolowania.
17. Systemy pojazdów powinny być zaprojektowane z uwzględnieniem planowanych przyszłych możliwości poprawy bezpieczeństwa, tak aby przez cały okres eksploatacji pojazdów wszelkie używane protokoły, które staną się przestarzałe, mogły zostać zaktualizowane lub zastąpione.
18. W stosownych przypadkach całe dostarczone oprogramowanie musi być skonfigurowane zgodnie z krajowym programem list kontrolnych. Wymóg ten powinien być stosowany do

wszystkich komponentów oprogramowania, do których mają zastosowanie krajowe listy kontrolne.

Wymagania dodatkowe dotyczące cyberbezpieczeństwa pasażerskiego taboru kolejowego w odniesieniu do systemów z dostępem bezprzewodowym:

Jeśli oferowany system ma dostęp bezprzewodowy lub przytorowy/przydrożny/naziemny, należy spełnić następujące wymagania zgodnie ze specyfikacją techniczną:

1. Komunikacja bezprzewodowa z sieci pokładowej poza pojazdem do usług przydrożnych powinna odbywać się za pośrednictwem połączenia VPN..
2. Komunikacja powinna być bezpieczna i szyfrowana, aby uniemożliwić nieautoryzowanym użytkownikom dostęp do danych lub systemu. Komunikacja powinna odbywać się zarówno przy użyciu bezpiecznej łączności bezprzewodowej, jak i tunelu VPN do przydrożnego systemu monitorowania i diagnostyki (WMDS). Cały ruch inny niż VPN powinien być automatycznie odrzucany.
3. Przekazanie informacji na temat całej komunikacji (np. protokołów) wymaganej między siecią pokładową a usługami przydrożnymi - zarówno przychodzącymi, jak i wychodzącymi - oraz zidentyfikowanie każdej z nich.
4. Ocena podatności na włamania za pośrednictwem dostępu bezprzewodowego powinna być udokumentowana w ‘planie zapewniania cyberbezpieczeństwa przyjętym przez dostawcę’ (Supplier Cybersecurity Assurance Plan – SCAP).

4.1.5.5. Karty kontrolne dla oceny typu pasażerskiego taboru kolejowego w zakresie cyberbezpieczeństwa

Niniejsze karty należy wypełnić dla analizowanego typu taboru poprzez przypisanie odpowiedziom wartości wg wzoru. Zaznacza się, że w ramach dowodu spójności bezpieczeństwa, ochrony i cyberbezpieczeństwa należy uwzględnić informacje pozwalające na zweryfikowanie odpowiedzi. Stosowne dane mogą być zawarte w pełnym zakresie w dowodzie lub częściowo opierać się na przywoływanych dokumentach, które wówczas muszą być udostępnione jednostce oceniającej dowód.

Cztery karty kontrolne od G10 do G13 powinny zostać wypełnione osobno dla każdego systemu/podsystemu/komponentu zawierającego elementy programowe z wyłączeniem jedynie systemów/podsystemów/komponentów, które dedykowane są do funkcji związanych z zapewnieniem bezpieczeństwa ruchu kolejowego i objęte są w pełni właściwymi i wiarygodnymi dowodami bezpieczeństwa potwierdzającymi zastosowanie zasady SIL-4 dla konkretnego zastosowania (Specific Application Safety Case SASC) opracowanymi oraz zweryfikowanymi zgodnie z normami RAMS [9÷13].

UWAGA: Karty kontrolne od G10 do G13 przywołują normy serii 27000 oraz normy serii 62443. Istnieje możliwość stosowania systemów/podsystemów/komponentów z oprogramowaniem, które zostały zweryfikowane na zgodność z innymi podobnymi normami np. amerykańskimi, ale w takich przypadkach konieczne jest przeprowadzenie porównania wymagań i opracowanie oceny ryzyka uwzględniającej wszystkie ryzyka wynikające z ewentualnych różnic w wymaganiach.

Karta kontrolna cyberbezpieczeństwa RMF-G10 bezpieczne tworzenie oprogramowania
Założenia: Tworzenie oprogramowania powinno odbywać się w sposób skoordynowany, z pełnym nadzorem nad bezpieczeństwem oprogramowania oraz w zgodzie z właściwymi dokumentami normatywnymi.

Pytania kontrolne	**Wartości ref.**
RMF-10.1 – proces bezpieczeństwa przy tworzeniu oprogramowania 1. Czy jest wprowadzony proces bezpieczeństwa zgodnie z normą IEC 62443-2-1? TAK = 1, NIE = 0 2. Czy wymagane właściwości zostały wykazane przez analizę/testowanie? TAK = 1, NIE = 0	Iloczyn odpowiedzi: 0 lub 1

RMF-10.2 – analiza zagrożeń 1. Czy została przeprowadzona analiza zagrożeń bezpieczeństwa i ryzyka, np. zgodnie z normą zgodnie z ISO 27005 w oparciu o model zagrożeń z IEC 62443-4-1 rozdz. 6.3? TAK = 1, NIE = 0 2. Czy przeprowadzono test bezpieczeństwa IT, co najmniej test podatności z zgodnie z IEC 62443-4-1 rozdział 9.4? TAK = 1, NIE = 0 3. Czy jest wdrożony proces usuwania luk w zabezpieczeniach zgodnie z normą IEC 62443-4-1 rozdział 10? TAK = 1, NIE = 0 4. Czy jest wdrożony interfejs dla powiadomień o stwierdzonych lukach w zabezpieczeniach? TAK = 1, NIE = 0 5. Czy wymagane właściwości zostały wykazane przez analizę/testowanie? TAK = 1, NIE = 0	Iloczyn odpowiedzi: 0 lub 1
RMF-10.3 – osoba odpowiedzialna za bezpieczeństwo oprogramowania 1. Czy jest wyznaczona osoba kontaktowa odpowiedzialną za bezpieczeństwo IT dla zakresu danego systemu/podsystemu/komponentu z oprogramowaniem? TAK = 1, NIE = 0 2. Czy jest zapewniony odpowiedni personel, posiadający wystarczającą wiedzę w zakresie bezpieczeństwa IT? TAK = 1, NIE = 0 3. Czy jest wdrożony proces powiadamiania o zmianach personelu odpowiedzialnego za bezpieczeństwo IT? TAK = 1, NIE = 0 4. Czy wymagane właściwości zostały wykazane przez analizę/testowanie? TAK = 1, NIE = 0	Iloczyn odpowiedzi: 0 lub 1
RMF-10.4 – wrażliwe dane systemu/podsystemu/komponentu zawierającego elementy programowe 1. Czy jest wprowadzony proces określający, że wrażliwe dane projektu (np. dokumenty bezpieczeństwa IT, dane, konfiguracje oprogramowania, dokumenty poufne) muszą być przetwarzane i przekazywane w sposób bezpieczny (np. nie mogą być przesyłane pocztą elektroniczną i innymi technologiami elektronicznymi bez zaszyfrowania)? TAK = 1, NIE = 0 2. Czy wymagane właściwości zostały wykazane przez analizę/testowanie? TAK = 1, NIE = 0	Iloczyn odpowiedzi: 0 lub 1
RMF-10.5 – dostępność wsparcia technicznego dla oprogramowania 1. Czy jest wprowadzony proces określający, że używane oprogramowanie i oprogramowanie sprzętowe nie są wycofane ze wsparcia technicznego (koniec okresu eksploatacji nie został jeszcze osiągnięty) w momencie dostawy? TAK = 1, NIE = 0 2. Czy jest pisemne potwierdzenie, że używane oprogramowanie i oprogramowanie sprzętowe nie są wycofane ze wsparcia (koniec okresu nie został jeszcze osiągnięty) w momencie dostawy? TAK = 1, NIE = 0 3. Czy wymagane właściwości zostały wykazane przez analizę/testowanie? TAK = 1, NIE = 0	Iloczyn odpowiedzi: 0 lub 1
RMF-10.6 – cyberbezpieczeństwo w całym okresie eksploatacji 1. Czy Dostawca systemów i komponentów podłączonych do dowolnej sieci łączności pociągów zaproponował plan mający na celu zapewnienie cyberbezpieczeństwa systemu przez cały okres jego eksploatacji? TAK = 1, NIE = 0 2. Czy wymagane właściwości zostały wykazane przez analizę/testowanie? TAK = 1, NIE = 0 3. Czy jeśli system zostanie dotknięty nową luką w zabezpieczeniach, dostawca powiadomi zamawiającego/użytkownika i dostarczy odpowiednią poprawkę bezpieczeństwa? TAK = 1, NIE = 0 4. Czy te rozwiązania i warunki są opisane w planie zapewniania cyberbezpieczeństwa SCAP? TAK = 1, NIE = 0 5. Czy wymagane właściwości zostały wykazane przez analizę/testowanie? TAK = 1, NIE = 0	Iloczyn odpowiedzi: 0 lub 1
Zbiorcza wartość referencyjna dla grupy RMF-G10 **dla danego systemu/podsystemu/komponentu z oprogramowaniem** iloczyn wartości referencyjnych RMF-10.1 ÷ RMF-10.6	Iloczyn odpowiedzi: 0 lub 1

--- --- ---

Karta kontrolna cyberbezpieczeństwa RMF-G11 kontrola dostępu
Założenia: Systemy/podsystemy/komponenty z oprogramowaniem powinny być odpowiednio zabezpieczone przed nieuprawnionym dostępem. W okresie eksploatacji kontrolę nad dostępem powinien sprawować przewoźnik lub podmiot odpowiedzialny za utrzymanie taboru. Kontrola taka może być powierzona producentowi, ale wówczas przewoźnik lub podmiot odpowiedzialny za utrzymanie taboru mszą sprawować nad nią nadzór..

