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

# Wytyczne dotyczące cyberbezpieczeństwa pasażerskiego taboru kolejowego

**wersja 1.0, korekta A do wydania dwujęzycznego**

Warszawa, 25 lipca 2023 (korekta, 25 stycznia 2024)

**Polish Rail Transport Subsector**
**Information Sharing and Analysis Centre**
**„ISAC – Kolej”**

# Recommendations regarding railway passenger rolling stock cybersecurity

**version 1.0, revision A for bilingual edition**

Warsaw, 31 July 2023 (revision, 25 January 2024)

Wersjonowanie dokumentu:

| Wersja | Zmiany |
|---|---|
| 1.0 | Pierwsza kompletna wersja dokumentu<br>przyjęta przez ISAC-Kolej w dniu: 31 lipca 2023 r. |
| 1.0(A) | Korekta A dla potrzeb wydania dwujęzycznego<br>opracowana z zachowaniem podziału na strony, z poprawkami edycyjnymi dla zachowania pełnej spójności między wersją polską i angielską, z poprawieniem błędów na stronie 49. |
| --- | 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.

==========

Document data sheet:

| Version | Changes |
|---|---|
| 1.0 | First complete version of the document<br>accepted by ISAC-Kolej on the 31 July 2023 |
| 1.0(A) | Revision A for the bilingual edition<br>prepared keeping subdivision into pages, with editorial corrections for full consistency between the Polish and English versions, with correction of errors on page 49. |
| --- | <br>accepted by ISAC-Kolej on the …….. |

==========

It is declared that:

- In accordance with ISAC-Kolej decision, taken at the plenary meeting, which took place on the 31st July 2023, document “Recommendations regarding railway passenger rolling stock cybersecurity” will be handed-over to rolling stock manufacturers with suggestion to undertake attempts to apply the document to chosen types of passenger rolling stock in order to gain initial experience and formulate possible comments on recommendations;
- The intention of the authors of the document is not only to make it available to the industry and Polish railway undertakings and infrastructure managers; but also to
- Translate the document into English and submit it to the European Union Agency for Cybersecurity ENISA with permission for dissemination.

==========

## Spis treści:

strona

## Table of contents:

page

# 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

# 1. Introduction

In December 2022, the EU European Parliament and Council adopted the Directive on measures for a high common level of cybersecurity across the Union [3]. This document (NIS 2 Directive) defines requirements regarding paying attention to protection against cyberthreats for railway undertakings, among others. The previous directive (NIS Directive) [2] only required railway undertakings to take measures against cyberthreats if they already obtained appropriate administrative decision issued by the competent national authority. The NIS 2 Directive requires appropriate efforts from, inter alia, railway undertakings, with the exception of those who employ no more than 49 persons and at the same time have an annual turnover of less than 10 000,- euro. The NIS 2 Directive therefore imposes new transport cybersecurity obligations on almost all rail undertakings.

Independently of the change in European law, which has yet to be implemented into national law, the current international situation has resulted in an exponential increase in cyberthreats to transport in Poland from February 2022. Particularly vulnerable is railway transport as it is intensively utilised in support of military and diplomatic activities across Poland's eastern border.

Developed on the basis of the “Transport Cybersecurity Toolkit” and adopted by ISAC-Kolej in 2021 “Cybersecurity guidelines for the employees of the railway entities” have become insufficient, although ISAC-Kolej members are receiving, since 2022, by emails:

- daily country reports on malicious network traffic (recommendations on blocking specific IPs),
- weekly country reports on detected vulnerabilities in IT products (recommendations for system and software updates),
- bi-weekly ‘PKP Informatyka’ SOC newsletter on cybersecurity in railway transport,

and in cases when threats are detected:

- information on new phishing campaigns,
- information regarding registration of the domains that can be used for phishing attacks (recommendations to block malicious domains on the edge devices, to use appropriate anti-spam filters, to be vigilant when sending/receiving e-mails from employees),
- information on the detection of zero-day vulnerabilities, the possibility of their exploitation and the IoC (recommendations - various, depending on the type of vulnerability),
- information on phishing campaigns distributing malware and the IoC of the malicious campaign (recommendations - implementation of relevant rules on e-mail filtering devices),
- in case of detection - information about DDoS attacks, including possible attacks on websites and services (recommendations - anti-DDoS protection, monitoring of infrastructure, preparation for traffic limitations in case of escalation), as well as
- if necessary - useful information, e.g. on the activities of APT groups, Killnet, etc.

The NIS 2 Directive requires railway undertakings to identify and counter threats and report on cyberattacks and incidents. Although the NIS 2 Directive has not yet been implemented into national law, some railway undertakings, when preparing tenders for the purchase of rolling stock, have found it necessary to include cybersecurity requirements in the tender documentation due, among other things, to current cyber threats and the fact that the supply of rolling stock is scheduled after the day NIS 2 Directive start to be binding for them.

## 1.1. Regulations governing cybersecurity of the railway transport

All successive EU Railway Interoperability Directives since ones accepted in 1996 for high-speed railways and in 2001 for conventional railways define in Annex III essential requirements, including the essential requirement 'safety'. Part of the provisions defining the essential requirement 'safety' in the presently binding, being in force, Railway Interoperability Directive (EU) 2016/797 [1] apply to electronic

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 17 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.

and programmable solutions with regard to, inter alia, the provisions to guarantee safety at the adequate level also for specific degraded situations e.g. for control command and signalling systems, as well as suitable levels of integrity and dependability for the storage and transmission of the safety-related information, as an example within telematics applications. However, it has to be admitted, that requirements explicitly dedicated to cybersecurity are neither detailed in the framework of the Directive nor in the Technical Specifications for Interoperability adopted by European Commission Regulations supplementing the Railway Interoperability Directive.

The European Union Agency for Cybersecurity (ENISA) was established in 2004. Presently binding, being in force, Directive (EU) 2016/1148 concerning measures for a high common level of security of network and information systems across the Union (NIS Directive) [2], adopted in 2016, included in its scope, inter alia, the rail transport. This directive, in 2022, was replaced by Directive (EU) 2022/2555 on measures for a high common level of cybersecurity (NIS 2 Directive) [3], which, as mentioned in the introduction, imposes a number of obligations on railway undertakings to ensure an adequate level of cybersecurity. The NIS 2 Directive will replace the NIS Directive when implemented in the national law of the EU Member States, which in accordance with binding legal requirements shall take place by 17 October 2024 at the latest. In parallel, the European Parliament adopted Directive (EU) 2022/2557 on the resilience of critical entities [4], which recognises railway undertakings as critical entities required to conduct risk assessments covering all the relevant natural and man-made risks and to take necessary measures to minimise threats. The content of this directive does not explicitly refer to cybersecurity. The directive focuses specifically on physical protection and crisis management, which are complementary to cyberthreats, which cannot be ignored in risk analyses. The provisions of Directive 2022/2557 require, due to the link between physical security and cybersecurity of the critical entities, that the implementations of both Directives, 2022/2555 and 2022/2557, have to be coordinated.

Due to the subject of the recommendations, the Regulation (EU) 2021/782 on rail passengers' rights and obligations [5] shall not be omitted. In accordance with this regulation railway undertakings shall, in agreement with public authorities, infrastructure managers, and station managers, take adequate measures to ensure passengers’ personal security in railway stations and on trains and to manage risks. Thus, the railway undertakings shall take into account the cybersecurity not only of the digital systems affecting traffic safety, but also cybersecurity of the systems supporting passengers' personal security, e.g. passenger information systems, public address systems, assistance call systems.

## 1.2. Challenges regarding railway passenger rolling stock cybersecurity

In case of modern passenger rolling stock, both an adequate level of railway traffic safety, and an adequate level of transport security, ensuring in particular the personal security of the passengers, are provided with use of the digital solutions, which shall be adequately protected against cyberthreats. Appropriate protection means shall ensure high and at the same time similar level of protection in different areas, in order not to leave unprotected or clearly less protected areas that could be utilised for cyberattack. The required and optional protection measures against cyberattacks, taking into account the principle of equal protection against risks regarding traffic safety, transport security and cyberthreats, and the way they shall be documented and assessed for specific new types of passenger rolling stock are presented in Chapter 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.

In that chapter the principles for documenting and assessing the integrity of the safety, security and cybersecurity of the new passenger rolling stock are defined. The challenge for any new type of rolling stock is to select appropriate protection means and to implement them in the rolling stock, taking into account different risks arising from cyberthreats, including the possible use of unauthorised access to systems and/or equipment.

Long operational life of the passenger rolling stock, spanning over several decades, requires cyberthreats to be taken into account in the operation and maintenance phase of the lifecycle of the rolling stock, with particular consideration, on one side, of the risks associated with changes in the environment, such as the development of security breach tools, and, on the other side, of the risks associated with access by maintenance staff to all different implemented digital solutions that perform functions utilised for ensuring traffic safety, transport security and/or digital solutions' protection against cyberthreats. Suggestions in this respect are summarised and presented in Chapter 5. The challenge applies both to the rolling stock built and accepted in accordance with these recommendations and to the rolling stock already in operation and the one which will be put in service without taking into account these recommendations.

Maintaining high, and well balanced between different areas, level of protection regarding traffic safety, transport security and cyberthreats is even more challenging when modifications are introduced in existing rolling stock. This applies both to rolling stock designed and built in accordance with these recommendations and to existing rolling stock designed and built without direct consideration of these recommendations. Suggestions in this respect are summarised and presented in Chapter 6.

### 1.3. How cybersecurity shall be understood

"Security of network and information systems", in relation to networks and information systems including those utilised for the purpose of the railway transport, is defined in the Directive concerning measures for a high common level of security of network and information systems [2] as follows:

> *'security of network and information systems' means the ability of network and information systems to resist, at a given level of confidence, any action that compromises the availability, authenticity, integrity or confidentiality of stored or transmitted or processed data or the related services offered by, or accessible via, those network and information systems;*
>
> *[in accordance with art. 4 of the Directive 2016/1148]*

"Cybersecurity" and "cyberthreats" are defined by the "Cybersecurity Act", namely Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013.

> *'cybersecurity' means the activities necessary to protect network and information systems, the users of such systems, and other persons affected by cyber threats;*
>
> *'cyber threat' means any potential circumstance, event or action that could damage, disrupt or otherwise adversely impact network and information systems, the users of such systems and other persons;*
>
> *[in accordance with art. 2 of the Regulation 2019/881]*

Regulation 2019/881 does not apply to railway undertakings, and therefore has been omitted in the compilation of the reference documents (Chapter 7.). It does, however, contain an applicable definition of cybersecurity, which is referred to above.

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.

**Cybersecurity** defined this way, applies both to the information systems used for the purpose of the railway transport and to the operational systems used for the purpose of the railway traffic safety as well as to the operational systems used for the purpose of the railway transport security.

Information systems and solutions, IT systems (Information Technologies), comprise both IT supporting railway infrastructure managers and railway undertakings in carrying out generic tasks and business activities (e.g. personnel and asset management systems, invoicing, IT tools supporting team working) and railway transport-related tasks (e.g. timetabling/scheduling and ticketing systems). Operational systems and solutions, OT (Operational Technologies), comprise both electronic components of signalling systems and control command systems as well as systems ensuring operational communication (e.g. electronic interlockings and ETCS the European Train Control System) as well as systems and solutions utilised for transport security.

Directive on the resilience of critical entities [4] defines “resilience measures” of critical entities in the following way:

*… appropriate and proportionate technical, security and organisational measures to ensure their resilience, based on the relevant information provided by Member States on the Member State risk assessment and on the outcomes of the critical entity risk assessment, including measures necessary to:*

*a) prevent incidents from occurring, duly considering disaster risk reduction and climate adaptation measures;*

*b) ensure adequate physical protection of their premises and critical infrastructure, duly considering, for example, fencing, barriers, perimeter monitoring tools and routines, detection equipment and access controls;*

*c) respond to, resist and mitigate the consequences of incidents, duly considering the implementation of risk and crisis management procedures and protocols and alert routines;*

*d) recover from incidents, duly considering business continuity measures and the identification of alternative supply chains, in order to resume the provision of the essential service;*

*e) ensure adequate employee security management, duly considering measures such as setting out categories of personnel who exercise critical functions, establishing access rights to premises, critical infrastructure and sensitive information, setting up procedures for background checks in accordance with Article 14 and designating the categories of persons who are required to undergo such background checks, and laying down appropriate training requirements and qualifications;*

*f) raise awareness about the measures referred to in points (a) to (e) among relevant personnel, duly considering training courses, information materials and exercises.*

*[in accordance with art. 13 of the Directive 2022/2557]*

This implies, as a minimum, the requirement to provide adequate physical security, proper protection against unauthorised access taking into account digital systems and devices, as such access can be utilised to carry out cyberattacks.

## 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. INFRASTRUKTURA: 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. ENERGIA: Funkcjonowanie systemów dostaw energii nie może szkodzić bezpieczeństwu pociągów lub ludzi (użytkowników, obsługi, osób mieszkających w pobliżu torowiska oraz osób trzecich).*

*1.1.8. STEROWANIE: 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. TABOR: Struktura taboru i połączeń między pojazdami muszą być zaprojektowane tak, aby chronić pasażerów i kabiny maszynistów w przypadku kolizji lub wykolejenia. Urządzenia elektryczne nie mogą szkodzić bezpieczeństwu i funkcjonowaniu instalacji sterowania. Techniki hamowania oraz wywierany nacisk muszą być zgodne z projektem toru, obiektów inżynieryjnych oraz systemów sygnalizacji. Należy podjąć kroki celem uniemożliwienia dostępu do elementów pod napięciem, tak aby nie narażać bezpieczeństwa ludzi. W przypadku niebezpieczeństwa urządzenia muszą umożliwiać pasażerom poinformowanie o nim maszynisty, a obsłudze towarzyszącej – kontakt z nimi. Zapewnione musi być bezpieczeństwo pasażerów wsiadających do pociągów i z nich wysiadających. Drzwi zewnętrzne muszą być wyposażone w system otwierania i zamykania gwarantujący bezpieczeństwo pasażerów. Pociąg musi posiadać oznaczone wyjścia bezpieczeństwa. Należy stworzyć właściwe przepisy celem uwzględnienia szczególnych warunków bezpieczeństwa w bardzo długich tunelach. Na pokładzie pociągów obowiązkowy jest system oświetlenia awaryjnego o wystarczającym natężeniu i czasie funkcjonowania. Pociągi muszą być wyposażone w system komunikacji publicznej stanowiący środek informowania pasażerów przez personel pokładowy. Pasażerowie muszą zarówno na stacjach kolejowych, jak i w pociągach otrzymywać zrozumiałe i wyczerpujące informacje na temat przepisów mających do nich zastosowanie.*

# 2. Definitions

Safety, security and cybersecurity in the context of the EU regulatory framework shall be understood as specified in Subchapters 2.1., 2.2. and 2.3. The broad perception of railway transport safety contained in these subchapters, not limited to railway traffic safety, shall be taken into account when developing documents whose nature, content and structure are defined in Chapter 4.

## 2.1. Safety from the point of view of the railway system interoperability

Safety, as an essential requirement applicable to railway system and to the subsystems constituting the railway system, is defined in Annex III of the Railway Interoperability Directive [1]. The description of the **essential requirement 'safety'** is quoted below in the frame in accordance with the Directive without distinguishing between requirements applicable to the railway system and requirements applicable to individual subsystems constituting the railway system. Two generic requirements related to the need to ensure an adequate level of transport security have been added, below the frame, to gain complete overview.

1.1. *Safety*

*1.1.1. The design, construction or assembly, maintenance and monitoring of safety-critical components, and more particularly of the components involved in train movements, must be such as to guarantee safety at the level corresponding to the aims laid down for the network, including those for specific degraded situations.*

*1.1.2. The parameters involved in the wheel/rail contact must meet the stability requirements needed in order to guarantee safe movement at the maximum authorised speed. The parameters of brake equipment must guarantee that it is possible to stop within a given brake distance at the maximum authorised speed.*

*1.1.3. The components used must withstand any normal or exceptional stresses that have been specified during their period in service. The safety repercussions of any accidental failures must be limited by appropriate means.*

*1.1.4. The design of fixed installations and rolling stock and the choice of the materials used must be aimed at limiting the generation, propagation and effects of fire and smoke in the event of a fire.*

*1.1.5. Any devices intended to be handled by users must be designed in such a way as not to impair the safe operation of the devices or the health and safety of users if used in a foreseeable manner, albeit not in accordance with the posted instructions.*

*1.1.6. INFRASTRUCTURE: Appropriate steps must be taken to prevent access to, or undesirable intrusions into, installations. Steps must be taken to limit the dangers to which persons are exposed, particularly when trains pass through stations. Infrastructure to which the public has access must be designed and made in such a way as to limit any human safety hazards (stability, fire, access, evacuation, platforms, etc.). Appropriate provisions must be laid down to take account of the particular safety conditions in very long tunnels and viaducts.*

*1.1.7. ENERGY: Operation of the energy-supply systems must not impair the safety either of trains or of persons (users, operating staff, trackside dwellers and third parties).*

*1.1.8. CONTROL COMMAND & SIGNALLING: The control-command and signalling installations and procedures used must enable trains to travel with a level of safety which corresponds to the objectives set for the network. The control-command and signalling systems must continue to provide for safe passage of trains permitted to run under degraded conditions.*

*1.1.9. ROLLING STOCK: The rolling-stock structures and those of the links between vehicles must be designed in such a way as to protect the passenger and driving compartments in the event of collision or derailment. The electrical equipment must not impair the safety and functioning of the control-command and signalling installations. The braking techniques and the stresses exerted must be compatible with the design of the tracks, engineering structures and signalling systems. Steps must be taken to prevent access to electrically-live constituents in order not to endanger the safety of persons. In the event of danger, devices must enable passengers to inform the driver and accompanying staff to contact them. The safety of passengers boarding and alighting from trains must be ensured. The access doors must incorporate an opening and closing system which guarantees passenger safety. Emergency exits must be provided and indicated. Appropriate provisions must be laid down to take account of the particular safety conditions in very long tunnels. An emergency lighting system having a sufficient intensity and duration is an absolute requirement on board trains. Trains must be equipped with a public address system which provides a means of communication to the public from on-board staff. Passengers must be given easily understandable and comprehensive information about rules applicable to them both in railway stations and in trains..*

*1.1.10. RUCH: 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.*

*1.1.11. TELEMATYKA: Zapewniony zostać musi odpowiedni poziom uczciwości i niezawodności w zakresie gromadzenia i przekazywania informacji dotyczących 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 [8] 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.

*1.1.10. OPERATION & TRAFFIC MANAGEMENT: Alignment of the network operating rules and the qualifications of drivers and on-board staff and of the staff in the control centres must be such as to ensure safe operation, bearing in mind the different requirements of cross- border and domestic services The maintenance operations and intervals, the training and qualifications of the maintenance and control centre staff and the quality assurance system set up by the operators concerned in the control and maintenance centres must be such as to ensure a high level of safety.*

*1.1.11. TELEMATICS: Suitable levels of integrity and dependability must be provided for the storage or transmission of safety-related information.*

*[in accordance with Annex III of the Directive 2016/797]*

1.1.12. Monitoring of the areas accessible for passengers and other persons (e.g. accompanying passengers) shall ensure appropriate detection of dangerous situations and enable taking appropriate actions.

1.1.13. Monitoring of the areas, rooms, containers, and cabinets, which are not accessible for unauthorised persons shall ensure appropriate protection against vandals, thieves and unauthorised persons having other types of bad intentions, as well as activation of appropriate systems and procedures.

Compliance with the **essential requirement 'safety'**, understood as a set of all of the requirements quoted above as defined in Annex III of the Directive 2016/797, by individual subsystems of the railway system, including the passenger rolling stock, is assessed by EC verification. The principles applicable in this respect are briefly presented in Chapter 3.1. Proving that the generic requirements defined in 1.1.12. and 1.1.13. above are met goes beyond the requirements of the Railway Interoperability Directive. However, the relevant principles are included in these recommendations, in particular in Chapter 4.1, because of the need to ensure an adequate level of protection for the systems providing transport safety.

## 2.2. Security

As already mentioned in the previous chapter, operational processes shall be performed ensuring widely understood transport security, i.e. safety of persons and properties with appropriate measures supporting protection. Therefore for the protection of life, health and property, including in particular the passengers' personal security as referred to in the Regulation on rail passengers' rights and obligations [5], following generic requirements shall apply:

a) Monitoring of the areas accessible to the public (see 1.1.12.) and
b) Monitoring of the areas not accessible to the public (see 1.1.13.).

Technical measures supporting security are in particular: measures supporting the health of the passengers, protections against vandalism, protections against terrorism, measures to protect property, as well as measures against disasters and adverse weather conditions. Defining and analysing security measures shall also take into account the context of the Directive on the resilience of critical entities [4].

## 2.3. Cybersecurity

Cybersecurity, as described in Chapter 1.3. of this recommendations, comprises both, safety of the IT systems as well as safety of the OT systems. In relation to that, it should be noted that both IT systems and OT systems utilise the same types of solutions increasing security of network and information systems. These include:

- organisational and procedural protection means, including information security management systems [8] and systems for granting and revoking access rights;
- systems and solutions ensuring the business continuity of the IT and OT systems, including means for creating and utilising backups, hardware and software redundancies, means protecting data centres against power loss and against fire;
- technological protection means, including authentication systems, anti-malware protection and data processing and transmission control systems; as well as
- physical protection, including remotely supervised locks, video surveillance systems and other systems supporting physical security.

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]).

Recommendations regarding railway passenger rolling stock cybersecurity, due to their scope and purpose, comprise requirements for OT systems supporting railway traffic safety and OT systems supporting transport security.

NOTE: Information security management and IT systems protection will have to be implemented by the railway undertakings in accordance with the series of standards EN ISO/IEC 27000, including in particular EN ISO/IEC 27001 [8] defining the requirements applicable to an information security management system ISMS. The internal regulations adopted as part of the ISMS may require the digital OT systems supporting safety and/or security to utilise certain defined solutions improving the security of network and information systems, e.g. a specific log-in procedure for users or a specific way of collecting logs or making back-ups and recovering systems and data from back-ups after disasters. Some suggestions in this respect are given in Chapter 5. of these recommendations.

## 2.4. Key definitions of various terms presupposed for recommendations

1) **Safety** – freedom from unacceptable risk [9].
2) **Cybersecurity** – activities necessary to protect network and information systems, the users of such systems, and other persons affected by cyberthreats [2019/881].
3) **Cyberthreats** – any potential circumstance, event or action that could damage, disrupt or otherwise adversely impact network and information systems, the users of such systems and other persons [2019/881].
4) **Security of network and information systems** – the ability of network and information systems to resist, at a given level of confidence, any action that compromises the availability, authenticity, integrity or confidentiality of stored or transmitted or processed data or the related services offered by, or accessible via, those network and information systems [2].
5) **Safety case** – documented demonstration that the product (e.g. a system, subsystem or equipment) complies with the specified safety requirements [9].
6) **SSC case proving safety, security and cybersecurity integrity** – document prepared by the **contractor** for the concept, design or construction, complying with the requirements specified in Chapter 4.1. of this document, to be evaluated in accordance with the requirements specified in Chapter 4.2. of this document.
7) **Internal safety coordinator** – that part of the internal structure of the railway undertaking, which coordinates the railway undertaking's internal processes with regard to safety.
8) **Competent independent inspection body** - a body accredited by the National Accreditation Body as an assessment body for risk analyses and evaluations carried out in accordance with the Risk Evaluation and Assessment Regulation [6, 7] covering with its accreditation all five structural subsystems – Infrastructure, Energy, Trackside Control-Command and Signalling as well as Rolling Stock and On-board Control-Command and Signalling subsystem, which is carrying out assessment of the '**SSC case proving safety, security and cybersecurity integrity**'.
9) **Risk** – combination of expected frequency of loss and the expected degree of severity of that loss [9].
10) **Contractor** – entity developing a concept or designing, or constructing railway passenger rolling stock, or installing equipment on such stock, or making changes to the concept, design or construction of railway passenger rolling stock or its equipment.
11) **Generic requirements regarding security** – requirements 1.1.12 and 1.1.13. described in Chapter 2.1. of these recommendations (defined as high level requirements in relation to transport security).
12) **Essential requirement 'safety'** – requirements from 1.1.1. to 1.1.11. quoted in chapter 2.1. of these recommendations (in accordance with Annex III of the Directive on the interoperability [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 dyrektywą 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. Właściwe działania 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,*

# 3. Interoperability versus cybersecurity

The need to ensure interoperability of the railway system derives from the Directive 2016/797 [1] while the need to ensure cybersecurity of the railway transport derives from the Directive 2016/1148 [2] replaced by the Directive 2022/2555 [3]. These directives, and the specific documents issued under them, do not contain provisions to trace the relationship between the formal requirements regarding interoperability and the formal requirements regarding cybersecurity. Notwithstanding this, requirements from both areas, in many cases, simultaneously apply to the same digital technical solutions utilised, for example, in railway passenger rolling stock.

## 3.1. Interoperability

As stated in the Directive 2016/797 [1], interoperability means "*the ability of a railway system to allow the safe and uninterrupted movement of trains, which accomplish the required levels of performance for these railway lines; The ability which depends on all the regulatory, technical and operational conditions, which must be met in order to satisfy the essential requirements*". Among the six essential requirements defined in the Directive, one, the **essential requirement 'safety'**, is directly linked to **cybersecurity** requirements for technical solutions that are digital in nature.

Simultaneous applicability of interoperability requirements and cybersecurity requirements therefore applies, for example, to the on-board systems ensuring communication between the driver and the traffic controllers, and to the on-board installations of the ETCS European Train Control System.

## 3.2. Security

In accordance with the provisions of the Regulation 2021/782 [5], railway undertakings, in agreement with public authorities, infrastructure managers, and station managers, are required to take appropriate measures to ensure passengers' personal security at the railway stations and on the trains. Appropriate activities shall result from risk control processes starting with the identification of threats, including the identification of cyberthreats relevant for railway passenger rolling stock. Railway undertakings are also required to undertake such activities on the basis of the Directive on the resilience of critical entities [4].

Digital systems utilised to ensure passengers' personal security on the trains, such as video surveillance systems, passenger information systems, and passenger brake systems, shall be taken into account when cybersecurity of the railway passenger rolling stock is under consideration.

## 3.3. Cybersecurity

Major threats regarding transport cybersecurity are described in Chapter 3.3.1. Chapter 3.3.2 presents adopted classification of railway passenger rolling stock functionalities. The types of unauthorised interventions into the cybersecurity of rolling stock, which were identified during the development of the recommendations are presented in Chapter 3.3.3. An overview of the measures utilised to ensure cybersecurity in rail transport is described in Chapter 3.3.4, while cybersecurity measures for railway passenger rolling stock are described in Chapter 3.3.5.

### 3.3.1. Major threats regarding cybersecurity in railway transport

Initial identification of the major threats was based on the "Transport cybersecurity toolkit", which was developed and made available in the year 2020 by the European Commission. According to the provisions of this document, both individuals or organisations may intentionally or unintentionally expose and exploit vulnerabilities, which have the potential of causing incidents and affecting transport services including their safety, security, business, finance and reputation. Threat actors involve, among others,

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, grupy sponsorowane przez państwa narodowe i 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 cyber-incydentami 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 usług (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)**
(cyberataki 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**
(cyberataki 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 (1 do 4 wg przywołanego dokumentu) 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.

state-sponsored groups, cyber criminals, cyber terrorists, hacktivists[1)], hackers (including script kiddies[2)]), and insiders with authorised access to inside information (including privileged insiders with authorised access to such information).

The most significant malicious actors intentionally targeting transport organisations are cyber criminals, insiders, nation states and state-sponsored groups. Adversaries such as cyber criminals conduct massive attack campaigns and are often in the game for monetary rewards.

Insiders, know the singularities of the organisations they work for and are often well aware of subtle security vulnerabilities. Insider threat actors may involve disgruntled employees, suppliers and individual contractors. As global geopolitical tensions intensify, nation states and state-sponsored groups target strategy long-term objectives. They often try to conceal themselves in the depth of organisations' systems and collect sensitive information. Once they establish their foothold into systems, state sponsored attackers look to gain a position that has the potential to create the worst damage possible. For example, they may target other organisations' systems by exploiting the organisations' network connections.

Other threat actors involve insiders, who may unintentionally or accidentally perform actions resulting in cybersecurity events and, in worst cases, cyber incidents affecting the safety and security of transport services.

According to the document “Transport cybersecurity toolkit”, there are a substantial number of cyberthreats targeting transport: distributed denial of service (DDoS), denial of service (DoS), data theft, malware diffusion, phishing, software manipulation, unauthorised access, destructive attacks, falsification or bypassing of security operator decision process, masquerading of identity, abuse of access privileges, social engineering, defacement, eavesdropping, misuse of assets, and hardware manipulation.

The document states, that based on comprehensive literature research of publicly available documentations and interviews with experts, the most pressing emerging cyberthreats affecting transport are following four threats:

**1. Malware**
(malicious software that may potentially affect individuals or organisations across transport modes)

**2. (Distributed) Denial of Service (DDoS & DoS)**
(cybersecurity attacks preventing individuals or organisation to access relevant transport services and resources)

**3. Unauthorised Access and Theft**
(unauthorised access, appropriation, and exploitation of critical assets)

**4. Software Manipulation**
(cybersecurity attacks targeting software in order to modify its behaviour & conducting specific attacks)

These four threats as a result of the war beyond Poland's eastern border shall be supplemented by:

**5. Remote (authorized) Shutdown R(A)S**
(remote shutdown of a system by a person/entity claiming to be entitled or even obliged to shut down the system)

The various cyberthreats (1 to 4 according to the quoted document) shall be understood as follows:

[1)] Hacktivists are individuals using computers and networks to promote social and political goals, especially freedom of expression, human rights and access to information.