Pytania kontrolne	Wartości ref.
RMF-11.1 – ograniczanie dostępu do niewykorzystywanych funkcji, portów, protokołów i/lub usług 1. Czy systemy/podsystemy/komponenty z oprogramowaniem podłączone do dowolnej sieci łączności pociągowej zapobiegają lub odpowiednio ograniczają korzystanie z niepotrzebnych funkcji, portów, protokołów i/lub usług? TAK = 1, NIE = 0 2. Czy używane porty, protokoły lub usługi są udokumentowane w specyfikacji zabezpieczeń? TAK = 1, NIE = 0 3. Czy wymagane właściwości zostały wykazane przez analizę/testowanie? TAK = 1, NIE = 0	Iloczyn odpowiedzi: 0 lub 1
RMF-11.2 – wyłączanie niewykorzystywanych portów fizycznych 1. Czy systemy/podsystemy/komponenty z oprogramowaniem podłączone do dowolnej sieci komunikacyjnej pociągu zostały poddane procesowi wzmocnienia/utwardzania (hardening) w celu wyłączenia niepotrzebnych portów fizycznych? TAK = 1, NIE = 0 2. Czy istniejące porty fizyczne, porty włączone i porty wyłączone zostały określone w planie zapewniania cyberbezpieczeństwa SCAP? TAK = 1, NIE = 0 3. Czy wymagane właściwości zostały wykazane przez analizę/testowanie? TAK = 1, NIE = 0	Iloczyn odpowiedzi: 0 lub 1
RMF-11.3 – zapewnienie braku dostępność niepotrzebnych zasobów 1. Czy systemy/podsystemy/komponenty z oprogramowaniem mają wyłączone niepotrzebne funkcje, porty, protokoły i/lub usługi? TAK = 1, NIE = 0 2. Czy zastosowano zasady zgodne z IEC 62443-3-3: FR 7: Dostępność zasobów? TAK = 1, NIE = 0 3. Czy w odniesieniu do systemów, których restart może być obserwowany przez pasażerów zastosowano zasadę bootowania systemów z ukrytym ciągiem zdarzeń (tzw. silent boot)? TAK = 1, NIE = 0 4. Czy wymagane właściwości zostały wykazane przez analizę/testowanie? TAK = 1, NIE = 0	Iloczyn odpowiedzi: 0 lub 1
RMF-11.4 – wymagania informacyjne w planie zapewniania cyberbezpieczeństwa SCAP 1. Czy dla każdego wcześniej zidentyfikowanego portu logicznego/usługi/protokołu określono następujące informacje w planie zapewniania cyberbezpieczeństwa SCAP: - port fizyczny - numer logicznego portu IP (jeśli sieć Ethernet) - protokół komunikacyjny - opis funkcji/uzasadnienie? TAK = 1, NIE = 0 2. Czy wymagane właściwości zostały wykazane przez analizę/testowanie? TAK = 1, NIE = 0	Iloczyn odpowiedzi: 0 lub 1
RMF-11.5 – identyfikacja i uwierzytelnianie na interfejsach 1. Czy systemy/podsystemy/komponenty z oprogramowaniem podłączone do dowolnej sieci łączności pociągowej wymuszają identyfikację i uwierzytelnianie we wszystkich interfejsach zarządzania, konfiguracji lub diagnostyki wszystkich użytkowników, oprogramowania procesów i urządzeń? TAK = 1, NIE = 0 2. Czy wymuszanie takiej identyfikacji i uwierzytelniania ma miejsce na wszystkich interfejsach zapewniających dostęp do systemu? TAK = 1, NIE = 0 3. Czy jest wymuszanie szyfrowania danych uwierzytelniających? TAK = 1, NIE = 0 4. Czy nieużywane interfejsy fizyczne (np. USB, Ethernet / Profinet, Wi-Fi, Bluetooth), jak również porty debugowania są dezaktywowane lub mechanicznie zablokowane? TAK = 1, NIE = 0	

5. Czy mechanizmy automatycznego uruchamiania są chronione (np. hasłem) lub dezaktywowane? TAK = 1, NIE = 0 6. Czy w przypadku każdego interfejsu zarządzania, konfiguracji i diagnostyki w planie zapewniania cyberbezpieczeństwa SCAP określono następujące informacje: - mechanizm uwierzytelniania? - protokół mechanizmu uwierzytelniania? TAK = 1, NIE = 0 7. Czy wymagane właściwości zostały wykazane przez analizę/testowanie? TAK = 1, NIE = 0	Iloczyn odpowiedzi: 0 lub 1
RMF-11.6 – hasła i/lub zabezpieczenie alternatywne zapewniające taki sam lub wyższy poziom zabezpieczenia 1. Czy w systemach/podsystemach/komponentach z oprogramowaniem i ich komponentach podłączonych do dowolnej sieci łączności pociągów zastosowano domyślne zmiany hasła i zastosowano politykę silnych haseł? TAK = 1, NIE = 0 2. Czy w systemach/podsystemach/komponentach i ich komponentach z oprogramowaniem podłączonych do dowolnej sieci łączności pociągów, zastosowano warunek, że nie wolno używać niezmienionych haseł domyślnych (np. klucza hosta SSH, klucza prywatnego samodzielnie podpisanych certyfikatów)? TAK = 1, NIE = 0 3. Czy mechanizm uwierzytelniania wymusza ustanowienie silnego hasła opartego na wielkich i małych literach, znakach niealfanumerycznych (tj. $, %, &, @, ...) i długości co najmniej 12 znaków? TAK = 1, NIE = 0 4. Czy systemy, podsystemy, komponenty są dostarczane z hasłami, które odpowiadają regułom złożoności ustalonym przez integratora w zakresie długości hasła i typów znaków? TAK = 1, NIE = 0 5. Czy integrator ma możliwość zmiany haseł i kluczy (czy brak jest zakodowanych sekretów w obrazie oprogramowania/oprogramowania układowego (SW/FW)? TAK = 1, NIE = 0 6. Czy hasła i klucze są chronione przed nieautoryzowaną modyfikacją i ujawnieniem w spoczynku i podczas transportu? TAK = 1, NIE = 0 7. Czy dla systemów/podsystemów/komponentów z oprogramowaniem podłączonych do dowolnej sieci łączności pociągowej jest wprowadzony wymóg przekazania listy haseł, mechanizmów zmiany poświadczeń, również resetowania i odzyskiwania haseł dla wszystkich kont (użytkowników i składników) integratorowi systemu/sieci? TAK = 1, NIE = 0 8. Czy hasła zostały przekazane integratorowi przed rozpoczęciem rozruchu statycznego? TAK = 1, NIE = 0 9. Czy wymagane właściwości zostały wykazane przez analizę/testowanie? TAK = 1, NIE = 0	Iloczyn odpowiedzi: 0 lub 1
RMF-11.7 – dzienniki logowania 1. Czy systemy/podsystemy/komponenty z oprogramowaniem podłączone do dowolnej sieci łączności pociągów zapewniają możliwość generowania dzienników istotnych dla bezpieczeństwa dla kategorii: próby logowania? TAK = 1, NIE = 0 2. Czy Dzienniki te są dostępne dla przewoźnika lub podmiotu odpowiedzialnego za utrzymanie taboru? TAK = 1, NIE = 0 3. Czy w planie zapewniania cyberbezpieczeństwa SCAP określono następujące informacje: - mechanizm/procedura dostępu do pliku dziennika - plik dziennika zawierający zdarzenie próby logowania - format pliku dziennika i informacje w nim zawarte? TAK = 1, NIE = 0 4. Czy wymagane właściwości zostały wykazane przez analizę/testowanie? TAK = 1, NIE = 0	Iloczyn odpowiedzi: 0 lub 1
RMF-11.8 – wykluczanie prostych haseł 1. Czy systemy/podsystemy/komponenty z oprogramowaniem, które wymagają uwierzytelniania hasłem, stosują wytyczne dotyczące najlepszych praktyk w zakresie konfiguracji haseł i wykluczają hasła domyślne? TAK = 1, NIE = 0 2. Czy hasła są konfigurowalne przez Operatora?	

TAK = 1, NIE = 0 3. Czy kontrola identyfikacji i uwierzytelniania realizowana jest zgodnie z IEC 62443-3-3: FR 1: Kontrola identyfikacji i uwierzytelniania? TAK = 1, NIE = 0 4. Czy wymagane właściwości zostały wykazane przez analizę/testowanie? TAK = 1, NIE = 0	Iloczyn odpowiedzi: 0 lub 1
RMF-11.9 – uwierzytelnianie 1. Czy dostęp do systemów/podsystemów/komponentów z oprogramowaniem jest zapewniony poprzez uwierzytelnianie? TAK = 1, NIE = 0 2. Czy wymagane właściwości zostały wykazane przez analizę/testowanie? TAK = 1, NIE = 0	Iloczyn odpowiedzi: 0 lub 1
RMF-11.10 – szyfrowanie 1. Czy systemy/podsystemy/komponenty z oprogramowaniem, które stosują szyfrowanie, są zgodne z najlepszymi praktykami i standardami dotyczącymi ich mechanizmów kryptograficznych? TAK = 1, NIE = 0 2. Czy zastosowano wymagania dotyczące poufności zdefiniowane w IEC 62443-3-3: FR 4: Poufność danych? TAK = 1, NIE = 0 3. Czy wymagane właściwości zostały wykazane przez analizę/testowanie? TAK = 1, NIE = 0	Iloczyn odpowiedzi: 0 lub 1
Zbiorcza wartość referencyjna dla grupy RMF-G11 **dla danego systemu/podsystemu/komponentu z oprogramowaniem** iloczyn wartości referencyjnych RMF-11.1 ÷ RMF-11.10	Iloczyn odpowiedzi: 0 lub 1

--- --- ---

Karta kontrolna cyberbezpieczeństwa RMF-G12 zarządzanie konfiguracją
Założenia: Procesy/podsystemy/komponenty z oprogramowaniem powinny być odpowiednio konfigurowane.

Pytania kontrolne	Wartości ref.
RMF-12.1 – integralność oprogramowania 1. Czy Dostawca gwarantuje, że integralność oprogramowania i oprogramowania układowego (firmware) dla jego komponentów obejmuje ochronę przed ukierunkowaną manipulacją oprogramowaniem lub firmwar'em które można załadować do systemu/podsystemu/komponentu? TAK = 1, NIE = 0 2. Czy jest stosowane sprawdzenie podpisu cyfrowego oprogramowania po załadowaniu do komponentu w oparciu o algorytmy podpisu oparte na kryptografii asymetrycznej lub algorytmach HMAC. TAK = 1, NIE = 0 3. Czy wymagane właściwości zostały wykazane przez analizę/testowanie? TAK = 1, NIE = 0	Iloczyn odpowiedzi: 0 lub 1
RMF-12.2 – dzienniki zmiany konfiguracji 1. Czy systemy/podsystemy/komponenty z oprogramowaniem podłączone do dowolnej sieci łączności pociągowej zapewniają możliwość generowania dzienników związanych z bezpieczeństwem następujących kategorii: zmiany konfiguracji. TAK = 1, NIE = 0 2. Czy Dzienniki te są dostępne dla przewoźnika lub podmiotu odpowiedzialnego za utrzymanie? TAK = 1, NIE = 0 3. Czy w planie zapewniania cyberbezpieczeństwa SCAP określono następujące informacje: - mechanizm/procedura dostępu do pliku dziennika - plik dziennika zawierający zdarzenie zmiany konfiguracji - format pliku dziennika i informacje w nim zawarte TAK = 1, NIE = 0 4. Czy wymagane właściwości zostały wykazane przez analizę/testowanie? TAK = 1, NIE = 0	Iloczyn odpowiedzi: 0 lub 1
RMF-12.3 – możliwość zewnętrznego nadzoru nad dziennikami 1. Czy systemy/podsystemy/komponenty z oprogramowaniem i ich komponenty zapewniają możliwość automatycznego i natychmiastowego przesyłania wygenerowanych dzienników do zewnętrznych systemów zarządzania dziennikami przy użyciu najlepszych w branży protokołów (na przykład syslog)?	Iloczyn odpowiedzi: 0 lub 1

TAK = 1, NIE = 0 2. Czy wymagane właściwości zostały wykazane przez analizę/testowanie? TAK = 1, NIE = 0	
RMF-12.4 – znane luki w zabezpieczeniach 1. Czy systemy/podsystemy/komponenty z oprogramowaniem podłączone do dowolnej sieci łączności pociągów są wolne od znanych luk w zabezpieczeniach? TAK = 1, NIE = 0 2. Czy w planie zapewniania cyberbezpieczeństwa SCAP określono następujące informacje: - Raport ze skanowania pod kątem luk we wszystkich fizycznych portach Ethernet? TAK = 1, NIE = 0 3. Czy wymagane właściwości zostały wykazane przez analizę/testowanie? TAK = 1, NIE = 0	Iloczyn odpowiedzi: 0 lub 1
RMF-12.5 – alerty dla zmian konfiguracji 1. Czy w przypadku systemów/podsystemów/komponentów z oprogramowaniem, do których możliwy jest dostęp człowieka (np. w celu wykonania aktualizacji oprogramowania, zmian konfiguracji), są generowane alerty, które mogą być dostarczane do systemu zewnętrznego w przypadku dostępu i/lub zmiany? TAK = 1, NIE = 0 2. Czy odpowiadająca za to funkcjonalność jest zgodna z wymaganiami IEC 62443-3-3: FR 2: Kontrola użytkowania, lub podobną normą? TAK = 1, NIE = 0 3. Czy wymagane właściwości zostały wykazane przez analizę/testowanie? TAK = 1, NIE = 0	Iloczyn odpowiedzi: 0 lub 1
RMF-12.6 – ochrona przed ujawnieniem i modyfikacją danych 1. Czy systemy/podsystemy/komponenty z oprogramowaniem mają możliwość ochrony danych przed nieuprawnionym ujawnieniem lub modyfikacją, a także środki proceduralne umożliwiające usunięcie danych poprzez ich wymianę lub wyłączenie? TAK = 1, NIE = 0 2. Czy wymagane właściwości zostały wykazane przez analizę/testowanie? TAK = 1, NIE = 0	Iloczyn odpowiedzi: 0 lub 1
RMF-12.7 – aktualizacje i uaktualnienia poprawkami bezpieczeństwa 1. Czy systemy/podsystemy/komponenty z oprogramowaniem, mają możliwość aktualizacji i uaktualniania za pomocą poprawek bezpieczeństwa dla wszystkich części danego rozwiązania (np. oprogramowania układowego, oprogramowania aplikacyjnego, oprogramowania pośredniczącego)? TAK = 1, NIE = 0 UWAGA: Nie jest wymaganie, aby wszystkie systemy/podsystemy/komponenty z oprogramowaniem obsługiwały takie elementy, jak: automatyczne aktualizacje, regularne procesy łatania zabezpieczeń lub skanowanie luk w zabezpieczeniach. 2. Czy funkcje realizujące te procesy są zgodne z wymaganiami IEC 62443 4-2: FR 3: Integralność systemu, lub podobnymi normami? TAK = 1, NIE = 0 3. Czy wymagane właściwości zostały wykazane przez analizę/testowanie? TAK = 1, NIE = 0	Iloczyn odpowiedzi: 0 lub 1
RMF-12.8 – dokumentowanie bezpiecznej konfiguracji 1. Czy systemy/podsystemy/komponenty z oprogramowaniem mają udokumentowaną bezpieczną konfigurację? TAK = 1, NIE = 0 2. Czy konfiguracja opiera na zalecanych ustawieniach bezpieczeństwa i najlepszych praktykach? TAK = 1, NIE = 0 3. Czy jest zgodna z wymaganiami IEC 62443-3-3: FR 7: Dostępność zasobów? TAK = 1, NIE = 0 4. Czy wymagane właściwości zostały wykazane przez analizę/testowanie? TAK = 1, NIE = 0	Iloczyn odpowiedzi: 0 lub 1
RMF-12.9 – przywracanie znanego stanu bezpiecznego 1. Czy systemy/podsystemy/komponenty z oprogramowaniem umożliwiają odzyskanie i przywracanie do znanego stanu bezpiecznego po zakłóceniu lub awarii? TAK = 1, NIE = 0 2. Czy odbywa się to zgodnie z IEC 62443-3-3: FR 7: Dostępność zasobów TAK = 1, NIE = 0 3. Czy wymagane właściwości zostały wykazane przez analizę/testowanie? TAK = 1, NIE = 0	Iloczyn odpowiedzi: 0 lub 1
RMF-12.10 – generowanie zdarzeń 1. Czy systemy/podsystemy/komponenty z oprogramowaniem mają możliwość generowania zdarzeń związanych z bezpieczeństwem i przesyłania ich do aplikacji	

zewnętrznych? TAK = 1, NIE = 0 UWAGA: Zdolność ta może być zapewniana bezpośrednio przez systemy/ podsystemy/komponenty lub pośrednio poprzez alternatywne środki? 2. Czy jest ona realizowana zgodnie z wymaganiami IEC 62443-3-3: FR 2: Kontrola użycia, lub podobnych norm. TAK = 1, NIE = 0 3. Czy wymagane właściwości zostały wykazane przez analizę/testowanie? TAK = 1, NIE = 0	Iloczyn odpowiedzi: 0 lub 1
RMF-12.11 – egzekwowanie ograniczeń użytkownika 1. Czy systemy/podsystemy/komponenty z oprogramowaniem oraz sieci mają możliwość egzekwowania ograniczeń użytkowania (np. ograniczeń użytkowania w zakresie wyłączania nieużywanych portów USB, białej listy i kontroli dostępu do sieci)? TAK = 1, NIE = 0 2. Czy odbywa się to zgodnie z wymaganiami IEC 62443-3-3: FR-2: Kontrola użytkowania, lub innych podobnych norm? TAK = 1, NIE = 0 3. Czy wymagane właściwości zostały wykazane przez analizę/testowanie? TAK = 1, NIE = 0	Iloczyn odpowiedzi: 0 lub 1
RMF-12.12 – nieudane instalacje aktualizacji 1. Czy systemy/podsystemy/komponenty z oprogramowaniem posiadają mechanizmy zapewniające bezpieczny powrót do poprzedniego stanu w przypadku nieudanej instalacji aktualizacji? TAK = 1, NIE = 0 2. Czy wymagane właściwości zostały wykazane przez analizę/testowanie? TAK = 1, NIE = 0	Iloczyn odpowiedzi: 0 lub 1
RMF-12.13 – wykrywanie nieautoryzowanych zmian oprogramowania 1. Czy wykrywane są nieautoryzowane zmiany w oprogramowaniu i oprogramowaniu układowym (firmware) używanym przez systemy/podsystemy/komponenty z oprogramowaniem? TAK = 1, NIE = 0 2. Czy wymagane właściwości zostały wykazane przez analizę/testowanie? TAK = 1, NIE = 0	Iloczyn odpowiedzi: 0 lub 1
RMF-12.14 – wykrywanie złośliwego oprogramowania (malware'u) 1. Czy systemy/podsystemy/komponenty z oprogramowaniem mają możliwość wykrywania i zgłaszania złośliwego lub nieautoryzowanego oprogramowania? TAK = 1, NIE = 0 2. Czy odbywa się to zgodnie z wymaganiami IEC 62443-3-3: FR 3: Integralność systemu, lub innych podobnych norm? TAK = 1, NIE = 0 3. Czy wymagane właściwości zostały wykazane przez analizę/testowanie? TAK = 1, NIE = 0	Iloczyn odpowiedzi: 0 lub 1
RMF-12.15 – fizyczne zabezpieczenie złącz 1. Czy systemy/podsystemy/komponenty z oprogramowaniem, które mają złącza tworzące punkt wejścia do samego systemu/podsystemu/komponentu i/lub sieci (oprócz ich własnego połączenia sieciowego), są fizycznie zabezpieczone? TAK = 1, NIE = 0 2. Czy wymagane właściwości zostały wykazane przez analizę/testowanie? TAK = 1, NIE = 0	Iloczyn odpowiedzi: 0 lub 1
RMF-12.16 – odporność na przeciążenia 1. Czy systemy/podsystemy/komponenty z oprogramowaniem są odporne na przeciążenia i reagują w określony sposób? TAK = 1, NIE = 0 2. Czy uwzględniono różne protokoły i warstwy np. aplikacje internetowe, zastrzeżone protokoły i warstwę sieciową? TAK = 1, NIE = 0 3. Czy wymagane właściwości zostały wykazane przez analizę/testowanie? TAK = 1, NIE = 0	Iloczyn odpowiedzi: 0 lub 1
Zbiorcza wartość referencyjna dla grupy RMF-G12 **dla danego systemu/podsystemu/komponentu z oprogramowaniem** iloczyn wartości referencyjnych RMF-12.1 ÷ RMF-12.16	Iloczyn odpowiedzi: 0 lub 1