[2)] Script kiddies are individuals using programs and scripts written by others without in-depth knowledge of their functioning, for the sole purpose of gaining unauthorised access to digital user accounts or files or to carry out attacks on computer systems.

**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.).

**Ad. 1. Malware**
Malware consists of malicious software, which may include different types of software applications such as viruses, trojans, worms, ransomwares, cryptocurrency-miners, or any software that may have potentially adverse impacts on organisations or individuals across transport modes.

Mitigating the diffusion of malware designed for intentionally damaging computers, servers, clients, networks, or all of them is amongst the main priorities of cybersecurity across all modes of transport. A typical attack vector may involve phishing emails targeting employees. Other attack vectors may involve different and sophisticated social engineering strategies such as plugging in a USB key into a free port (e.g. charging of mobile phone).

By clicking hyperlinks in suspicious emails or opening file attachments, the user may unknowingly be installing software or knowingly jeopardising transport services and resources.

For example, the WannaCry ransomware cyber-attack affected more than 150 countries and infected over 230 000 systems. It involved a ransomware that usually spreads via phishing emails containing malicious attachments or hyperlinks. This type of attack exploits social engineering maliciously in order to mislead system users into installing (or activating) specific malware.

**Ad. 2. (Distributed) Denial of Service (DDoS & DoS)**
Distributed Denial of Service (DDoS) and Denial of Service (DoS) attacks affect availability and accessibility of data, services, systems, and other resources.

These types of attacks can range in duration and may target more than one service or system at a time. DDoS attacks employ multiple systems (or channels of attack) in order to overload target services or systems with requests. Successful attacks affect service and system capabilities to deal with unexpected volume requests. This results in denying access to services and resources.

Note that affected services and systems belonging to transport organisations may be exploited in order to conduct DDoS and DoS attacks to target specific systems in operations or other organisations as well. For example, corporate information systems (such as personal computers and devices) may be targeted in order to access operation technologies, which may be connected to the internet or accessing networks in order to transfer operational data. Connections between different systems and networks (such as corporate networks, operation technologies and remote maintenance accesses) may represent exploitable vulnerabilities for conducting DDoS or DoS attacks to critical transport services and systems. For example, DDoS and DoS attacks can exploit common network and communication protocols such as the Web Services Dynamic Discovery (WS Discovery), which loT devices may use to automatically discover each node on Local Area Networks (LANs). lf loT devices present vulnerabilities, attackers may exploit them in order to discover other connected devices and conduct DDoS or DoS attacks.

**Ad. 3. Unauthorised Access and Theft**
Threat actors may want to gain logical or physical access without permission to a network, system, application, data, or another resource in order to conduct malicious activities, including theft of sensitive data or resources (including physical resources). Disruptive actions are considered to be both intervention with programmes and data and physical loss of programmes and/or data.

Unauthorised access and theft threats target confidential and proprietary assets (including personal identities, credentials of privileged accounts, systems, and other types of confidential and proprietary information). These threats may exploit systems vulnerabilities as well as unaware individuals disclosing sensitive data such as credentials (e.g. login, password, etc.) or personal data (e.g. email, personal identification number, etc.).

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. Cyberataki 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.

*In relation to unauthorised access, identity theft is the illicit use of personal data or unique identifiers in order to impersonate persons or services and systems to gain access to private or proprietary resources (e.g. including financial and physical resources). Such cybersecurity threats may target also physical assets across transport modes.*

***Ad.4. Software Manipulation***

*Misconfigurations and manipulations of software and related systems or components may have a direct impact on the security posture of transport services and systems. Cybersecurity attacks exploiting software manipulations modify software settings or affect the integrity of data in order to change the behaviours of systems and services.*

*Attackers may intentionally manipulate software (or part of it) in order to gain advantages (e.g. obtaining unauthorised access, preventing legitimate individuals or systems access to necessary resources, collecting sensitive information, changing functional behaviours, etc.) over sensitive assets.*

*For example, attackers may target communication channels of manufacturers in order to upload malicious software updates on services and systems (including operation technologies) in operations. A threat agent uses compromised authorisation credentials to access a secured remote maintenance network interface in order to install manipulated software and further compromise other accessible services and systems. The threat agent installs manipulated software that further compromises target services and systems, or attacks other connected services or systems, or introduce software changes designed to enable a cyberattack.*

**Ad. 5. Remote (authorized) Shutdown R(A)S**

The avalanche of cyberattacks since the beginning of 2022 in connection with the war beyond the Polish eastern border has shown that serious consideration shall also be given to the possibility of remote shutdown of various types of systems and devices by persons or entities who manufactured, configured or maintained them and who, in light of the legal or military situation, deem it necessary to take advantage of the possibility of remotely shutdown the system or device and remotely remove or modify their software in such a way as to make it impossible to turn them back on without the involvement of the manufacturer or authorised service provider.

In March 2023, the European Union Agency for Cybersecurity ENISA released the Threat Landscape for the Transport Sector for the period January 2021 to October 2022. This document contains analysis for the entire transport sector and separate analyses for air, water, rail, road, and 'cross sector attacks'. The following types of attacks are considered:

**Ransomware**

Ransomware is defined as a type of attack where threat actors take control of a target's assets and demand a ransom in exchange for the return of the asset's availability.

**Threats against data**

Sources of data are being targeted with the aim of unauthorised access and disclosure and manipulating data to interfere with the behaviour of systems. These threats are also the basis of many other threats, also discussed in this report. For instance, ransomware, or DDoS attacks aim to deny access to data and possibly collect a payment to restore this access. Technically speaking, threats against data can mainly be classified as data breaches and data leaks. A data breach is an intentional attack brought by a cybercriminal with the goal of gaining unauthorised access and the release of sensitive, confidential or protected data. A data leak is an event that can cause the unintentional release of sensitive, confidential or protected data due to, for example, misconfigurations, vulnerabilities or human errors.

**Malware**

Malware is an overarching term used to describe any software or firmware intended to perform an unauthorised process that will have an adverse impact on the confidentiality, integrity or availability of a system. Traditionally, examples of malicious code types include viruses, worms, trojan horses, spyware, adware or other code-based entities that infect a host.

**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]*

**Denial of service**
Availability is the target of a plethora of threats and attacks, among which DDoS stands out. DDoS attacks target system and data availability and, though not a new threat, have a significant role in the cybersecurity threat landscape of the transport sector. Attacks occur when users of a system or service are not able to access relevant data, services or other resources. This can be accomplished by exhausting the service and its resources or overloading the components of the network infrastructure. Present geopolitical developments and hacktivist activities increased the number of DDoS attacks against transport organisations.

**Vulnerability exploitation**
Vulnerability exploitation refers to exploitation of known or zero-day vulnerabilities.

**Social engineering**
Social engineering encompasses a broad range of activities that attempt to exploit a human error or human behaviour with the objective of gaining access to information or services. It uses various forms of manipulation to trick victims into making mistakes or handing over sensitive or secret information. In cybersecurity, social engineering lures users into opening documents, files or emails, visiting websites or granting unauthorised persons access to systems or services. This threat canvas consists mainly of the following vectors: phishing, spear-phishing, whaling, smishing, vishing, business email compromise, fraud, impersonation and counterfeiting. Presently we primarily observed phishing and spear phishing attacks targeting transport users and fraud, impersonation and counterfeit incidents.

**Attacks to suppliers and supply-chain attacks**
A supply-chain attack targets the relationship between organisations and their suppliers. According to ENISA 'Threat Landscape for Supply Chain' document an attack is considered to have a supply-chain component when it consists of a combination of at least two attacks. For an attack to be classified as a supply-chain attack, both the supplier and the customer have to be targets. Threat actors are continuing to feed on this source to conduct their operations and gain a foothold within organisations, in an attempt to benefit from the widespread impact and potential victim base of such attacks. Presently both supply-chain attacks, as defined above, and attacks to suppliers that caused disruptions or losses to entities in the transport sector are observed.

**Breach/intrusion**
Breach/intrusion refers to incidents where an attack to a system has been confirmed or made public and attackers have gained access to systems, but the details of how the breach or the intrusion took place are not clear.

Other threats include single occasions of **credential harvesting** and **spoofing of geolocation** in the maritime sector.

Finally, there is a small percentage of incidents where even though a cyberattack took place, there is insufficient information to allow for the incident to be categorised. Such incidents are accounted as **unknowns**.

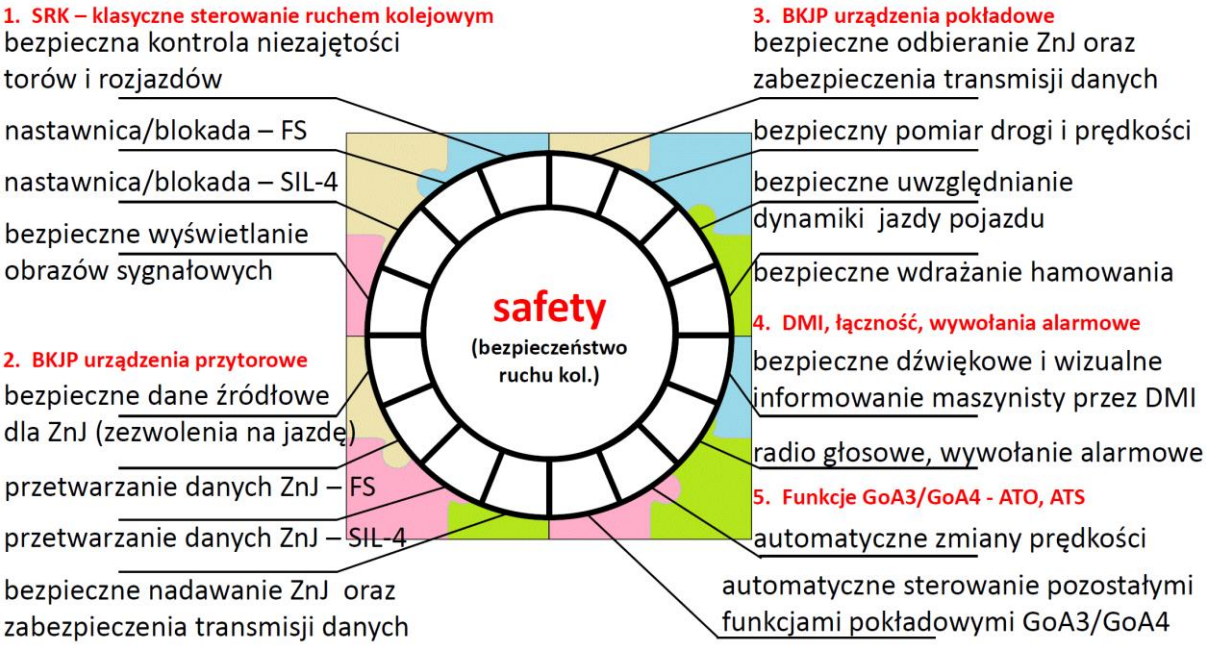
*[in accordance with ENISA Threat Landscape: Transport Sector, March 2023]*

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 trzy 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 5 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.

An analysis of the 2021 and 2022 cyberattacks indicates that railway transport shall be protected in particular against:

a) ransomware,
b) threats against data,
c) DoS, DDoS, RDoS attacks,
d) breach/intrusions, and
e) vulnerability exploitation.

### 3.3.2. Identification of digital functionalities of the systems and equipment of the passenger rolling stock

In passenger rolling stock, including trainsets and trains composed of locomotives and coaches, three areas regarding rolling stock movement safety functionalities “safety” and four areas of transport security functionalities “security” were distinguished. The 'safety' areas are shown in Figure 1, together with the two complementary safety areas that remain on the infrastructure side, while the 'security' areas are shown in Figure 2.

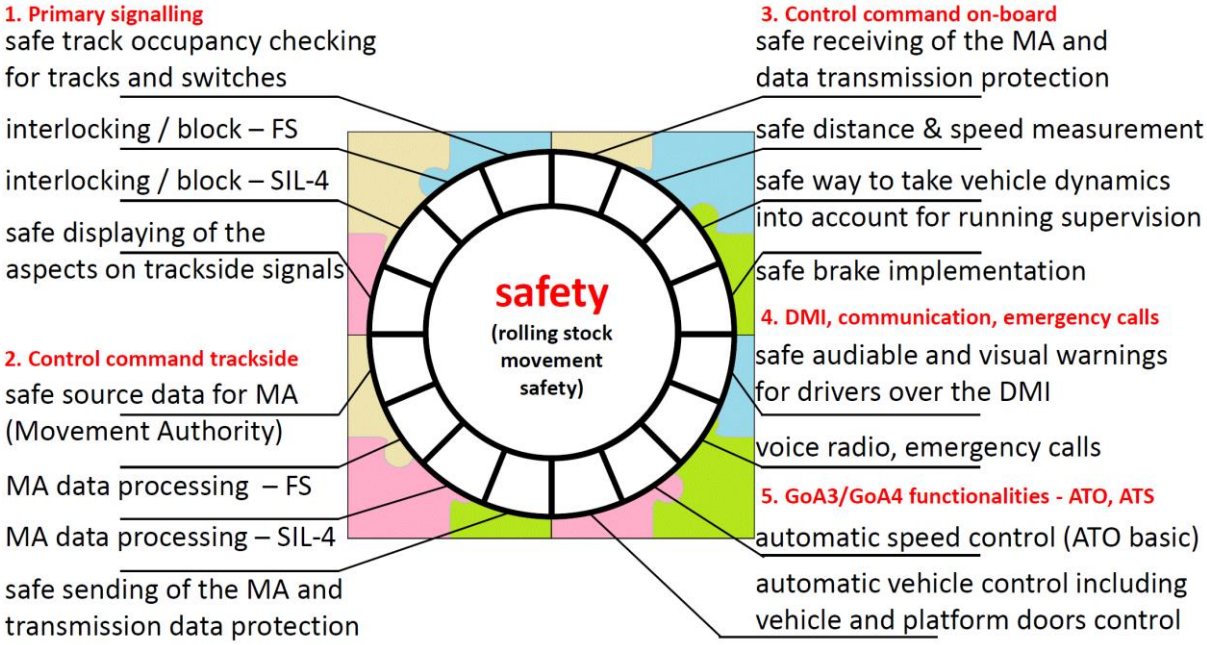



Figure 1. Rolling stock movement safety functional areas – safety
(source: own elaboration)