--- --- ---

Karta kontrolna cyberbezpieczeństwa RMF-G13 oprogramowanie wspomagające eksploatację i utrzymanie	
Założenia: Konieczne jest zapewnienie bezpieczeństwa korzystania z oprogramowania narzędziowego i serwisowego.	
Pytania kontrolne	**Wartości ref.**
RMF-13.1 – złośliwe oprogramowanie w oprogramowaniu narzędziowym 1. Czy oprogramowanie narzędziowe i serwisowe jest wolne od złośliwego oprogramowania w momencie przekazania integratorowi? TAK = 1, NIE = 0 2. Czy wymagane właściwości zostały wykazane przez analizę/testowanie? TAK = 1, NIE = 0	Iloczyn odpowiedzi: 0 lub 1
RMF-13.1 – ograniczanie praw użytkownikowi oprogramowania narzędziowego 1. Czy oprogramowanie narzędziowe i serwisowe działa z najmniejszymi możliwymi uprawnieniami (np. użytkownik zamiast uprawnień administratora)? TAK = 1, NIE = 0 2. Czy wymagane właściwości zostały wykazane przez analizę/testowanie? TAK = 1, NIE = 0	Iloczyn odpowiedzi: 0 lub 1
Zbiorcza wartość referencyjna dla grupy RMF-G12 **dla danego systemu/podsystemu/komponentu z oprogramowaniem** iloczyn wartości referencyjnych RMF-13.1 ÷ RMF-13.2	Iloczyn odpowiedzi: 0 lub 1

--- --- ---

Kolejna karta kontrolna (karta G14) ma charakter zbiorczy. Karty od G10 do G13 stosuje się dla poszczególnych systemów/podsystemów/komponentów z o[programowaniem, podczas gdy karta G14 ma zastosowanie do oceny zbiorczej cyberbezpieczeństwa danego typu pasażerskiego taboru kolejowego i jako taka bazuje między innymi na kartach systemów/podsystemów/komponentów.

Karta kontrolna cyberbezpieczeństwa RMF-G14 komplet funkcjonalności dedykowanych cyberbezpieczeństwu	
Założenia: 1. Systemy/podsystemy/komponenty realizujące funkcje związane z bezpieczeństwem ruchu powinny być objęte dowodami bezpieczeństwa potwierdzającymi zastosowanie zasady SIL-4 dla konkretnego zastosowania (Specific Application Safety Case SASC) opracowanymi oraz zweryfikowanymi zgodnie z normami RAMS [9÷13]. Ich ponowne weryfikowanie z wykorzystaniem kart kontrolnych od G10 do G13 uznaje się za nadmiarowe i tym samym zbędne. 2. Wszystkie pozostałe systemy/podsystemy/komponenty powinny być objęte analizą z wykorzystaniem kart kontrolnych od G10 do G13, przy czym relacje pomiędzy wszystkimi wydzielonymi systemami/ podsystemami/komponentami z oprogramowaniem powinny być przedstawione na początku rozdziału 4. **dowodu spójności bezpieczeństwa, ochrony i cyberbezpieczeństwa** dla danego typu taboru. 3. Należy zapewnić ochronę przed cyberatakami wszystkim przewodowym i bezprzewodowym systemom transmisji danych, które są wykorzystywane na potrzeby bezpieczeństwa ruchu kolejowego, także tym które są ujęte w dowodach bezpieczeństwa o których mowa w punkcie 1. powyżej. 4. Należy zapewnić ochronę przed cyberatakami wszystkim przewodowym i bezprzewodowym systemom transmisji danych, które są wykorzystywane na potrzeby ochrony transportu kolejowego (bezpieczeństwa transportu).	
Pytania kontrolne	**Wartości ref.**
RMF-14.1 – bezpieczne tworzenie oprogramowania 1. Czy dla wszystkich systemów/podsystemów/komponentów z oprogramowaniem, oprogramowanie tworzono w sposób bezpieczny? (Czy w kartach RMF G10 dla wszystkich pytań dla wszystkich systemów/ podsystemów/komponentów z oprogramowaniem jako właściwe podano odpowiedzi którym przypisano wartość „1”?) TAK = 1, NIE = 0	Iloczyn zbiorczych wartości referencyjnych z kart G10 dla wszystkich systemów/podsystemów/ komponentów 0 lub 1
RMF-14.2 – kontrola dostępu 1. Czy dla wszystkich systemów/podsystemów/komponentów z oprogramowaniem zapewniono odpowiednią kontrolę dostępu? (Czy w kartach RMF G11 dla wszystkich pytań dla wszystkich systemów/ podsystemów/komponentów z oprogramowaniem jako właściwe podano odpowiedzi którym przypisano wartość „1”?) TAK = 1, NIE = 0	Iloczyn zbiorczych wartości referencyjnych z kart G10 dla wszystkich systemów/podsystemów/ komponentów 0 lub 1

RMF-14.3 – zarządzanie konfiguracją 1. Czy dla wszystkich systemów/podsystemów/komponentów z oprogramowaniem zapewniono odpowiednie zarządzanie konfiguracją? (Czy w kartach RMF G12 dla wszystkich pytań dla wszystkich systemów/ podsystemów/komponentów z oprogramowaniem jako właściwe podano odpowiedzi którym przypisano wartość „1”?) TAK = 1, NIE = 0	Iloczyn zbiorczych wartości referencyjnych z kart G10 dla wszystkich systemów/podsystemów/ komponentów 0 lub 1
RMF-14.4 – oprogramowanie wspomagające eksploatację i utrzymanie 1. Czy dla wszystkich systemów/podsystemów/komponentów z oprogramowaniem zapewniono bezpieczeństwo oprogramowania narzędziowego wspomagającego eksploatację i utrzymanie? (Czy w kartach RMF G13 dla wszystkich pytań dla wszystkich systemów/ podsystemów/komponentów z oprogramowaniem jako właściwe podano odpowiedzi którym przypisano wartość „1”?) TAK = 1, NIE = 0	Iloczyn zbiorczych wartości referencyjnych z kart G10 dla wszystkich systemów/podsystemów/ komponentów 0 lub 1
RMF-14.5 – zasilanie awaryjne **1.** Czy pokładowe systemy bezpiecznej kontroli jazdy oraz łączności głosowej (maszynisty z dyżurnym ruchu) mają zapewnione zasilanie rezerwowe w przypadku odłączenia głównego źródła zasilania pozwalające na dalszą pracę w normalnym trybie przez minimum 30 minut, z funkcją informowania maszynisty o załączeniu zasilania rezerwowego i konieczności zatrzymania się w miejscu dogodnym do działań służb (technicznych, ratunkowych, bezpieczeństwa) i ewakuacji przed upływem 30 minut (czasu gwarantowanego zasilania rezerwowego)? TAK = 2, NIE = 1 **2.** Czy systemy/podsystemy/komponenty z oprogramowaniem, które sterują systemami hamowania, sterowania drzwiami i wysuwnymi stopniami, wentylacją, wykrywaniem i gaszeniem pożaru oraz informacją pasażerską (minimum głosową) i systemami wspierającymi bezpieczeństwo pasażerów (awaryjnego otwierania drzwi, awaryjnego powiadamiana maszynisty/personelu (wzywania pomocy) oraz hamulca bezpieczeństwa pasażera) oraz pulpit maszynisty, a także kable i sieciowe urządzenia aktywne wykorzystywane do sterowania tymi systemami/podsystemami/ komponentami przez maszynistę mają zapewnione zasilanie w przypadku odłączenia głównego źródła zasilania pozwalające na dalszą pracę w normalnym trybie przez minimum 2 godziny? TAK = 2, NIE = 1 **3.** Czy system monitoringu wizyjnego ma zapewnione zasilanie w przypadku odłączenia głównego źródła zasilania pozwalające na dalszą pracę przez minimum 30 minut oraz zachowanie zapisów zarówno sprzed utraty głównego źródła zasilania jak i z kolejnych minimum 30 minut? TAK = 1, NIE = 0	Iloczyn odpowiedzi: 0 lub 1 lub 2 lub 4
RMF-14.6 – aktywna kopia oprogramowania układowego (firmwaru) **1.** Czy dostępna jest kopia oprogramowania układowego (firmwaru) systemów/ podsystemów/komponentów z oprogramowaniem, które sterują systemami hamowania, sterowania drzwiami i wysuwnymi stopniami, wentylacją, wykrywaniem i gaszeniem pożaru oraz informacją pasażerską (minimum głosową) i systemami wspierającymi bezpieczeństwo pasażerów (awaryjnego otwierania drzwi, awaryjnego powiadamiana maszynisty/personelu (wzywania pomocy) oraz hamulca bezpieczeństwa pasażera) oraz system wykrywania ingerencji w to oprogramowanie układowe (firmware) oparty np. na funkcjach haszujących, który wykrywa zmiany oprogramowania układowego (firmwaru) i w przypadku wykrycia zmiany oprogramowania powiadomi maszynistę (względnie system ATS w przypadku taboru autonomicznego) i podmieni oprogramowanie układowe (firmware) po uzyskaniu zgody maszynisty/operatora systemu ATS? TAK = 2, NIE = 1	Odpowiedź: 1 lub 2
Zbiorcza wartość referencyjna dla grupy RMF-G14 iloczyn wartości referencyjnych RMF-14.1 ÷ RMF-14.6	0 lub 1 lub 2 lub 4 lub 8

--- --- ---

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 taboru innych pytań różnicujących. Zastosowanie innego pytania różnicującego wymaga każdorazowo uzyskania formalnej zgody zamawiającego . 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.

4.1.6. 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 „8”. Mogą one jednakże przyjmować wyłącznie wartości „0”, „1”, „2”, „4” i „8”. Określone w taki sposób skumulowane wartości referencyjne mogą być przedstawiane w postaci wektorowej jako:

$$[bezpieczeństwo\,, ochrona\,, cyberbezpieczeństwo] \tag{4.1}$$

czyli

$$[SF, SC, CS] \tag{4.2}$$

gdzie:
SF – skumulowana wartość referencyjna dla bezpieczeństwa,
SC – skumulowana wartość referencyjna dla ochrony,
CS – skumulowana (zbiorcza) wartość referencyjna dla cyberbezpieczeństwa.

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

$$[G01 \times G02 \times G03 \times G04\,,\ G06 \times G07 \times G08 \times G09\,, G10] \tag{4.3}$$

Dla systemów, w których pociągi zdolne są do poruszania się bez maszynistów, z wykorzystaniem systemów klasy ATO oraz wymianą danych z systemami klasy ATS, wektor przyjmuje postać:

$$[G01 \times G02 \times G03 \times G04 \times G05\,,\ G06 \times G07 \times G08 \times G09\,, G10] \tag{4.4}$$

W obu przypadkach (4.3) i (4.4) maksymalne poziomy osiągamy dla wektora (4.2):

$$[8, 8, 8] \tag{4.5}$$

Dla nowego taboru pasażerskiego 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.

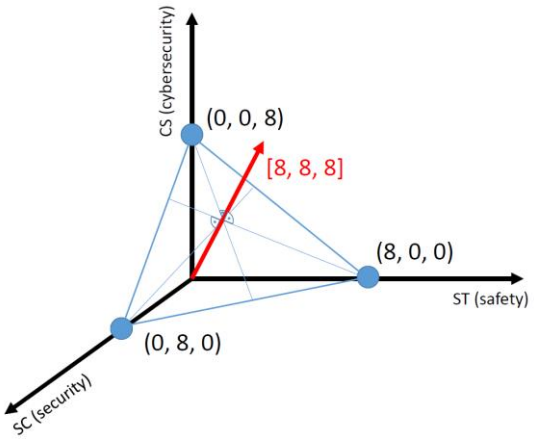
Wektorowa reprezentacja skumulowanych wartości (4.3) i (4.4) pozwala na szacunkowe określanie poziomu spójności funkcjonalnej skumulowanych wartości referencyjnych bezpieczeństwa i ochrony oraz skumulowanej (zbiorczej) wartości referencyjnej cyberbezpieczeństwa. Jeśli wartości referencyjne są takie same, 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 (4.5) 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 (4.3) lub (4.4).

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

$$\Pi_{odn} = \begin{matrix} 8 & 0 & 0 \\ 0 & 8 & 0 \\ 0 & 0 & 8 \end{matrix} \tag{4.6}$$

w której wiersze reprezentują punkty, a kolumny ich współrzędne w przestrzeni trójwymiarowej i dla której wektor (4.5) jest wektorem normalnym, co pokazano na Rysunku 6.



Rysunek 6 Wektor normalny do płaszczyzny odniesienia

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

$$FIL_{SS\&C} = \sin \measuredangle \left(\begin{matrix} 8 & 0 & 0 \\ 0 & 8 & 0 \\ 0 & 0 & 8 \end{matrix}, [\, SF, SC, CS \,] \right) \quad \left| \begin{matrix} SF \neq 0 \\ SC \neq 0 \\ CS \neq 0 \end{matrix} \right. \tag{4.7}$$

gdzie:

$FIL_{SS\&C}$ – 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*).

4.1.6.1. Określanie wartości FIL dla poziomów SF, SC, CS wyrażonych w postaci wartości całkowitych

Wektor [*SF, SC, CS*] jest uporządkowanym zbiorem, natomiast zbiorami złożonymi z elementów zbiorów zajmuje się kombinatoryka definiująca permutacje z i bez powtórzeń oraz kombinacje z i bez powtórzeń. W przypadku wektora [*SF, SC, CS*] punktem zaczepienia wektora (podstawą) jest zawsze punkt (0, 0, 0), natomiast punktem reprezentującym koniec wektora (głowę) jest punkt (*SF, SC, CS*). Mamy więc do czynienia z trójelementowym uporządkowanym zbiorem, w którym każdy z elementów może przyjmować dowolną wartość ze zbioru {0, 1, 2, 4, 8}. Przyjęcie przez dowolną współrzędną wektora [*SF, SC, CS*] wartości {0} dyskwalifikuje rozwiązanie techniczne ze względu na brak zapewnienia przynajmniej jednej funkcjonalności wymaganej z punktu widzenia bezpieczeństwa, ochrony lub cyberbezpieczeństwa. Wartości *FIL* oblicza się więc tylko wówczas, gdy współrzędne końca wektora (głowy) przyjmują wartości ze zbioru {1, 2, 4, 8}. Mamy więc do czynienia ze zbiorem trój elementowym, w którym istotna jest kolejność elementów, a każdy element może przyjmować cztery różne wartości.

Liczba k-elementowych kombinacji z powtórzeniami ze zbioru n-elementowego wyraża się wzorem:

$$L = \frac{(k+n-1)!}{k!\,(n-1)} \tag{4.8}$$

Przy czym *L* uwzględnia możliwość wielokrotnego występowania tej samej wartości ze zbioru *n*-elementowego, ale nie kolejność ich występowania w *k*-elementowym wektorze.

$$L = \frac{(3+4-1)!}{3!\,(4-1)!} = \frac{1*2*3*4*5*6}{1*2*3*1*2*3} = \frac{4*5*6}{2*3} = 20 \tag{4.9}$$

Musimy więc zidentyfikować 20 kombinacji, przy czym w zależności od zróżnicowania elementów pojedynczej kombinacji odpowiadać będą jeden, trzy lub sześć wektorów. Jednocześnie zauważyć należy, że spójność funkcjonalna bezpieczeństwa, ochrony i cyberbezpieczeństwa nie będzie zależna od indywidualnego wektora a od kombinacji ponieważ wszystkie trzy czynniki potraktowano w ten sam sposób uznając je za równie ważne. Podsumowanie możliwych wartości FIL przedstawiono w tabeli poniżej.

Tablica 4.1. Wartości FIL dla wartości całkowitych poziomów SF, SC, CS

lp.	Kombinacja	Wektory	wartość FIL
1.	{1, 1, 1}	[1, 1, 1]	1
2.	{1, 1, 2}	[1, 1, 2], [1, 2, 1], [2, 1, 1]	0,94281
3.	{1, 1, 4}	[1, 1, 4], [1, 4, 1], [4, 1, 1]	0,81650
4.	{1, 1, 8}	[1, 1, 8], [1, 8, 1], [8, 1, 1]	0,79045
5.	{1, 2, 2}	[1, 2, 2], [2, 1, 2], [1, 2, 2]	0,96225
6.	{1, 2, 4}	[1, 4, 2], [1, 2, 4], [2, 1, 4] [4, 1, 2], [2, 4, 1], [4, 2, 1]	0,88192
7.	{1, 2, 8}	[1, 8, 2], [1, 2, 8], [2, 1, 8] [8, 1, 2], [2, 8, 1], [8, 2, 1]	0,76455
8.	{1, 4, 4}	[1, 4, 4], [4, 1, 4], [4, 4, 1]	0,90453
9.	{1, 4, 8}	[1, 4, 8], [1, 8, 4], [8, 1, 4] [4, 1, 8], [8, 4, 1], [4, 8, 1]	0,83395
10.	{1, 8, 8}	[1, 8, 8], [8, 1, 8], [8, 8, 1]	0,86416
11.	{2, 2, 2}	[2, 2, 2]	1
12.	{2, 2, 4}	[2, 2, 4], [2, 4, 2], [4, 2, 2]	0,94281
13.	{2, 2, 8}	[2, 2, 8], [2, 8, 2], [8, 2, 2]	0,81650
14.	{2, 4, 4}	[4, 4, 2], [4, 2, 4], [2, 4, 4]	0,96225
15.	{2, 4, 8}	[2, 4, 8], [4, 2, 4], [2, 4, 4]	0,88192
16.	{2, 8, 8}	[8, 8, 2], [8, 2, 8], [2, 8, 8]	0,90453
17.	{4, 4, 4}	[4, 4, 4]	1
18.	{4, 4, 8}	[4, 4, 8], [4, 8, 4], [8, 4, 4]	0,94281
19.	{4, 8, 8}	[8, 8, 4], [8, 4, 8], [4, 8, 8]	0,96225
20.	{8, 8, 8}	[8, 8, 8]	1

Powyższa tabele przedstawia wartości FIL dla wartości całkowitych poziomów SF, SC, CS. Jednak odpowiedzi na pytania różnicujące nie zawsze są w pełni oczywiste i mogą być częściowo twierdzące.