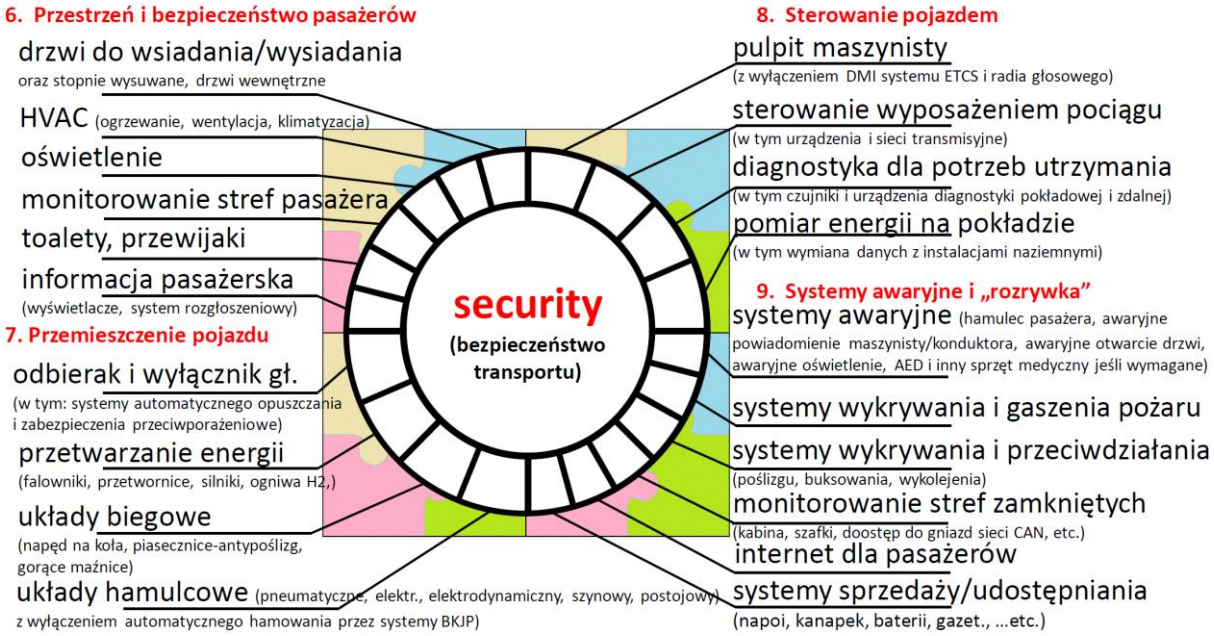
Areas 1 to 5 correspond to the control sheets given in Chapter 4. It is underlined that the control sheets “1. Primary signalling” and “2. Trackside Control-Command” contain reference values for the answers to the control questions, describing the characteristics of trackside control-command and signalling equipment of the reference infrastructure. Which is the infrastructure in relation to which safe supervision of the way drivers are driving and/or safe automatic train operation are assessed. The second for the vehicles equipped with automatic train operation functions indicated as being provided by the systems providing grades of automation GoA3 and GoA4 defined in IEC 62267:2009-07. This standard defines the grades of automation in accordance with table below. Control sheets “3. On-board Control-Command” and “4. DMI, communication, emergency calls”, and “5. GoA3/GoA4 functionalities - ATO, ATS” contain control questions used to assess rolling stock in relation to railway traffic safety.

Tabela 1. Poziomy automatyzacji prowadzenia pociągu – 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)

Table 1. Train operation Grades of Automation - GoA

| Grades of automation ➔ / Basic functions of train operation | | On-sight train operation | Non-automated train operation | ETCS baseline 2.3.0.d 3.4.0/3.6.0 | Semi-automated train operation | ETCS baseline 4.0.0 TSI 2023 | Driverless train operation | Unattended train operation | ETCS baseline 5.0.0 (?) TSI 2025 |
|---|---|---|---|---|---|---|---|---|---|
| | | TOS | NTO | NTO | STO | STO | DTO | UTO | UTO |
| | | GoA0 | GoA1 | GoA1 | GoA2 | GoA2 | GoA3 | GoA4 | GoA4 |
| Ensuring safe movement of trains | Ensure safe route | X (points command/ control in system) | S | S | S | S | S | S | S |
| | Ensure safe separation of trains | X | S | S | S | S | S | S | S |
| | Ensure safe speed | X | X (partly supervised by system) | S | S | S | S | S | S |
| Driving | Control acceleration and braking | X | X | braking - S accelerating - X | S | S | S | S | S |
| Supervising guideway | Prevent collision with obstacles | X | X | X | X | X | S | S | S |
| | Prevent collision with persons | X | X | X | X | X | S | S | S |
| Supervising passenger transfer | Control passengers doors | X | X | X | X | X | X or S | S | S |
| | Prevent injuries to persons between cars or between platform and train | X | X | X | X | X | X or S | S | S |
| | Ensure safe starting conditions | X | X | X | X | X | X or S | S | S |
| Operating a train | Put in or take out of operation | X | X | X | X | X | X | S | S |
| | Supervise the status of the train | X | X | X | X | X | X | S | S |
| Ensuring detection and management of emergency situations | Perform train diagnostic, detect fire/smoke and detect derailment, handle emergency situations (call/evacuation, supervision) | X | X | X | X | X | X | S and/or OCC staff | S and/or OCC staff |

X = staff responsibility  S = realised by technical system

Figure 2. shows the functional areas 6. to 9. which correspond to the control sheets “6. Passenger space and safety”, “7. Vehicle movement”, “8. Vehicle control”, and “9. Emergency systems and ‘entertainment’” given in Chapter 4. Which contain the control questions used to assess rolling stock in relation to transport security.

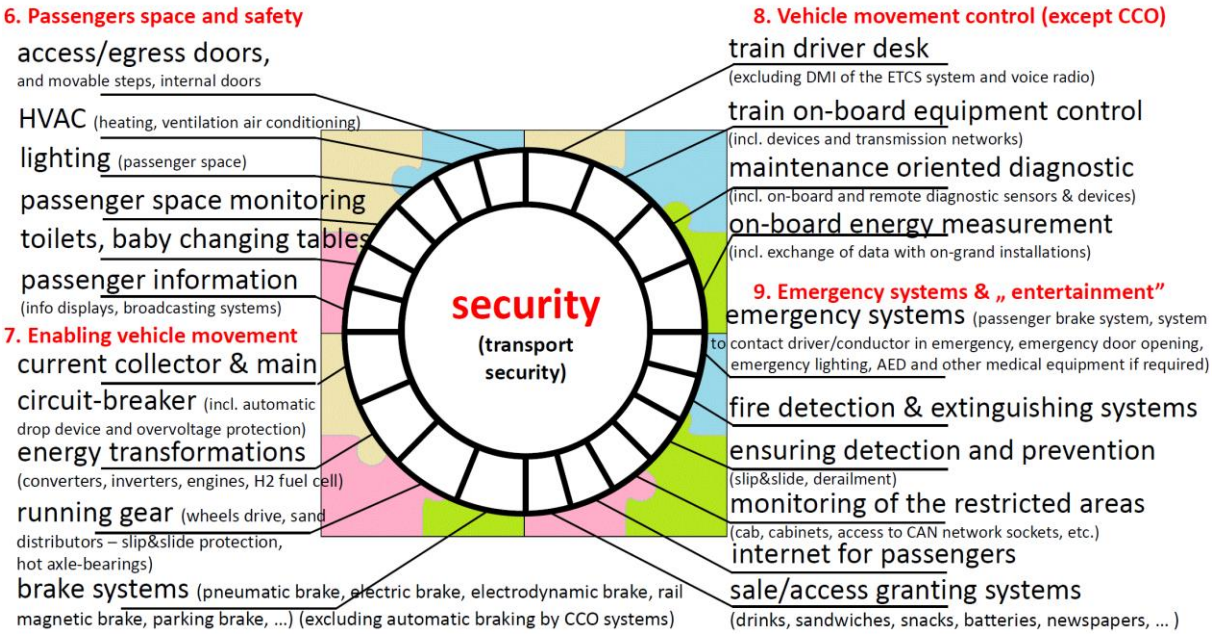
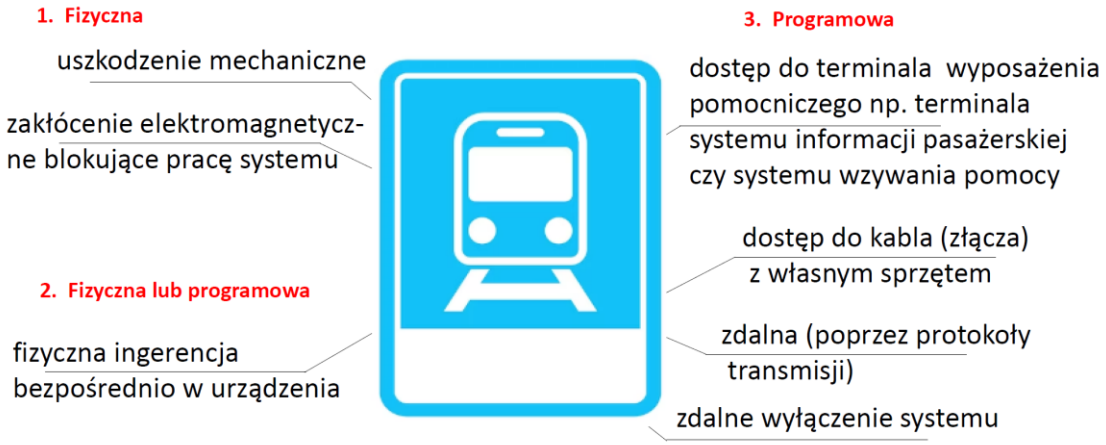



Figure 2. Transport security functional areas
(source: own elaboration)

### 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 nie tylko dezaktywować 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.

### 3.3.3. Types of unauthorised interventions in the passenger rolling stock and its equipment

Intervention in the rolling stock on-board systems can take place at a number of levels of access, ranging from mechanical intervention, through unauthorised connection to the network/system, to remote intervention that does not require the attacker to be on board, or even close to the vehicle. The different levels and cases of intervention in rolling stock and its equipment are shown in Figure 3.

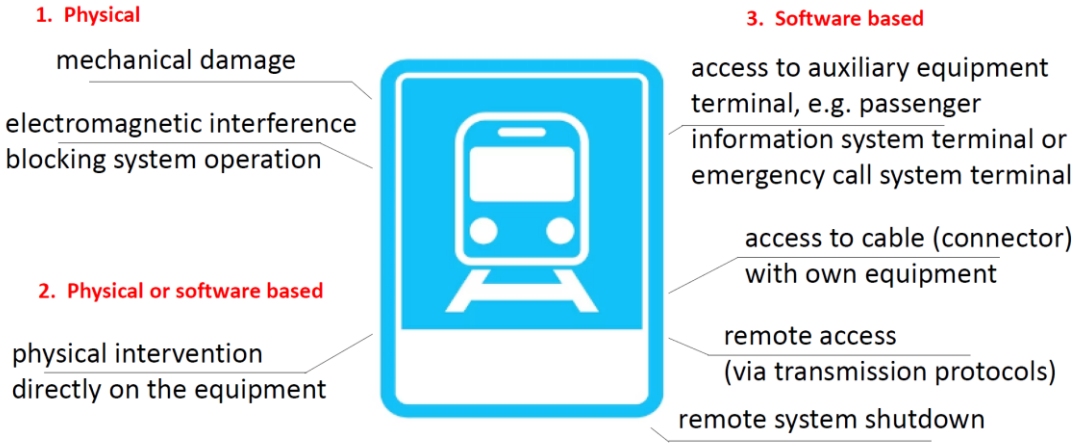



Figure 3. Levels of intervention in on-board rolling stock systems

**Physical intervention** is based on the possibility of manipulation directly at the device location. This manipulation can be mechanical, e.g. by changing the position of switches or disconnecting cables, or software based - by changing the software settings of the device using the available human-machine interface. The effect of such manipulation can be, for example, switching off the device, activating or deactivating of its functions, or changing its firmware by swapping files or launching an update procedure from external media directly plugged into the port of the device under attack.

By **accessing the terminal**, it is possible to influence the way the device's software is working, i.e. maliciously activate or deactivate its functions, change settings, operating parameters or even enter a service mode enabling update or deactivation of software.

Using **cable access** (access to a connector or internal port, e.g. a USB connector) with own hardware, one can eavesdrop on the transmission, interfere with it and, in most cases, connect to the internal network using own terminal. That makes it possible to continue to operate in the system on a software level. In the worst-case scenario, cable access provides the same possibilities as physical access to the device or its terminal with the possibility of modifying and/or deleting data.
**Remote intervention** uses available remote transmission protocols (such as bluetooh, wi-fi) with open communication ports to connect to and modify the vehicle's on-board system.

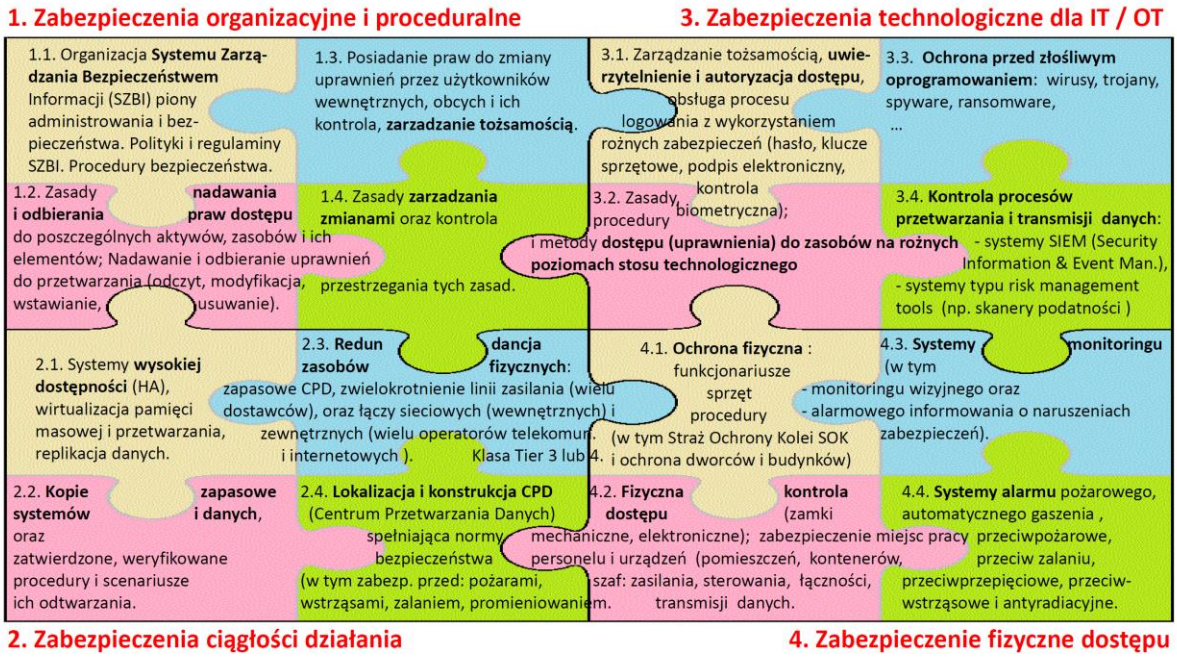
Through **mechanical damage**, systems can be forced to deactivate, transmission between systems can be broken, and/or systems can be forced to operate/not operate under certain conditions.

Intentionally generated strong **electromagnetic interference** can not only deactivate wireless transmission systems, but also can lead to a reset or suspension of the digital systems. For example, relatively simple drone deactivation systems are known, which are based on the directional emission of a strong electromagnetic interference.