4.1.6.2. Określanie poziomów SF, SC, CS wartościami z przedziału otwartego (1, 2)

Opieranie się na w pełni jednoznacznych odpowiedziach na pytania różnicujące nie zawsze jest możliwe i potencjalnie może prowadzić do nieuwzględniania w ocenie istotnych zastosowanych zabezpieczeń oraz do sugerowania stosowania zabezpieczeń także tam, gdzie w ocenie producenta nie są one zasadne. Z tego względu dla pytań różnicujących zasadne i możliwe jest zastosowanie wartości z przedziału otwartego (1, 2).

Określanie takich wartości wymaga uwzględniania skali zabezpieczenia i/lub skali zastosowania zabezpieczenia, któremu przypisano pytanie różnicujące. Zarówno skala zabezpieczenia jak i skala zastosowania mogą być mniejsze niż 100%. Odpowiedzi na pytanie różnicujące należy przypisać wartość sumy 1 plus procent zabezpieczenia lub 1 plus procent zastosowania lub jeśli zarówno poziom zabezpieczenia jak i skala zastosowania nie są pełne w świetle pytania różnicującego wartość sumy 1 plus iloczyn skali zabezpieczenia i skali zastosowania.

Zgoda na korzystanie z wartości ułamkowych powinna być potwierdzona przez podmiot zamawiający tabor. Natomiast przyjęte wartości powinny być dobrze uzasadnione jako że podlegają weryfikacji w ramach oceny, o którem mowa w rozdziale 4.2.

4.1.6.3. Określanie wartości FIL dla poziomów SF, SC, CS wyrażonych w postaci wartości z przedziału otwartego (1, 2)

Proponuje się, aby określanie wartości sinusa kąta pomiędzy wektorem i płaszczyzną odniesienia w przypadku poziomów SF, SC, CS wyrażonych w postaci wartości z przedziału otwartego (1, 2) opierało się na wartości kąta pomiędzy wektorem (x.x) a wektorem normalnym do płaszczyzny odniesienia.
Znając wektor kierunkowy prostej $\vec{v} =$ [A, B, C] oraz wektor normalny płaszczyzny odniesienia $\vec{u} =$ [X, Y, Z], można wyliczyć kąt pomiędzy prostą i wektorem wykorzystując własności iloczynu wektorowego tych wektorów:

$$\measuredangle(\vec{v},\vec{u}) = arccos\frac{AX + BY + CZ}{\sqrt{A^2 + B^2 + C^2} * \sqrt{X^2 + Y^2 + Z^2}} \quad (4.10)$$

W naszym przypadku wektor kierunkowy to wektor [SF, SC, CS]. Natomiast wektor normalny do płaszczyzny odniesienia określić można w naszym przypadku np. jako [8, 8, 8]. Tak więc kąt pomiędzy tymi wektorami wyrażony w radianach wynosi:

$$\measuredangle(\vec{v},\vec{u}) = arccos\frac{(SF * 8) + (SC * 8) + (CS * 8)}{\sqrt{SF^2 + SC^2 + CS^2} * \sqrt{192}} \quad (4.11)$$

Kąt pomiędzy wektorem [SF, SC, CS] a płaszczyzną odniesienia to $\frac{\pi}{2} - \measuredangle(\vec{v},\vec{u})$, ponieważ kąt między wektorem normalnym do płaszczyzny i płaszczyzną wynosi 90° czyli dokładnie $\frac{\pi}{2}$ w radianach. Po podstawieniu do wzoru (x.zz) otrzymujemy wzór na określanie wartości FIL dla poziomów SF, SC, CS wyrażonych w postaci wartości z przedziału otwartego (1, 2).

$$FIL_{SF,SC,CS} = \sin\left(\frac{\pi}{2} - \left(arccos\frac{(SF * 8) + (SC * 8) + (CS * 8)}{\sqrt{SF^2 + SC^2 + CS^2} * 8\sqrt{3}}\right)\right) \quad \begin{vmatrix} SF \neq 0 \\ SC \neq 0 \\ CS \neq 0 \end{vmatrix} \quad (4.12)$$

Powyższy wzór pozwala na obliczenie wartości *FIL* z wykorzystaniem kalkulatorów naukowych lub arkuszy kalkulacyjnych z zachowaniem zarówno zgodności z wzorem ogólnym (4.7) jak i uwzględnianiem częściowo pozytywnych odpowiedzi na pytania różnicujące wykorzystywane dla potrzeb określania wartości poziomów bezpieczeństwa, ochrony i cyberbezpieczeństwa przedstawianych łącznie w postaci wektora (4.2).

4.1.6.4. Określanie wymagań odnośnie poziomów SF, SC, CS i ich spójności przez użytkowników taboru – indeks bezpieczeństwa taboru pasażerskiego

Zdefiniowanie przez przyszłego użytkownika pasażerskiego taboru kolejowego wymaganych wartości poziomów SF, S.C. i CS oraz wymaganej wartości ich spójności może opierać się zarówno na:

- bezpośrednim wskazaniu minimalnych wartości poziomów SF, SC i CS oraz spójności FIL,
- wskazaniu minimalnej wartości poziomów SF, SC i CS wraz ze wskazaniem maksymalnego dopuszczalnego zróżnicowania SF, SC i CS oraz wskazaniu minimalnej spójności FIL, lub
- wskazaniu średniej wartości poziomów SF, SC i CS wraz ze wskazaniem maksymalnego dopuszczalnego zróżnicowania SF, SC i CS oraz wskazaniu minimalnej spójności FIL, lub
- wskazaniu indeksu cyfrowego bezpieczeństwa taboru pasażerskiego (PTDSI – passenger train digital safety index) zgodne z poniższą tablicą.

Tablica 2. Indeks cyfrowego bezpieczeństwa taboru pasażerskiego (PTDSI)

PTDSI				
spójność podstawowa (PTDSI basic integrity) (**FIL BI**)	SF ≥ 1	SC ≥ 1	CS ≥ 1	FIL ≥ 0,7
PTDSI 1 (**FIL index 1**)	SF ≥ 2	SC ≥ 2	CS ≥ 2	FIL ≥ 0,8
PTDSI 2 (**FIL index 2**)	SF ≥ 4	SC ≥ 4	CS ≥ 4	FIL ≥ 0,9
PTDSI 3 (**FIL index 3**)	SF ≥ 6	SC ≥ 6	CS ≥ 6	FIL ≥ 0,9
PTDSI 4 (**FIL index 4**)	SF = 8	SC = 8	CS = 8	FIL = 1

Przykładowo przyszły użytkownik pasażerskiego taboru kolejowego może wymagać od producenta, aby dla oferowanego taboru minimalna wartość poziomów SF, SC, CS wynosiła 2, a spójność FIL wynosiła minimum 0,88, lub aby średnia wartość poziomów SF, SC, CS wynosiła 2, a spójność FIL wynosiła

minimum 0,85. Zaleca się jednakże definiowanie wymagań poprzez wskazanie wartości indeksu cyfrowego bezpieczeństwa taboru pasażerskiego (PTDSI).

4.1.7. 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, oraz wynikowe poziomy bezpieczeństwa, ochrony i cyberbezpieczeństwa oraz wynikowy poziom spójności bezpieczeństwa, ochrony i cyberbezpieczeństwa, oraz wynikową wartość indeksu cyfrowego bezpieczeństwa dla analizowanego taboru pasażerskiego.

4.2. Zasady weryfikowania spójności bezpieczeństwa, ochrony i cyberbezpieczeństwa pasażerskiego taboru kolejowego

Weryfikacja '**dowodu spójności bezpieczeństwa, ochrony i cyberbezpieczeństwa**' powinna być przeprowadzona przez **kompetentną niezależną jednostkę inspekcyjną** posiadającą akredytację Polskiego Centrum Akredytacji dla jednostki oceniającej analizy i wyceny ryzyka realizowane zgodnie z rozporządzeniem w sprawie oceny i wyceny ryzyka [6, 7] dla pięciu podsystemów strukturalnych – podsystemów „Infrastruktura", „Energia", „Sterowanie – urządzenia przytorowe" oraz „Tabor" i „Sterowanie – urządzenia pokładowe". Dodatkowo jednostka w zakresie akredytacji powinna posiadać kompetencje do przeprowadzenia oceny bezpiecznej integracji w ww. obszarach.

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 [6, 7], wytycznych Polskiego Centrum Akredytacji, Urzędu Transportu Kolejowego 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 budowy taboru pasażerskiego 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 zamawiającego, , 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 nowego taboru pasażerskiego.

Rozdział 3 powinien zawierać ocenę analizy zabezpieczeń przed cyberzagrożeniami włącznie z analizą pełnego stosowania zasad systemu zarządzania bezpieczeństwem informacji przyjętych przez przewoźnika kolejowego zgodnie z normą PN-EN ISO/IEC 27001 [8].

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 zamawiającego. W tym celu **wykonawca** powinien zwrócić się do wewnętrznego zespołu odpowiedzialnego za bezpieczeństwo u zamawiającego.

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

5. Cyberbezpieczeństwo pasażerskiego taboru kolejowego w eksploatacji

Eksploatacja i utrzymanie, także w odniesieniu do zastosowanych w kolejowym taborze pasażerskim rozwiązań cyfrowych powinny być realizowane zgodnie z planem eksploatacji i utrzymania. Plan taki opracowywany jest przez producenta taboru (zamykany w fazie 10 cyklu życia zgodnie z PN EN 50126-1:2018-02) i przekazywany użytkownikowi wraz z pierwszym egzemplarzem danego typu taboru. Zgodnie z zapisami PN EN 50126-1:2018-02:

Zaleca się, aby plany eksploatacji i utrzymania obejmowały:

1) *wyjaśnienie statusu eksploatacyjnego: Zaleca się zdefiniowanie warunków, które istnieją w każdym systemie/podsystemie/sprzęcie, tak aby zapewnić personelowi eksploatacyjnemu i utrzymaniowemu wystarczającą wiedzę w następujących sytuacjach:*
   a) *rozruch: zaleca się opisanie warunków rozruchu systemu, podsystemu lub sprzętu podczas pierwszego załączenia zasilania oraz po wyłączeniu z powodu przerwy w zasilaniu lub z innej przyczyny;*
   b) *normalna praca: należy określić warunki podczas normalnej pracy po pomyślnym zakończeniu inicjalizacji systemu/podsystemu/sprzętu;*
   c) *przełączanie: jeżeli system/podsystem lub sprzęt, na którym jest on skonfigurowany, ma możliwość przełączania się do trybu zimnej lub gorącej rezerwy systemu/podsystemu, to zaleca się aby warunki określone w pozycjach a) i b) były określone także dla takich przełączeń. Reakcja systemu/podsystemu lub sprzętu na przełączanie uszkodzonych modułów również powinna być jasno określona;*
   d) *wyłączenie: gdy system/podsystem lub sprzęt zostaną celowo wyłączone z powodu zmiany konfiguracji lub likwidacji lub wyłączone nieintencjonalnie z powodu awarii zasilania, to należy określić wszystkie odpowiednie warunki.*
2) *zaleca się określenie kwestii utrzymania w odniesieniu do:*
   a) *prac podejmowanych w systemie na miejscu oraz powtarzalnych prac realizowanych w dedykowanych warsztatach utrzymaniowych;*
   b) *napraw lub odnów systemów, podsystemów lub sprzętu, które nie są realizowane na miejscu lub są realizowane w warsztatach niesklasyfikowanych jako dedykowane do powtarzalnych prac utrzymaniowych, np. remontów generalnych, które są realizowane przez klienta i producenta;*
   c) *utrzymania prewencyjnego;*
   d) *utrzymania korekcyjnego;*
   e) *środków wspomagania utrzymania: zaleca się określenie dla każdego poziomu utrzymania środki wspomagania utrzymania dostępnych dla personelu;*
3) *analizę czynników ludzkich i wymagań kompetencyjnych w zakresie utrzymania, które mogą mieć wpływ na ciągłe osiąganie wymaganej wydajności RAMS;*
4) *analizę czynników ludzkich i wymagań kompetencyjnych w eksploatacji, które mogą mieć wpływ na ciągłe osiąganie wymaganej wydajności RAMS.*

Należy wdrożyć procedury eksploatacyjne i utrzymaniowe, w szczególności w odniesieniu do wydajności systemu i kwestii kosztów cyklu życia. Wymaga to rozpatrzenia wyrobu, systemu lub procesu w jego środowisku eksploatacyjnym, np. z uwzględnieniem stosowania zewnętrznych środków zmniejszających ryzyko.

Zgodność z wymaganiami RAMS na tym etapie cyklu życia powinna być zapewniona dzięki:

a) *regularnym przeglądom i aktualizacjom planów i procedur eksploatacji i utrzymania;*
b) *zgodności z planami i procedurami eksploatacji;*
c) *zgodności z planami i procedurami utrzymania;*
d) *regularnym przeglądom dokumentacji systemu związanej ze szkoleniami;*
e) *regularnym przeglądom i aktualizacjom (w stosownych przypadkach) eksploatacyjnego rejestru zagrożeń;*
f) *zapewnieniu zgodności z warunkami stosowania związanymi z bezpieczeństwem (SRAC);*
g) *badaniu i obsłudze niebezpiecznych wydarzeń i wypadków oraz zapewnianiu szybkiego wykrywania niezdatności;*

h) w przypadku systemów poddawanych modyfikacji, określaniu i wdrażaniu działań łagodzących, w stosownych przypadkach, w celu zapewnienia ogólnej integralności systemu do czasu zakończenia modyfikacji lub zbadania i usunięcia zgłoszonych problemów;

i) zgodności z umowami o wsparciu, w tym logistyką, częściami zamiennymi, naprawami, narzędziami, kalibracjami i środkami jakościowymi w celu zapobiegania uszkodzeniom lub wykrywania uszkodzeń występujących podczas magazynowania i transportu;

j) utrzymywaniu systemu raportowania uszkodzeń oraz planowania działań naprawczych (FRACAS).

UWAGA 1 Eksploatacyjny rejestr zagrożeń opiera się na ewidencji zagrożeń uzyskanej z rejestru zagrożeń z 10. fazy cyklu życia.

W odniesieniu do powyższego zapisu normy zwrócić należy uwagę na właściwą interpretację powyżej przywołanych zapisów dotyczących eksploatacji i utrzymania taboru w odniesieniu do jego cyfrowego wyposażenia przy uwzględnieniu zarówno elementów sprzętowych jak i oprogramowania.

Przekazany użytkownikowi plan eksploatacji i utrzymania powinien być dokumentem uzupełnianym i aktualizowanym przez użytkownika taboru kolejowego. Zgodnie z zapisami PN EN 50126-1:2018-02:

Przeglądy i aktualizacje planu eksploatacji i utrzymania powinny obejmować kwestie podniesione i rozwiązane podczas początkowej fazy eksploatacji i utrzymania oraz na odpowiednich etapach później.

Należy wdrożyć proces w celu:

a) pozyskiwania danych o wydajności RAMS;

b) rejestracji danych dotyczących wydajności RAMS oraz związanych z nimi analiz i wycen, jeśli mają zastosowanie, np. za pomocą FRACAS.

Przez cały okres eksploatacji systemu należy rejestrować wzorzec systemu i śledzić jego zmiany pod nadzorem systemu zarządzania konfiguracją.

UWAGA 2 Ma to szczególne znaczenie w przypadku wykrycia krytycznych niezdatności i konieczności ich usunięcia w więcej niż jednej instalacji. Producenci i personel utrzymaniowy mogą być zmuszeni do wdrożenia komplementarnych ustaleń w zakresie zarządzania konfiguracją. Dlatego producenci powinni mieć możliwość sprawdzenia wzorców systemów dostarczanych poszczególnym klientom, a personel utrzymaniowy poszczególnych klientów sprawdzenia lokalizacji poszczególnych elementów.

Wymaga to wdrożenia i wykorzystywania przez użytkownika taboru nie tylko planu eksploatacji i utrzymania, ale także systemu zarządzania konfiguracją taboru, w tym w szczególności konfiguracją w odniesieniu do cyfrowego wyposażenia taboru z uwzględnieniem zarówno elementów sprzętowych jak i oprogramowania.

Właściwe prowadzenie nadzoru nad eksploatacją oraz prac utrzymaniowych wymaga wdrożenia i utrzymywania systemu FRACAS (systemu raportowania i analizy uszkodzeń oraz działań korekcyjnych). Zgodnie z zapisami PN EN 50126-1:2018-02:

Proces FRACAS jest wymagany do ciągłego zapewniania kierownikowi ds. bezpieczeństwa eksploatacji, projektantowi, producentowi, kierownikowi eksploatacji i kierownikowi utrzymania informacji zwrotnej o wszelkich uszkodzeniach i wadach (oraz ich możliwych przyczynach) wykrytych podczas eksploatacji. Uszkodzenia mogą mieć różne przyczyny, w tym uszkodzenia komponentów, błędy eksploatacji, utrzymania i inne błędy. Konieczne jest zatem, aby proces zgłaszania był przejrzysty i logiczny oraz aby istniało wspólne forum dla wszystkich interesariuszy dla uzgadniania najbardziej prawdopodobnych źródeł uszkodzeń, a tym samym właściwych działań dochodzeniowych i naprawczych.

UWAGA 3

1) *Występować może konieczność przechowywania komplementarnych zapisków FRACAS przez różne podmioty. Podmioty odpowiedzialne za utrzymanie mogą dysponować ogólnym FRACAS, który obejmuje wiele różnych rodzajów systemów, za które są odpowiedzialni. Natomiast producenci mogą dysponować FRACAS, który obejmuje systemy dostarczane bardzo różnym klientom. Producenci mogą diagnozować te uszkodzenia komponentów, które nie są dostępne dla personelu utrzymaniowego.*

2) *Powiązania z wypadkami, zagrożeniami i przyczynami powinny być spójne z dowodami bezpieczeństwa oraz innymi narzędziami i procesami monitorowania wydajności. Pomoże to odpowiednim organizacjom w porównywaniu wyzwań i identyfikowaniu trendów.*

FRACAS należy utrzymywać przez cały cykl eksploatacji i utrzymania. Aby zapewnić rozwiązanie problemów priorytetowych, zaleca się kategoryzowanie uszkodzeń i wad zarówno ze względu na bezpieczeństwo, jak i niezawodność według różnych poziomów dotkliwości/krytyczności. FRACAS powinien zawierać co najmniej informacje o uszkodzeniach i wadach zidentyfikowanych podczas eksploatacji i utrzymania. Informacje te powinny obejmować:

a) czas uszkodzenia;

b) przyczynę uszkodzenia;

c) szczegółowy opis uszkodzenia;

d) podjęte działania naprawcze;

e) ranking bezpieczeństwa dla uszkodzenia;

f) kiedy i jak wykryto uszkodzenia i wady (np. podczas pracy lub podczas planowego utrzymania);

g) skutki uszkodzeń i wad do poziomu systemu kolejowego.