**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 (patrz Rys. 1. oraz Rys. 2.).




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:

**Remote system shutdown** is most often a function implemented in the system software of the devices by manufacturers, e.g. in the event of equipment theft. In theory, no one should have access to this function and it should only be possible to activate it under strictly defined conditions. Unauthorised activation of this function results in system shutdown and often the inability to restart the system without the involvement of the manufacturer or its authorised service centre.

### 3.3.4. Cybersecurity measures in railway transport

There are four groups of cybersecurity measures providing protection for different IT and different OT systems. The adopted subdivision of the cybersecurity measures is shown schematically in Figure 4. in the form which is used as a background against which the relevant functionalities of IT and OT systems are presented (see Fig. 1. and Fig. 2.).

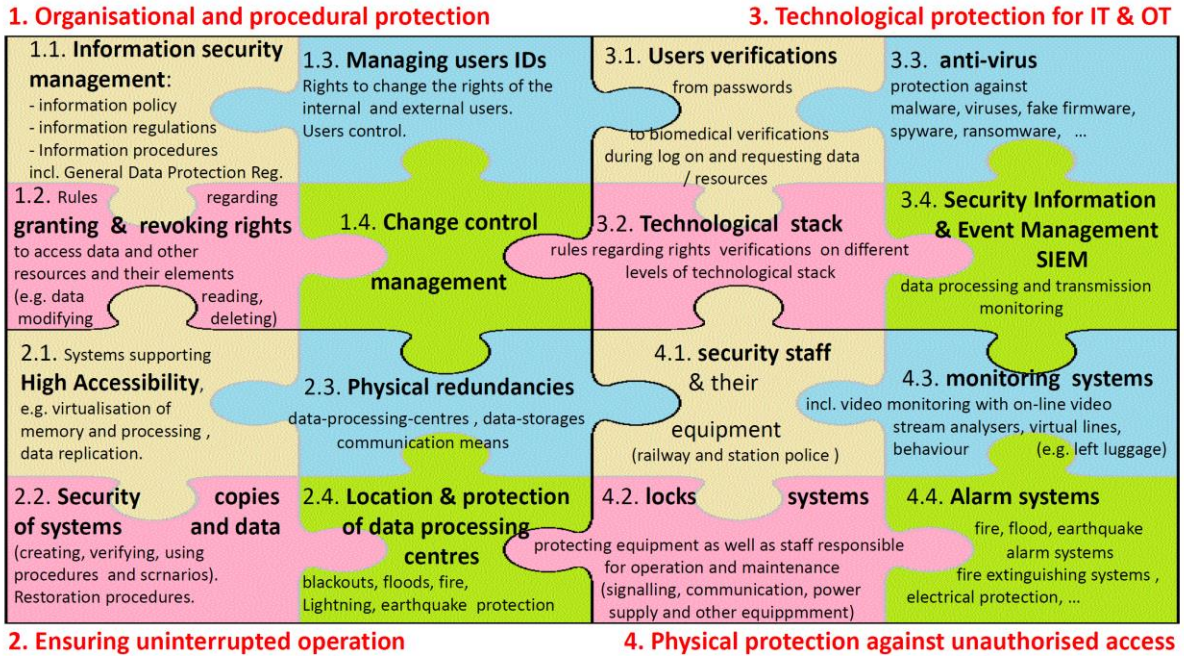



Figure 4. Cybersecurity measures in railway transport
(source: own elaboration)

Cybersecurity measures are subdivided into:

**1. Organisational and procedural protection means**

Organisational and procedural protection means shall be structured and precisely described as part of the implementation of the Information Security Management System (ISMS) by railway undertakings and railway infrastructure managers. Respective means are subdivided as follows:

1.1. Organisation of the Information Security Management System (ISMS), including the responsibilities and activities of the administration and security divisions, as well as ISMS policies and regulations and security procedures;

1.2. Rules regarding granting and revoking rights to access individual assets, resources and their elements. The granting and revoking data processing rights with subdivision into reading, modifying, inserting and deleting rights;

1.3. Provision and control of rights to change the rights by internal and external users, along with other identity management issues;

1.4. Change control management rules for changes influencing organisational and procedural protection means including monitoring of the application of the rules which are adopted.

**2. Ensuring uninterrupted operation**

Development and application of Business Continuity Plans (BCP), taking into account requirements of the ISO 22301 standard and good practices. Respective means are subdivided as follows:

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 zweryfikowane i zatwierdzone procedury tworzenia, weryfikacji kopii oraz 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 bezpieczeństwa; 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.

2.1. High-availability (HA) systems, mass storage virtualisation, and data processing virtualisation as well as data replication;
2.2. Backuping – making and using security copies of systems (software) and data, including verified and approved procedures describing the way copies are made and verified as well as scenarios regarding restoring systems and data in the event of loss or damage;
2.3. Use of physical resources redundancies, including backup Data Processing Centres (DPC), multiplication of electrical power supply lines (including option with power supply from multiple suppliers), multiplication of network connections (internal) and external network connections (including option with connections provided by different telecoms and/or different internet providers). Tier 3 or 4 class;
2.4. Principles regarding determining and accepting the location and design of the DPC centres taking into account security standards including, but not limited to, protection against: fires, vibrations, flooding, radiation.

**3. Technological protection for IT & OT systems**

Applied and possible technological and process protection means are subdivided into technological protection means (3.1., 3.2., 3.3.) and process based protection means (3.4.) as follows:

3.1. Identity management, including authentication and authorisation of access and handling the log-in process using the various applied and possible protection means (passwords, hardware keys, electronic signatures, biometric control);
3.2. Defining and applying rules, procedures and methods for accessing resources (obtaining authorisation and using authorisation) on different levels of the technological stack;
3.3. Protection against malware, including but not limited to viruses, trojans, spyware, ransomware;
3.4. Data processing and transmission monitoring, including systems such as SIEM (Security Information & Event Management) and tools and systems dedicated for risk management, such as vulnerability scanners.

**4. Physical protection against unauthorised access**

Physical protection is an absolutely necessary complementary area. Respective means are subdivided as follows:

4.1. Physical protection of infrastructure, including in particular the physical protection of buildings and premises housing systems and equipment from which unauthorised access to IT information systems and/or OT operational systems could be possible. Physical protection include, in particular, the officers, equipment and procedures of the Railway Police as well as the requirements imposed on other entities providing physical protection of such locations;
4.2. Mechanical and electronic locks and other solutions protecting staff workplaces as well as places where systems and equipment operate (traffic controllers' working rooms, drivers' cabs, maintenance workplaces, containers and cabinets containing equipment: power supply, control command and signalling, communication, data transmission, etc., both on the infrastructure and on the rolling stock sides);
4.3. Surveillance systems including both video monitoring systems and alarm systems to report security breaches; as well as
4.4. Protection systems against natural and construction disasters, including fire protection systems such as fire detection, smoke detection, automatic fire extinguishing, as well as flood protection, surge protection, anti-shock and anti-radiation systems.

### 3.3.5. Cybersecurity measures for the railway passenger rolling stock

From the point of view of assessing safety, security and cybersecurity and their functional integrity for a given type of vehicle/passenger train, type 1 protection means, i.e. organisational and procedural protection means applied by the railway undertaking, are not applicable. This does not mean that vehicle manufacturers do not need such protection means, but such protection means applied by manufacturers do not explicitly protect railway undertakings during rolling stock operation. At the same time, it shall be underlined that the railway undertakings and the entities in charge of maintenance need type 1 protection means, as the ones supporting maintenance supervision as well as registration and handling of the operational incidents.

Natomiast zabezpieczenia typu 2. zapewniające ciągłość działania rozwiązań technicznych oraz zabezpieczenia typu 3 czyli zabezpieczenia technologiczne oraz typu 4. czyli fizyczne zabezpieczenia przed nieuprawnionym dostępem powinny być stosowane w pasażerskim taborze kolejowym.

Pytania kontrolne wskazane w kartach kontrolnych 3., 4. oraz 5. w zakresie bezpieczeństwa ruchu kolejowego – safety, oraz 6., 7., 8., 9. w zakresie bezpieczeństwa transportu czyli szeroko rozumianej ochrony – security, a także pytania kontrolne wskazane w kartach kontrolnych 10., 11., 12., 13. oraz 14. dedykowanych 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 producentów 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.

In contrast, type 2. protection means ensuring uninterrupted functioning of the technical solutions and type 3. protection means, i.e. technological protection as well as type 4. protection means i.e. physical protection against unauthorised access, shall be applied in case of railway passenger rolling stock.

Control questions, which are listed in the control sheets 3., 4., and 5. regarding railway traffic safety – safety sheets, and which are listed in the control sheets 6., 7., 8., and 9. regarding transport safety, i.e. widely understood security – security sheets, as well as the ones, which are listed in the control sheets 10., 11., 12., 13., and 14., which are dedicated directly to cybersecurity, indicate required and optional application of individual cybersecurity measures for selected rolling stock functionalities and rolling stock equipment.

### 3.4. Interoperability versus cybersecurity understood as an adequate level of the integrity of safety, security and cybersecurity

Proving compliance with the essential requirements as they are defined in the Directive [1], including the essential requirement 'safety', require that:

a) all types of interoperability constituents, which are foreseen to be integrated into rolling stock possess EC certificates of conformity, which were issued by appropriate notified bodies for different technical solutions;
b) all individual interoperability constituents integrated into rolling stock were supplied together with individual EC declarations of conformity issued by their manufacturers or were supplied together with EC declaration of conformity for many individual interoperability constituents issued by their manufacturer;
c) all types of devices for which national type certificate is required (e.g. on-board class B radio), which are foreseen to be integrated into rolling stock possess type certificates issued by the respective national authority (e.g. UTK Office of Rail Transport) for different technical solutions;
d) all individual devices for which national type certificate is required, which are integrated into rolling stock were supplied together with individual declarations of conformity to type issued by their manufacturers or were supplied together with declaration of conformity to type for many individual devices issued by their manufacturer;
e) all structural subsystems (rolling stock subsystem and on-board control-command and signalling subsystem), constituting together the rolling stock, possess EC certificates of verification issued by appropriate notified bodies for the different subsystems;
f) all structural subsystems (rolling stock subsystem and on-board control-command and signalling subsystem), constituting together the rolling stock, possess EC declaration of verification issued by their manufacturers for the different subsystems;
g) rolling stock constituted by the structural subsystems (rolling stock subsystem and on-board control-command and signalling subsystem) is authorised to be put in service by national safety authority (e.g. UTK Office of Rail Transport) before being put into service.

Above mentioned requirements derive from legal provisions. EC Certificates of Conformity and EC Declarations of Conformity as well as Type Certificates and Declarations of Conformity to Type as well as EC Certificates of Verification and EC Declarations of Verification confirm compliance with the essential requirements, including the essential requirement 'safety' (essential requirements 1.1.1. to 1.1.11.). These confirmations are considered insufficient regarding safety, security and cybersecurity integrity as essential requirement 'safety' does not apply to those solutions that support security (generic requirements regarding security 1.1.12. and 1.1.13.) and does not apply to solutions supporting cybersecurity. In particular, it omits assemblies and components that are not interoperability constituents but contain firmware and are connected to the WTB and/or TCN on-board network.

# 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, zabezpieczenia 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.

Autorzy koncepcji/konstruktorzy (**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.

# 4. Detailed requirements for documenting and assessing safety, security and cybersecurity integrity for new railway passenger rolling stock

Principles regarding proving and verifying safety, security and cybersecurity integrity, which are defined in Chapter 4 of this document, collectively provide methodology adopted for the purpose of verification of the functional completeness and adequacy of safety, security and cybersecurity of the passenger rolling stock.

Chapter 4.1 defines the principles for proving safety, security and cybersecurity integrity by rolling stock manufacturers developing concepts/designs for new types of rolling stock and then producing passenger rolling stock, and by entities implementing technical changes affecting such rolling stock safety, security or cybersecurity when rolling stock is already in service.

Chapter 4.2 defines the rules for the verification of safety, security and cybersecurity integrity by a **competent independent inspection body**.

## 4.1. SSC cases proving safety, security and cybersecurity integrity

### 4.1.1. Generic requirements for rolling stock SSC cases proving safety, security and cybersecurity integrity

For the concepts, designs and procurement of a new rolling stock, it is required that the contractor develops “rolling stock SSC case proving safety, security and cybersecurity integrity” and obtains a report of an independent assessment of such SSC case.

It is required that the **SSC case proving safety, security and cybersecurity integrity**:

a) takes into account random failures and systematic failures and confirm the use of the safety features indicated in the standards [9÷13] as appropriate for the levels of safety integrity assigned to each technical solution according to the rules indicated in these standards and regulations;
b) comprises technical solutions ensuring functional completeness and adequacy of technical safety, life, health and property security, and cybersecurity in the event of failures and unauthorised interventions, including cyberattacks;
c) is subdivided into an analysis of the technical protection means associated with ensuring rolling stock safety proven in accordance with the requirements of chapter 4.1.2, and an analysis of the technical protection means associated with ensuring an adequate level of security for persons and property proven in accordance with the requirements of chapter 4.1.3.;
d) takes into account, for both technical protection means related to ensuring vehicle movement safety and technical protection means related to ensuring rolling stock security, protection against cyberthreats and proves them in accordance with the requirements of chapter 4.1.4;
e) determines the level of safety, security and cybersecurity integrity in accordance with the requirements of chapter 4.1.5.;
f) determines the passenger rolling stock digital safety index in accordance with the requirements of chapter 4.1.6.4.

Concept authors/designers (**contractors**) of the new rolling stock designs shall, together with the design, submit an **SSC case proving safety, security and cybersecurity integrity**, consistent with the proposed concept, unless the contract provisions, due to the nature of the concept, explicitly state that the development of the “rolling stock SSC case proving safety, security and cybersecurity integrity” is not required.

**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).

**SSC case proving safety, security and cybersecurity integrity** for the concept/design or rolling stock construction or rolling stock alternation/modification shall include following five chapters:

1. Chapter 1 - Introduction with definition of the system to be assessed
2. Chapter 2 - Analysis of the technical protection means associated with ensuring rolling stock safety (see subchapter 4.1.2.)
3. Chapter 3 - Analysis of the technical protection means associated with ensuring passengers security (see subchapter 4.1.3.)
4. Chapter 4 - Analysis of the protection means against cyberthreats (see subchapter 4.1.4.)
5. Chapter 5 - Determination of the level of safety, security and cybersecurity and their integrity level (see subchapters 4.1.5. and 4.1.6.)
6. Chapter 6 - Conclusion of the SSC case proving safety, security and cybersecurity integrity (see subchapter 4.1.7.)

System to be assessed i.e. the new railway vehicle to which the **SSC case proving safety, security and cybersecurity integrity** relates, shall be defined including functions, boundaries, and external interfaces of the system under assessment. The boundaries and interfaces of the system shall be taken into account in the development of subsequent chapters.