Zapisy FRACAS powinny podlegać okresowym przeglądom w celu ustalenia, czy konieczna jest jakakolwiek poprawa następujących elementów:

h) procedur i instrukcji eksploatacji i utrzymania;

i) dokumentacji systemu w zakresie szkolenia;

j) eksploatacyjnego rejestru zagrożeń;

k) projektu systemu;

l) czynników ludzkich związanych z eksploatacją i utrzymaniem.

Po zaproponowaniu zmian należy przeprowadzić analizę wpływu obejmującą wszystkie żądania zmian. Analiza powinna obejmować przegląd wpływu na:

m) wydajność systemu/podsystemu lub sprzętu w zakresie bezpieczeństwa eksploatacyjnego /funkcjonalnego;

n) interfejsy systemów/podsystemów/sprzętu;

o) wydajność eksploatacyjną/funkcjonalną sąsiedniego systemu/podsystemu lub sprzętu;

p) prace instalacyjne związane z modyfikacją, z uwzględnieniem sąsiednich systemów/podsystemów i sprzętu, które mogą być dotknięte uszkodzeniami systematycznymi.

W wyniku analizy wpływu powinna zostać podjęta decyzja, które części cyklu życia bezpieczeństwa zostaną powtórzone w celu modyfikacji. Cała odpowiednia dokumentacja dla dotkniętych etapów cyklu życia powinna zostać zaktualizowana, z zachowaniem głębokości i jakości takiej samej, jaką ma oryginalna dokumentacja sporządzona podczas rozwoju systemu. Szczegóły i wyniki modyfikacji, analizy ryzyka i badania powinny być ujęte w dowodzie bezpieczeństwa.

Wszystkie zmiany oraz system/podsystem lub sprzęt zidentyfikowane jako zagrożone powinny być badane pod kątem poprawnego działania po zakończeniu zmiany.

Dla każdego zidentyfikowanego zalecenia powinna zostać podjęta decyzja, czy zalecenie powinno zostać zrealizowane, czy nie. Decyzje te powinny być uzasadnione i odnotowane.

W odniesieniu do powyższego zapisu normy zwrócić należy uwagę na właściwą interpretację powyżej przywołanych zapisów dotyczących eksploatacji i utrzymania taboru w odniesieniu do jego cyfrowego wyposażenia przy uwzględnieniu zarówno elementów sprzętowych jak i oprogramowania.

Zaleca się, aby zapisy rozdziału 5. Wytycznych dotyczących cyberbezpieczeństwa pasażerskiego taboru kolejowego były stosowane także do pasażerskiego taboru kolejowego, który został przekazany do eksploatacji przed przyjęciem wytycznych względnie z ich pominięciem, przy czym:

- Z inicjatywą objęcia danego typu taboru właściwymi systemami/dokumentami – planem utrzymania i eksploatacji, systemem zarządzania konfiguracją taboru, oraz systemem FRACAS (raportowania i analizy uszkodzeń oraz działań korekcyjnych) może wystąpić zarówno producent jak i użytkownik danego typu pasażerskiego taboru kolejowego.
- Niezależnie od tego, która ze stron wystąpi z inicjatywą objęcia danego typu pasażerskiego taboru kolejowego tymi systemami obie strony powinny współpracować przez opracowaniu i wdrożeniu stosownych systemów/dokumentów.
- Producent danego typu pasażerskiego taboru kolejowego powinien być upoważniony do wykorzystania opracowanych systemów/dokumentów także dla taboru tego samego typu wykorzystywanego przez innych użytkowników oraz dla pasażerskiego taboru kolejowego, który jest przez niego produkowany lub jest produkowany w oparciu o udostępnioną przez niego licencję a wykorzystuje tego samego typu lub pokrewne rozwiązania sprzętowe i/lub oprogramowanie.
- Użytkownik danego typu taboru zaangażowany w opracowanie systemów/dokumentów powinien rozpocząć ich stosowanie w procesie utrzymania i eksploatacji niezwłocznie po zamknięciu prac nad tymi systemami/dokumentami.
- Użytkownik danego typu taboru niezaangażowany w opracowanie systemów/dokumentów powinien rozpocząć ich stosowanie w procesie utrzymania i eksploatacji niezwłocznie po ich udostępnieniu przez producenta danego typu taboru.
- Każdy użytkownik danego typu pasażerskiego taboru kolejowego ma prawo do wprowadzania zmian w przedmiotowych systemach/dokumentach w ramach ich doskonalenia oraz dostosowywania do warunków eksploatacji i utrzymania jakie mają zastosowanie do taboru danego użytkownika.

6. Modyfikowanie taboru a cyberbezpieczeństwo

Wprowadzanie zmian w taborze wymaga stosowania analizy i wyceny ryzyka w sposób określony w rozporządzeniu w sprawie oceny i wyceny ryzyka [6, 7] do identyfikacji i potwierdzania eliminacji wszelkich nieakceptowalnych ryzyk oraz identyfikacji i mitygacji wszelkich ryzyk tolerowalnych wymagających nadzoru przewoźnika i/lub podmiotu odpowiedzialnego za utrzymanie podczas eksploatacji i utrzymania pasażerskiego taboru kolejowego.

Wprowadzanie zmian w taborze może wpływać między innymi na jego cyberbezpieczeństwo, dlatego analiza i wycena ryzyka, o której mowa powyżej powinna obejmować ewentualne zmiany w ramach systemów/podsystemów/komponentów z oprogramowaniem.

Wprowadzaniu zmian towarzyszyć powinna rewizja planu utrzymania i eksploatacji, systemu zarządzania konfiguracją taboru, oraz systemu FRACAS (raportowania i analizy uszkodzeń oraz działań korekcyjnych), lub ich opracowanie i wdrożenie.

Zaleca się, aby przy wprowadzaniu zmian w obrębie systemów/podsystemów/komponentów z oprogramowaniem oraz pokładowych i bezprzewodowych sieci wymiany danych, a także konfiguracji, w tym relacji pomiędzy systemami/podsystemami/komponentami i sieciami wymiany danych:

- zapewniane było wykorzystywanie pełnej dokumentacji komponentu cyfrowego,
- zachowywana była struktura pokładowych sieci wymiany danych, w tym zasady separacji podsieci wykorzystywanych dla potrzeb różnych funkcji,
- zmiany oprogramowania bazowały na kodach źródłowych a nie na modyfikowaniu wynikowego oprogramowania z wykorzystaniem narzędzi typu AI czy reverse engineering,
- uwzględniane były aspekty wskazane w kartach kontrolnych cyberbezpieczeństwa dla indywidualnych systemów/podsystemów/komponentów (G10÷G13) oraz karcie zbiorczej cyberbezpieczeństwa (G14) niniejszych wytycznych,
- opracowany (lub uaktualniony) oraz oceniony został **dowód spójności bezpieczeństwa, ochrony i cyberbezpieczeństwa**.

7. Dokumenty referencyjne

Dla potrzeb opracowania „Wytycznych dotyczących cyberbezpieczeństwa pasażerskiego taboru kolejowego” wykorzystano następujące dokumenty referencyjne:

dokumenty prawne UE:

- dokumenty formalne Parlamentu Europejskiego i Rady UE:
  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)
  3. Dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2555 z dnia 14 grudnia 2022 r. w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii, zmieniająca rozporządzenie (UE) nr 910/2014 i dyrektywę (UE) 2018/1972 oraz uchylająca dyrektywę (UE) 2016/1148 (dyrektywa NIS 2)
  4. Dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2557 z dnia 14 grudnia 2022 r. w sprawie odporności podmiotów krytycznych i uchylająca dyrektywę Rady 2008/114/WE
  5. Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2021/782 z dnia 29 kwietnia 2021 r. dotyczące praw i obowiązków pasażerów w ruchu kolejowym
- dokumenty formalne Komisji Europejskiej:
  6. 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)
  7. 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)

powołane normy i dokumenty normatywne:

- normy europejskie przejęte przez CEN, CENELEC, ETSI
  8. PN-EN ISO/IEC 27001:2017-06 Technika informatyczna -- Techniki bezpieczeństwa -- Systemy zarządzania bezpieczeństwem informacji -- Wymagania
  9. PN-EN 50126-1:2018-02 Zastosowania kolejowe -- Specyfikowanie i wykazywanie niezawodności, dostępności, podatności utrzymaniowej i bezpieczeństwa (RAMS) -- Część 1: Proces ogólny RAMS
  10. PN-EN 50126-2:2018-02 Zastosowania kolejowe -- Specyfikowanie i wykazywanie niezawodności, dostępności, podatności utrzymaniowej i bezpieczeństwa (RAMS) -- Część 2: Sposoby podejścia do bezpieczeństwa
  11. PN-EN 50128:2011+A2:2020 Zastosowania kolejowe -- Systemy łączności, przetwarzania danych i sterowania ruchem -- Oprogramowanie kolejowych systemów sterowania i zabezpieczenia, oraz
      PN-EN 50657:2017-10 Zastosowania kolejowe -- Zastosowania taborowe -- Oprogramowanie na pokładzie taboru, które łącznie w roku 2023 zastępuje norma
      EN 50716:2023 Cross-functional Software Standard for Railways
  12. PN-EN 50129:2019-01 Zastosowania kolejowe -- Systemy łączności, przetwarzania danych i sterowania ruchem -- Elektroniczne systemy sterowania ruchem związane z bezpieczeństwem
  13. PN-EN 50159:2011 Zastosowania kolejowe -- Systemy łączności, sterowania ruchem i przetwarzania danych -- Łączność bezpieczna w systemach transmisyjnych
  14. Normy serii PN-EN ISO/IEC 62443 Bezpieczeństwo w systemach sterowania i automatyki przemysłowej

--- ---