For each **SSC case proving safety, security and cybersecurity integrity** – for a specific type of the railway passenger rolling stock, the manufacturer or railway undertaking as the future user of the rolling stock shall obtain a positive independent assessment from a **competent independent inspection body** (see chapter 4.2. of this document).

### 4.1.2. Analysis of the technical protection means associated with ensuring safety of the rolling stock movements (Safety)

Analysis of the technical protection means associated with rolling stock impact on the railway traffic safety (Chapter 2 of the “rolling stock SSC case proving safety, security and cybersecurity integrity”) shall be based on the Reference Functional Model (hereafter RFM) provided in the chapter dedicated to safety and depictured in Figure 1.

In the RFM model, eight on-board functionalities, of a given rolling stock type, affecting railway traffic safety, were distinguished. At the same time, reference characteristics are defined for other eight complementary functionalities, which are provided on the infrastructure side by primary signalling systems and track-side control-command systems and devices. In that respect two generic principles are distinguished: the fail-safe (FS) principle and the SIL-4 principle, which imposes Safety Integrity Level 4 on electronic solutions in relation to both random failures and systematic failures. Mentioned above functionalities refer to the FS and SIL-4 principles, as well as to the primary signalling and control-command functionalities important from the rolling stock cybersecurity point of view.

These functionalities have been combined into following five groups:

RFM-G01 – Primary signalling – classic railway signalling (RFM-1.1 ÷ RFM-1.4),
RFM-G02 – CCT – control-command trackside systems and devices (RFM-2.1 ÷ RFM-2.4),
RFM-G03 – CCO – control-command on-board systems and devices (RFM-3.1 ÷ RFM-3.4),
RFM-G04 – DMI, communication, emergency calls (RFM-4.1 ÷ RFM-4.2),
RFM-G05 – GoA3/GoA4 functionalities – ATO, ATS (RFM-5.1 ÷ RFM-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,

Following issues, among others, were reflected in the form of questions grouped in the control sheets:

- 01 – separation of safety-relevant on-board data exchange from other on-board networks and systems,
- 02 – physical protection of the locations of the access points to the system (protection of the lowest - physical access layer),
- 03 – digital LAN network protection – separation of vehicle control systems from comfort systems (passenger information system, monitoring, ticketing, telephone charging, etc.),
- 04 – authorisation for employees (maintenance staff) having access to sensitive data,
- 05 - keeping a log of maintenance staff logs in to the system,
- 06 – protection of in-vehicle WiFi networks against external intervention (WPA security, one-way access),
- 07 – protection against unauthorised intervention in the operation of the drive and brake systems,
- 08 – protection against unauthorised generation of audible and visual signals in the driver's cab and unauthorised informing drivers by means of cab signals,
- 09 – providing voice radio connection, between trackside operational staff and on-board staff, specially between traffic controllers and train drivers, as well as possibility to generate safely emergency calls,
- 10 – providing voice (analogue audio link), between train driver and on-board staff, and between train driver and passenger using PEB (Passenger Emergency Brake), and the possibility to safely generate on-board emergency calls (voice information and infos on displays),
- 11 – Safe automated control of other on-board systems.

Chapter 2 of the “rolling stock SSC case proving safety, security and cybersecurity integrity” dedicated to the analysis of technical protection means associated with railway traffic safety, i.e. proper rolling stock construction in relation to the “safety” area, shall be subdivided into eight subchapters dedicated to functionalities 3.1 ÷ 3.4 and 4.1 ÷ 4.2 and 5.1 ÷ 5.2, so that the fields of the RFM model can be used to represent the level of safety, e.g. using grey tones or colours.

#### 4.1.3. Analysis of the technical protection means associated with ensuring security inside rolling stock (Security)

Analysis of the technical protection means associated with transport safety i.e. appropriate transport security (Chapter 3 of the “rolling stock SSC case proving safety, security and cybersecurity integrity”) shall be based on the **Reference Functional Model RFM** provided in the chapter dedicated to security and depictured in Figure 2.

In the RFM model, twenty on-board functionalities, of a given rolling stock type, affecting life, health and property security, were distinguished. These functionalities take into account both support for assistance in accidental cases involving individuals as well as protection in case of accumulation of threats and include risk prevention, mitigation, evacuation, rescue and securing the accident site.

These functionalities have been combined into following four groups:

- RFM-G06 – Passengers space and safety (RFM-6.1 ÷ RFM-6.6),
- RFM-G07 – Enabling vehicle movement (RFM-7.1 ÷ RFM-7.4),
- RFM-G08 – Vehicle movement control (RFM-8.1 ÷ RFM-8.4),
- RFM-G09 – Emergency systems and „entertainment” (RFM-9.1 ÷ RFM-9.6).

Following issues, among others, were reflected in the form of questions grouped in the control sheets:

- 01 – providing passenger information on-board of the rolling stock,
- 02 – ensuring fire protection in rolling stock,

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 na zewnątrz (np. peronów podczas wsiadania/wysiadania) 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.

03 – providing protection against emergency door activation,
04 – providing emergency medical equipment and equipment and systems supporting railway transport accessibility for persons with reduced mobility and wheelchair users,
05 – ensuring that assistance can be requested by provision of emergency call facilities and/or passenger emergency brake (PEB) installations,
06 – monitoring of external areas (e.g. platforms during access/egress) and vehicle interiors with video monitoring systems installed in rolling stock,
07 – providing protection of enclosed spaces against unauthorised access, including, in particular, access to the workplaces of those responsible for safety and driving the train.

Chapter 3 of the "rolling stock SSC case proving safety, security and cybersecurity integrity" dedicated to the analysis of technical protection means associated with providing transport security, i.e. proper rolling stock construction in relation to the "security" area, shall be subdivided into twenty subchapters dedicated to functionalities 6.1 ÷ 6.6 and 7.1 ÷ 7.4 and 8.1 ÷ 8.4 and 9.1 ÷ 9.6, so that the fields of the RFM model can be used to represent the level of safety, e.g. using grey tones or colours.

#### 4.1.4. Analysis of the protection means against cyberthreats

Both the technical protection means associated with rolling stock safety and the technical protection means associated with providing passenger security benefit from the storage, transmission and processing of data carried out by systems, subsystems and/or components having digital/software based nature, which are collectively referred to as digital systems/subsystems/components and the transmission systems that ensure the exchange of information between these systems/subsystems/components.

Chapter 4 of the "rolling stock SSC case proving safety, security and cybersecurity integrity" dedicated to the analysis of protection means against cyberthreats shall be subdivided into six following subchapters:

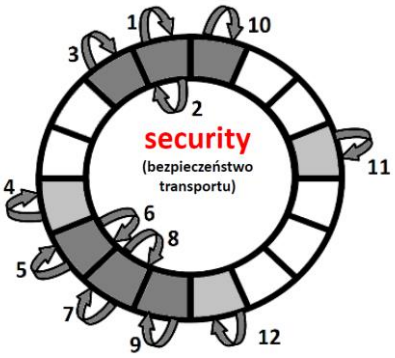
4.1 Description of the on-board structure of the digital systems/subsystems/components,
4.2 Storage and processing of traffic safety related data,
4.3. Storage and processing of transport security related data,
4.4. Exchange of traffic safety related data,
4.5. Exchange of transport security related data,
4.6. Utilising measures enhancing security of the networks and information systems for the purpose of the traffic safety related systems and transport security related systems.

Subsection 4.1 shall include and discuss block diagram showing all on-board digital systems/subsystems/components as well as transmission systems providing data exchange between them together with all links to wireless transmission systems for data exchange with trackside/infrastructure/ground systems. The proper identification of digital systems/sub¬sys¬tems/components and transmission systems are crucial to the proper application of cybersecurity related control sheets.

The subchapters dedicated to data storage and processing, subchapters 4.2. and 4.3., shall contain precise references to descriptions of the technical solutions. For technical protection means related to traffic safety (subchapter 4.2.) references to the descriptions in Chapter 2 of the '**SSC case proving safety, security and cybersecurity integrity'** and to the documents defining the technical solutions in details. For technical protection means related to ensuring transport security (subchapter 4.3.) references to the descriptions in Chapter 3 of the '**SSC case proving safety, security and cybersecurity integrity'** and to the documents defining the technical solutions in details. It is permissible to base these subchapters solely on references to the descriptions in chapters 1 and 2 of the '**SSC case proving safety, security and cybersecurity integrity'** and the documents defining the technical solutions in details.

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 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.

[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.

Subchapters dedicated to the exchange of data related to traffic safety and passenger security, subchapters 4.4. and 4.5. of the '**SSC case proving safety, security and cybersecurity integrity'** shall identify all transmission systems used for this purpose and take into account both the protection of the data against change during data exchange and the protection against data exchange impact on systems from which the data are taken. Subchapter 4.4 shall refer to the documents proving the proper application of EN 50159 [13], or explicitly include relevant evidences.

Transmission systems described in subchapters 4.4. and 4.5. of the '**SSC case proving safety, security and cybersecurity integrity'** shall be depicted on RFM models from chapters dedicated to traffic safety related technical protection means and transport security related technical protection means using block arrows, so that the arrow fields can be used to represent the level of security, e.g. using grey tones or colours. Next to each arrow representing transmission system, there shall be a reference, for example in the form of a number. An illustrative representation for data exchange supporting transport security is shown in Figure 5.

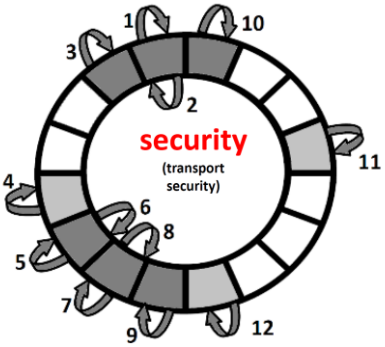



Figure 5. Example of the transmission systems visualisation
using a reference functional model
for technical protection means related to transport security
(source: own elaboration)

Subchapter 4.6 of the '**SSC case proving safety, security and cybersecurity integrity'** shall contain description how measures enhancing security of the networks and information systems are utilised to support traffic safety related systems and transport security related systems. All relevant relationships to the requirements of the Information Security Management System implemented by the Railway Undertaking in accordance with EN ISO/IEC 27001 [8] shall be included.[3)]

Particular attention should be paid to:
- user authentication,
- collecting data for monitoring and/or diagnostic purposes,
- creating and using backups of software and data.

### 4.1.5. Safety, security, and cybersecurity control sheets

Determination of the safety, security and cybersecurity integrity level for technical protection means related to traffic safety as well as for technical protection means related to transport security shall be based on control questions defined for groups of characteristics affecting traffic safety and groups of characteristics affecting transport security as well as for cybersecurity.

[3)] Directive EC 2022/2555 (NIS2) imposes, among other things, an obligation on railway undertakings to implement Information Security Management Systems (ISMS), the requirements for which are defined in the EN ISO/IEC 27001 standard.

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 3.4. 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.

Following principles apply for the purposes of determining the levels of safety, security and cybersecurity and the level of their integrity:

- control questions are defined for individual characteristics; the answers have assigned values of “0” or “1” for knock-out questions and “1” or “2” for the questions which are differentiating the technical solutions,
- the value “0” is assigned when the answer indicates that safety or security or cybersecurity is not provided in a manner consistent with the threats that are known to exist and that technical solutions are not only possible but also widely used, the non-application of which results in significant safety or security deficiencies,
- the value “1” is assigned when the answer indicates that safety or security or cybersecurity is provided in a manner that corresponds to the threats that are known to exist and that technical solutions that substantially minimise such threats are not only possible but widely implemented,
- the value “2” is assigned when the answer indicates that safety or security or cybersecurity is ensured in the best manner available at the time,
- the reference values for the individual characteristics are determined as products of the values assigned to the answers to the individual control questions,
- aggregate reference values for groups of functionalities are determined as products of the reference values for individual characteristics,
- aggregate reference values for safety, security and cybersecurity are determined as products of the aggregate reference values of the appropriate groups of functionalities.

Control questions are grouped into fourteen control sheets – two reference sheets, three sheets for safety, four sheets for security and five sheets for cybersecurity that is, two reference sheets and twelve sheets to assess the safety, security and cybersecurity of a type of railway rolling stock and to assess its safety, security and cybersecurity functional integrity.

NOTE: The purpose of the control sheets is not to verify all the requirements for new rolling stock. As stated in Chapter 3.4. and in accordance with the applicable legislation, the essential requirements are fully confirmed at the Rolling Stock subsystem and Control-Command and Signalling On-board subsystem level by the EC certificates of verification and EC declarations of verification, and for the relevant parts, at the product level, for products which gain by law status of the Interoperability Constituents, with EC certificates of conformity and EC declarations of conformity. Control sheets, on the other hand, take into account requirements for digital solutions that have an impact on the safety, security and cybersecurity integrity of the railway system and take into account rolling stock equipment. At the same time, it shall be noted that the assessment of the safety, security and cybersecurity integrity for new passenger rolling stock, which, according to the provisions of this document, is to be carried out taking into account the requirements of the Regulation on risk evaluation and assessment [6, 7], does not exhaust the scope of application of risk evaluation and assessment for new passenger rolling stock, because this, according to the applicable law, shall be applied to all technical, operational and organisational changes affecting safety.

#### 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**<br>funkcjonalności przytorowych systemów sterowania od kontroli niezajętości do wyświetlania obrazów sygnałowych na sygnalizatorach świetlnych (RMF-1.1 ÷ RMF-1.4) |
|---|
| **Założenia:**<br>1. Infrastruktura torowa podzielona jest na odstępy, na których co do zasady w normalnych warunkach eksploatacyjnych powinien w danym czasie znajdować się maksymalnie jeden pociąg.<br>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?<br>TAK = 1, NIE = 0 | Ad. 1 ➔ 1 |
| 2. Czy wszystkie zastosowane rozwiązania techniczne stosują zasadę FS? (Czy możliwe uszkodzenia modułów prowadzą do zgłaszania zajętości?)<br>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?)<br>TAK = 1, NIE = 0, NIE, ale system jest w pełni analogowy = 1 | Ad. 3 ➔ 1<br><br>Iloczyn odpowiedzi ➔ 1 |
| **RMF-1.2** | |
| 1. Czy wszystkie zastosowane rozwiązania techniczne stosują zasadę FS? (Czy możliwe uszkodzenia modułów prowadzą do stanów bezpiecznych?)<br>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?)<br>TAK = 1, NIE = 0 | Ad. 1. ➔ 1 |
| **RMF-1.4** | |
| 1. Czy wszystkie odstępy (ew. grupy odstępów) są osłonięte sygnalizatorami?<br>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?)<br>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?)<br>TAK = 1, NIE = 0, NIE, ale system jest w pełni analogowy = 1 | Ad. 3. ➔ 1<br><br>Iloczyn odpowiedzi: ➔ 1 |
| **Zbiorcza wartość referencyjna dla grupy RMF-G01**<br>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.

--- --- ---

#### 4.1.5.1. Reference infrastructure control sheets

These control sheets provide reference values assigned to the answers, which represent the reference infrastructure in terms of its railway traffic safety related systems and devices. The assigned reference values of "1" ensure that rolling stock manufacturers/suppliers are not responsible for the condition and equipment of the infrastructure on which railway passenger rolling stock will be operated.

| **Reference safety control sheet RFM-G01**<br>functionalities of the primary signalling, from track and turnout occupancy detection systems to the display of appropriate aspects on the colour light signals (RFM-1.1 ÷ RFM-1.4) | |
|---|---|
| **Assumptions:**<br>1. The track infrastructure is subdivided into sections where, in principle under normal operating conditions, not more than one train shall be present at one section at a time.<br>2. Traffic control is implemented under the supervision of signalling equipment (interlocking and/or line block system and/or shunting control system). | |
| **Control questions** | **Ref. values** |
| **RFM-1.1** | |
| 1. Are all tracks along their entire length covered by the occupancy detection system?<br>YES = 1, NO = 0 | Ad. 1 ➔ 1 |
| 2. Do all the technical solutions, which are used, apply the FS principle?<br>(Do potential module failures lead to occupancy reporting?)<br>YES = 1, NO = 0 | Ad. 2 ➔ 1 |
| 3. Do all the technical solutions used apply the SIL-4 principle?<br>(Are there reliable safety cases available for specific applications confirming SIL-4, verified by an independent safety assessors?)<br>YES = 1, NO = 0, NO, but system is fully analogue = 1 | Ad. 3 ➔ 1<br><br>Product of the answers: ➔ 1 |
| **RFM-1.2** | |
| 1. Do all the technical solutions, which are used, apply the FS principle?<br>(Do potential module failures lead to safe conditions?)<br>YES = 1, NO = 0 | Ad. 1 ➔ 1 |
| **RFM-1.3** | |
| 1. Do all the technical solutions, which are used, apply the SIL-4 principle?<br>(Are there reliable safety cases available for the specific applications confirming SIL-4, verified by independent safety assessors?)<br>YES = 1, NO = 0 | Ad. 1. ➔ 1 |
| **RFM-1.4** | |
| 1. Are all the sections (or groups of sections) covered by signals?<br>YES = 1, NO = 0, NO, but the on-board CCS system was used = 1 | Ad. 1 ➔ 1 |
| 2. Do all the technical solutions, which are used, apply the FS principle?<br>(Do potential module failures lead to safe conditions?)<br>YES = 1, NO = 0 | Ad. 2. ➔ 1 |
| 3. Do all the technical solutions, which are used, apply the SIL-4 principle?<br>(Are there reliable safety cases available for the specific applications confirming SIL-4, verified by independent safety assessors?)<br>YES = 1, NO = 0, NO, but system is fully analogue = 1 | Ad. 3. ➔ 1<br><br>Product of the answers: ➔ 1 |
| **Aggregate reference value for the group RFM-G01**<br>product of the reference values RFM-1.1 ÷ RFM-1.4 | **1** |

NOTE: in case of vehicles intended to run under the control of a control-command system in an operational mode based on moving block principle, it is not required that the tracks on which movement is/will take place in such mode are covered by occupancy checking systems formed by track circuits and/or axle counters. In such case occupancy checking is carried out within trains spacing management system using position data and possibly speed data of the individual trains. In existing systems this function is performed on the infrastructure side.

--- --- ---

| **Referencyjna karta kontrolna bezpieczeństwa RMF-G02**<br>funkcjonalności przytorowych urządzeń systemów bezpiecznej kontroli jazdy pociągu od obrazów sygnałowych do wysyłania elektronicznych zezwoleń ZnJ (RMF-2.1 ÷ RMF-2.4) |
|---|
| **Założenia:**<br>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?<br>TAK = 1, NIE = 0 | Ad. 1 ➔ 1 |
| 2. Czy wszystkie zastosowane rozwiązania techniczne stosują zasadę FS? (Czy możliwe uszkodzenia modułów prowadzą do stanów bezpiecznych?)<br>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?)<br>TAK = 1, NIE = 0, NIE, ale system jest w pełni analogowy = 1 | Ad. 3 ➔ 1<br><br>Iloczyn odpowiedzi ➔ 1 |
| **RMF-2.2** | |
| 1. Czy wszystkie systemy przetwarzania danych źródłowych definiujące ZnJ w pełnym zakresie stosują zasadę FS?<br>(Czy możliwe uszkodzenia modułów prowadzą do stanów bezpiecznych?)<br>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?<br>(Czy dostępne są wiarygodne dowody bezpieczeństwa dla aplikacji potwierdzające SIL-4, zweryfikowane przez niezależnego audytora?)<br>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?<br>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)?<br>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)?<br>TAK = 1, NIE = 0 | Ad. 3 ➔ 1<br>Iloczyn odpowiedzi ➔ 1 |
| **Zbiorcza wartość referencyjna dla grupy RMF-G02**<br>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.

--- --- ---

| **Reference safety control sheet RFM-G02**<br>functionalities of the trackside control command installations, from signal aspects to transmission of the electronic Movement Authorities MAs (RFM-2.1 ÷ RFM-2.4) |
|---|
| **Assumptions:**<br>1. The control command installation utilises ATP or ATC system. |

| **Control questions** | **Ref. values** |
|---|---|
| **RFM-2.1** | |
| 1. Has it been confirmed that taking source data for MAs from primary signalling does not affect operation of the primary signalling systems even under failure conditions?<br>YES = 1, NO = 0 | Ad. 1 ➔ 1 |
| 2. Do all the technical solutions, which are used, apply the FS principle?<br>(Do potential module failures lead to safe conditions?)<br>YES = 1, NO = 0 | Ad. 2 ➔ 1 |
| 3. Do all the technical solutions, which are used, apply the SIL-4 principle?<br>(Are there reliable safety cases available for the specific applications confirming SIL-4, verified by independent safety assessors?)<br>YES = 1, NO = 0, NO, but system is fully analogue = 1 | Ad. 3 ➔ 1<br><br>Product of the answers: ➔ 1 |
| **RFM-2.2** | |
| 1. Do all source data processing systems defining MAs fully apply the FS principle?<br>(Do potential module failures lead to safe conditions?)<br>YES = 1, NO = 0 | Ad. 1 ➔ 1 |
| **RFM-2.3** | |
| 1. Do all source data processing systems defining MAs fully apply the SIL-4 principle?<br>(Are there reliable safety cases available for the specific applications confirming SIL-4, verified by independent safety assessors?)<br>YES = 1, NO = 0 | Ad. 1 ➔ 1 |
| **RFM-2.4** | |
| 1. Do the MAs, which are sent, contain data that allow identification of a sender and identification of the receiver – is the transmission system a closed system?<br>YES = 1, NO = 0 | Ad. 1 ➔ 1 |
| 2. Do the MAs, which are sent, contain data necessary to verify MAs validity (e.g. request time and transmission time or common time stamp)?<br>YES = 1, NO = 0 | Ad. 2 ➔ 1 |
| 3. Do the MAs, which are sent, contain data that allow the data completeness and consistency to be verified (e.g. checksums, Hamming codes)?<br>YES = 1, NO = 0 | Ad. 3 ➔ 1<br>Product of the answers: ➔ 1 |
| **Aggregate reference value for the group RFM-G02**<br>product of the reference values RFM-2.1 ÷ RFM-2.4 | **1** |

NOTE: MA (plural MAs) stands for electronic Movement Authority, i.e. digital information sent by wireless transmission from the track to the train, on the basis of which, firstly, driving restrictions are displayed on the driver's desk and, secondly, electronic supervision of compliance with these restrictions is carried out.

--- --- ---

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

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**<br>funkcjonalności pokładowych urządzeń systemów bezpiecznej kontroli jazdy pociągu<br>od odebrania zezwolenia ZnJ do interwencyjnego wdrażania hamowania (RMF-3.1 ÷ RMF-3.4) |
|---|
| **Założenia:**<br>1. Bezpieczna kontrola jazdy pociągu wykorzystuje system klasy ATP lub ATC. |

| Pytania kontrolne | Wartości ref. |
|---|---|
| **RMF-3.1**<br>1. Czy wszystkie człony trakcyjne pasażerskiego taboru trakcyjnego danego typu są wyposażone w system automatycznego sterowania pociągiem ATC?<br>TAK = 1, NIE = 0<br>2. Czy pokładowe instalacje ATC stosują zasadę FS? (Czy możliwe uszkodzenia modułów prowadzą do stanów bezpiecznych?)<br>TAK = 1, NIE = 0<br>3. Czy pokładowe instalacje ATC stosują zasadę SIL-4? (Czy dostępne są wiarygodne dowody bezpieczeństwa dla aplikacji potwierdzające SIL-4, zweryfikowane przez niezależnego audytora?)<br>TAK = 1, NIE = 0<br>4. Czy odbierane ZnJ podlegają uwierzytelnieniu poprzez sprawdzenie identyfikatorów nadawcy/odbiorcy oraz weryfikację ważności ZnJ (np. czas żądania/czas nadania lub stempel czasu wspólnego)?<br>TAK = 1, NIE = 0<br>5. Czy odbierane ZnJ zawierają dane pozwalające na weryfikację kompletności oraz spójności danych (np. sumy kontrolne, kody hamminga) i podlegają weryfikacji kompletności oraz spójności?<br>TAK = 1, NIE = 0<br>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?<br>TAK = 1, NIE = 0<br>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]<br>7. Czy system radiowej transmisji ZnJ jest zgodny z dokumentami narzuconymi prawem w zakresie zabezpieczenia przed zakłóceniami i atakami?<br>TAK = 1, NIE = 0 | Iloczyn odpowiedzi:<br>0 lub 1 |
| **RMF-3.2**<br>1. Czy dla pomiaru drogi od punktu referencyjnego określany jest maksymalny błąd przeszacowania i czy jest on odejmowany od zmierzonej wartości?<br>TAK = 1, NIE = 0<br>2. Czy dla pomiaru prędkości określany jest maksymalny błąd niedoszacowania i czy jest on dodawany do zmierzonej wartości?<br>TAK = 1, NIE = 0<br>3. Czy zastosowane rozwiązania techniczne stosują zasadę SIL-4?<br>TAK = 1, NIE = 0 | Iloczyn odpowiedzi:<br>0 lub 1 |
| **RMF-3.3**<br>1. Czy wszystkie zastosowane rozwiązania techniczne BKJP stosują zasadę FS? (Czy możliwe uszkodzenia modułów prowadzą do stanów bezpiecznych?)<br>TAK = 1, NIE = 0<br>**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?)<br>TAK = 1, NIE = 0, NIE, ale system jest w pełni analogowy = 1 | Iloczyn odpowiedzi:<br>0 lub 1 |

#### 4.1.5.2. Control sheets for rolling stock type assessment regarding on-board control-command equipment providing railway traffic safety (safety sheets)

These control sheets shall be completed, for the type of the rolling stock, which is under consideration, by assigning values to the answers according to the templates. It is underlined that the SSC case proving safety, security and cybersecurity integrity shall include all information necessary to verify the answers. Relevant data may be included in full in the SSC case, and can also be partly based on referenced documents, which then shall be made available to the body assessing SSC case.

| **Safety control sheet RFM-G03**<br>functionalities of the on-board control command installations, from receiving electronic movement authorities MAs to automatic braking interventions (RFM-3.1 ÷ RFM-3.4) |
|---|
| **Assumptions:**<br>1. The control command installation utilises ATP or ATC system. |

| Control questions | Ref. values |
|---|---|
| **RFM-3.1**<br>1. Are all traction units, of the passenger rolling stock of a given type, equipped with an Automatic Train Control system ATC?<br>YES = 1, NO = 0<br>2. Do on-board ATC installations apply the FS principle?<br>(Do potential module failures lead to safe conditions?)<br>YES = 1, NO = 0<br>3. Do on-board ATC installations apply the SIL-4 principle?<br>(Are there reliable safety cases available for the specific applications confirming SIL-4, verified by independent safety assessors?)<br>YES = 1, NO = 0<br>4. Are the MAs, which are received, subject to authentication by checking sender/receiver identifiers and verification of the validity of the MAs (e.g. request time and transmission time or common time stamp)?<br>YES = 1, NO = 0<br>5. Do the MAs, which are received, contain data that allow the data completeness and consistency to be verified (e.g. checksums, Hamming codes) and are subject to completeness and consistency verification?<br>YES = 1, NO = 0<br>6. Is the MA transmission system a closed system in accordance with the definition in the EN 50159:2011 standard or an open system, but secured in accordance with the requirements of this standard?<br>YES = 1, NO = 0<br>NOTE: Adequate protection of the MA transmission system shall be included and confirmed in the safety case of the on-board control-command system developed and accepted in accordance with RAMS standards [9÷13]<br>7. Does the MA radio transmission system comply with the documents imposed by law with regard to protection against interference and attacks?<br>YES = 1, NO = 0 | Product of the answers:<br>0 or 1 |
| **RFM-3.2**<br>1. Is a maximum overestimation error defined for the distance measurement from the reference point and is it subtracted from the measured value?<br>YES = 1, NO = 0<br>2. Is a maximum underestimation error defined for the speed measurement and is it added to the measured value?<br>YES = 1, NO = 0<br>3. Do all the technical solutions used apply the SIL-4 principle?<br>YES = 1, NO = 0 | Product of the answers:<br>0 or 1 |
| **RFM-3.3**<br>1. Do all the technical solutions of the on-board CC system used apply the FS principle?<br>(Do potential module failures lead to safe conditions?)<br>YES = 1, NO = 0<br>**2.** Do all the technical solutions of the on-board CCS system apply the SIL-4 principle?<br>(Are there reliable safety cases available for the specific applications confirming SIL-4, verified by independent safety assessors?)<br>YES = 1, NO = 0, NO, but system is fully analogue = 1 | Product of the answers:<br>0 or 1 |

| | |
|---|---|
| **RMF-3.4**<br>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?)<br>TAK = 1, NIE = 0<br>2. Czy automatyczne wdrażanie hamowania interwencyjnego uwzględnia więcej niż jeden tryb hamowania interwencyjnego (hamowanie służbowe i hamowanie nagłe)?<br>TAK = 2, NIE = 1<br>3. Czy określana jest i sygnalizowana maszyniście lokalizacja, gdzie najpóźniej należy rozpocząć hamowanie dla odpowiedniego zmniejszenia prędkości przed ograniczeniem prędkości?<br>TAK = 2, NIE = 1<br>4. Czy jest możliwe wykrycie dysfunkcji układu hamulcowego w trakcji ukrotnionej?<br>TAK = 1, NIE = 0 | Iloczyn odpowiedzi:<br>0 lub 1 lub 2 lub 4 |
| **Zbiorcza wartość referencyjna dla grupy RMF-G03**<br>iloczyn wartości referencyjnych RMF-3.1 ÷ RMF-3.4 | 0 lub 1 lub 2 lub 4 |

--- --- ---

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

| Pytania kontrolne | Wartości ref. |
|---|---|
| **RMF-4.1**<br>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?<br>TAK = 1, NIE = 0<br>2. Czy wszystkie systemy AWS generujące sygnały ostrzegawcze (dźwiękowe i/lub wizualne) w kabinie maszynisty stosują zasadę FS?<br>(Czy możliwe uszkodzenia modułów prowadzą do stanów bezpiecznych?)<br>TAK = 1, NIE = 0<br>3. Czy eksploatowany system bezpiecznej kontroli jazdy pociągu klasy ATC prezentuje ZnJ na pulpicie w kabinie maszynisty?<br>TAK = 1, NIE = 0<br>UWAGA: jeśli system BKJP klasy ATC nie jest ani wymagany ani zastosowany, należy przyjąć wartość „1”. | Iloczyn odpowiedzi:<br>0 lub 1 |
| **RMF-4.2**<br>1. Czy zapewnione jest głosowe połączenie radiowe między maszynistą i dyżurnym ruchu (ew. dyspozytorem)?<br>TAK = 1, NIE = 0<br>2. Czy zastosowano zabezpieczenia przed możliwością nieuprawnionej cyfrowej ingerencji (włączenia się) w łączność głosową między maszynistą i dyżurnym ruchu (ew. dyspozytorem)?<br>TAK = 1, NIE = 0<br>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.<br>3. Czy zapewniona jest możliwość generowania sygnałów alarmowych przez maszynistów i odbierania sygnałów alarmowych generowanych przez maszynistów i dyżurnych ruchu?<br>TAK = 1, NIE = 0<br>4. Czy odebranie sygnału alarmowego przez pojazd powoduje automatyczne wdrożenie hamowania i zatrzymanie w miejscu, gdzie możliwa jest ewakuacja względnie działania służb ratunkowych?<br>TAK = 2, NIE = 1 | Iloczyn odpowiedzi:<br>0 lub 1 lub 2 |
| **Zbiorcza wartość referencyjna dla grupy RMF-G04**<br>iloczyn wartości referencyjnych RMF-4.1 ÷ RMF-4.2 | 0 lub 1 lub 2 |

--- --- ---

| | |
|---|---|
| **RFM-3.4**<br>5. Do automatic emergency braking initiation systems apply the SIL-4 principle? (Are there reliable safety cases available for the specific applications confirming SIL-4, verified by independent safety assessors?)<br>YES = 1, NO = 0<br>6. Do automatic emergency braking initiation systems foresee more than one braking intervention mode (full service braking and emergency braking)?<br>YES = 2, NO = 1<br>7. Is the location determined and communicated to the driver, where braking shall be initiated at the latest for adequate speed reduction before the speed limit?<br>YES = 2, NO = 1<br>8. Is it possible to detect braking system malfunctioning in case of multiple traction operation?<br>YES = 1, NO = 0 | Product of the answers:<br>0 or 1 or 2 or 4 |
| **Aggregate reference value for the group RFM-G03**<br>product of the reference values RFM-3.1 ÷ RFM-3.4 | 0 or 1 or 2 or 4 |

--- --- ---

| **Safety control sheet RFM-G04**<br>functionalities supporting manual train operation by drivers based on aspects on colour light signals and voice radio communication (RFM-4.1 ÷ RFM-4.2) | |
|---|---|
| **Assumptions:**<br>1. Trains are operated by train drivers.<br>2. Operational voice communication is provided. | |
| **Control questions** | **Ref. values** |
| **RFM-4.1**<br>1. Are all traction units of the passenger rolling stock of a given type equipped with all warning systems (AWS class systems) necessary to warn drivers when they are approaching hazardous locations, compatible with the trackside installations on the infrastructures over which the rolling stock will normally run?<br>YES = 1, NO = 0<br>2. Do all AWS class devices generating warning signals (audible and visual) in the driver's cab apply the FS principle?<br>(Do potential module failures lead to safe conditions?)<br>YES = 1, NO = 0<br>3. Does the on-board ATC class system display MAs on the driver's desk in the driver's cab?<br>YES = 1, NO = 0<br>NOTE: if on-board ATC class CC system is neither applied nor required, assume value "1". | Product of the answers:<br>0 or 1 |
| **RFM-4.2**<br>1. Is there voice radio communication between the driver and the traffic controller (or the dispatcher)?<br>YES = 1, NO = 0<br>2. Are protection means in place to prevent unauthorised digital intervention (breach) into voice communication between the driver and the traffic controller (or dispatcher)?<br>YES = 1, NO = 0<br>NOTE: If the communication system between the driver and the traffic controller is fully analogue system, the value '1' shall be taken due to the lack of possibility of a cyberattack, which does not mean that the installation of communication systems shall not be protected against other attacks, e.g. physical attacks.<br>3. Is it ensured that drivers could generate alarm signals and receive alarm signals generated by drivers and traffic controllers?<br>YES = 1, NO = 0<br>4. Does the reception of an emergency signal by a vehicle automatically trigger braking and bring the vehicle to a stop where evacuation or rescue operations are possible?<br>YES = 2, NO = 1 | Product of the answers:<br>0 or 1 |
| **Aggregate reference value for the group RFM-G04**<br>product of the reference values RFM-4.1 ÷ RFM-4.2 | 0 or 1 or 2 |

--- --- ---

| **Karta kontrolna bezpieczeństwa RMF-GB-05**<br>funkcjonalności automatycznego prowadzenia pociągu zastępujące maszynistę<br>w przyspieszaniu i hamowaniu oraz obsłudze innych urządzeń pokładowych<br>i synchronizacji pracy drzwi pokładowych i peronowych (RMF-5.1 ÷ RMF-5.2) | |
|---|---|
| **Założenia:**<br>1. Pociągi prowadzone są przez systemy klasy ATO.<br>2. Ruch pociągów jest nadzorowany przez systemy klasy ATS. | |
| **Pytania kontrolne** | **Wartości ref.** |
| **RMF-5.1**<br>1. Czy wszystkie człony trakcyjne pasażerskiego taboru kolejowego ocenianego typu są wyposażone w systemy klasy ATO?<br>TAK = 1, NIE = 0<br>2. Czy systemy ATO zapewniają bezpieczne automatyczne ograniczanie prędkości do zera oraz automatycznym ograniczaniem prędkości do wartości ograniczeń przed miejscami ograniczeń prędkości?<br>TAK = 1, NIE = 0<br>3. Czy systemy ATO zapewniają bezpieczne automatyczne rozpoczynanie jazdy oraz automatyczne zwiększanie prędkości do wartości dopuszczalnej zgodnie z ograniczeniami infrastrukturalnymi?<br>TAK = 1, NIE = 0<br>4. Czy zastosowane systemy klasy ATO same lub w powiązaniu z innymi urządzeniami pokładowymi zapewniają bezpieczne sterowanie prędkością pociągu zgodnie z zasadami FS oraz SIL-4?<br>(Czy dostępne są wiarygodne dowody bezpieczeństwa dla aplikacji potwierdzające SIL-4, zweryfikowane przez niezależnego audytora?)<br>TAK = 1, NIE = 0 | Iloczyn odpowiedzi:<br>0 lub 1 |
| **RMF-5.2**<br>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?<br>TAK = 1, NIE = 0<br>NOTE: 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.<br>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)?<br>TAK = 1, NIE = 0<br>NOTE: 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.<br>**3.** Czy zapewniona jest bezpieczna wymiana danych dla bezpiecznego automatycznego sterowania drzwiami peronowymi w synchronizacji z drzwiami pokładowymi?<br>TAK = 1, NIE = 0 | Iloczyn odpowiedzi:<br>0 lub 1 |
| **Zbiorcza wartość referencyjna dla grupy RMF-G5**<br>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.

| **Safety control sheet RFM-GB-05**<br>automatic train operation functionality replacing the driver in acceleration and deceleration and operating other on-board equipment and platform doors (RFM-5.1 ÷ RFM-5.2) | |
|---|---|
| **Assumptions:**<br>3. Trains are operated by ATO class systems.<br>4. Train traffic is supervised by ATS class systems. | |
| **Control questions** | **Ref. values** |
| **RFM-5.1**<br>1. Are all traction units of a passenger rolling stock of a type under consideration equipped with ATO class systems?<br>YES = 1, NO = 0<br>2. Do the ATO class systems ensure safe automatic speed limitation to zero and automatic speed limitation to the limit before speed limit locations?<br>YES = 1, NO = 0<br>3. Do the ATO class systems ensure safe automatic start-up and automatic speed increase to the speed limit in accordance with infrastructure constraints?<br>YES = 1, NO = 0<br>4. Do the ATO class systems alone or in combination with other on-board equipment ensure safe speed control of train according to the FS and SIL-4 principles?<br>(Are there reliable safety cases available for the applications confirming SIL-4, verified by independent safety assessors?)<br>YES = 1, NO = 0 | Product of the answers:<br>0 or 1 |
| **RFM-5.2**<br>1. Do the ATO systems implement all required functionalities of the GoA3 (Grade of Automation GoA3 for Driverless Train Operation DTO) as indicated in the IEC 62267:2009-07, including automatic control of on-board auxiliary equipment such as current collection systems or external doors?<br>YES = 1, NO = 0<br>NOTE: The standard also defines additional functionalities for GoA4 (Grade of Automation required for Unattended Train Operation UTO). Relevant functionalities may be required for a given type of the railway passenger rolling stock.<br>2. Do the on-board ATO systems ensure data exchange with track-side ATS class system covering all data necessary to ensure supervision of autonomous driving to the extent appropriate for the level of automation (GoA3 or GoA4)?<br>YES = 1, NO = 0<br>NOTE: Autonomous operation takes place under the supervision of an ATS class system, which can be operated by dispatcher or autonomous. The ATS system remains outside the rolling stock assessment, but data exchange between the autonomous vehicle and the ATS class system shall be included in the rolling stock safety assessment.<br>**3.** Is there a secured data exchange provided for safe automatic control of platform doors in synchronisation with on-board doors??<br>YES = 1, NO = 0 | Product of the answers:<br>0 or 1 |
| **Aggregate reference value for the group RFM-G5**<br>product of the reference values RFM-5.1 ÷ RFM-5.2 | 0 or 1 |

--- --- ---

### 4.1.5.3. Control sheets for passenger rolling stock type assessment in relation to transport security (security sheets)

These control sheets shall be completed for the type of the rolling stock, which is under consideration, by assigning values to the answers according to the templates. It is underlined that the SSC case proving safety, security and cybersecurity integrity shall include all information necessary to verify the answers. Relevant data may be included in full in the SSC case, and can also be partly based on referenced documents, which then shall be made available to the body assessing SSC case.

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

| Pytania kontrolne | Wartości ref. |
|---|---|
| **RMF-6.1**<br>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?<br>TAK = 1, NIE = 0<br>2. Czy drzwi zewnętrzne dla pasażerów w pojeździe objęte są monitoringiem wizyjnym?<br>TAK = 1, NIE = 0<br>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?<br>TAK = 1, NIE = 0<br>4. Czy zastosowane jest fizyczne zabezpieczenie przed ingerencją w systemy sterowania drzwiami wewnętrznymi?<br>TAK = 1, NIE = 0 | Iloczyn odpowiedzi:<br>0 lub 1 |
| **RMF-6.2**<br>1. Czy wszystkie przestrzenie, w których w normalnych warunkach eksploatacji mogą znajdować się pasażerowie wyposażone są w systemy ogrzewania, wentylacji i klimatyzacji?<br>TAK = 1, NIE = 0<br>2. Czy zastosowane jest fizyczne zabezpieczenie przed możliwością ingerencji zewnętrznej w system ogrzewania?<br>TAK = 1, NIE = 0<br>3. Czy zastosowane jest fizyczne zabezpieczenie przed możliwością ingerencji zewnętrznej w system wentylacji?<br>TAK = 1, NIE = 0<br>4. Czy istnieje zabezpieczenie przed możliwością ingerencji zewnętrznej w system klimatyzacji?<br>TAK = 1, NIE = 0 | Iloczyn odpowiedzi:<br>0 lub 1 |
| **RMF-6.3**<br>1. Czy wszystkie przestrzenie w których w normalnych warunkach eksploatacji mogą znajdować się pasażerowie wyposażone są w systemy oświetlenia?<br>TAK = 1, NIE = 0<br>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?<br>TAK = 1, NIE = 0<br>3. Czy zastosowane jest fizyczne zabezpieczenie przed możliwością ingerencji zewnętrznej w system oświetlenia oraz system oświetlenia awaryjnego (jeśli został zastosowany)?<br>TAK = 1, NIE = 0 | Iloczyn odpowiedzi:<br>0 lub 1 |
| **RMF-6.4**<br>1. Czy monitoring wizyjny obejmuje wszystkie obszary dostępne dla pasażerów w normalnych warunkach eksploatacyjnych?<br>TAK = 1, NIE = 0<br>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?<br>TAK = 1, NIE = 0<br>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?<br>TAK = 2, NIE = 1 | Iloczyn odpowiedzi:<br>0 lub 1 lub 2 |

| **Security control sheet RFM-G06**<br>functionalities for ensuring a minimum level of<br>personal safety (RFM-6.1 ÷ RFM-6.6) |
|---|
| **Assumptions:**<br>A minimum level of safety for persons shall be ensured in the areas accessible to passengers. |

| Control questions | Ref. values |
|---|---|
| **RFM-6.1**<br>1. Is there a physical protection against the possibility of intervention in the external door controllers (and movable egress steps, if any), and against intervention in the processing of the stay-in-standstill signal, which may result in the doors opening themselves while the train is running, or starting to run with the doors being open?<br>YES = 1, NO = 0<br>2. Are the external passenger doors of the vehicle subject to video surveillance?<br>YES = 1, NO = 0<br>3. Are both external and internal passenger doors equipped with a door occupancy detection system that locks the doors when a passenger is present?<br>YES = 1, NO = 0<br>4. Is there a physical protection against the possibility of intervention in the internal door controllers?<br>YES = 1, NO = 0 | Product of the answers:<br>0 or 1 |
| **RFM-6.2**<br>1. Are all areas, where passengers are allowed to be present under normal operating conditions, equipped with heating, ventilation and air-conditioning systems?<br>YES = 1, NO = 0<br>2. Is there a physical protection against the possibility of external intervention in the heating system?<br>YES = 1, NO = 0<br>3. Is there a physical protection against the possibility of external intervention in the ventilation system?<br>YES = 1, NO = 0<br>4. Is there a physical protection against the possibility of external intervention in the air-conditioning system?<br>YES = 1, NO = 0 | Product of the answers:<br>0 or 1 |
| **RFM-6.3**<br>1. Are all areas, where passengers are allowed to be present under normal operating conditions, equipped with lighting systems?<br>YES = 1, NO = 0<br>2. Are all areas, where passengers are allowed to be present under normal operating conditions, equipped with emergency lighting systems, if the passenger rolling stock of a given type is intended to run in tunnels?<br>YES = 1, NO = 0<br>3. Is there a physical protection against the possibility of external intervention in the lighting systems and emergency lighting systems (if available)?<br>YES = 1, NO = 0 | Product of the answers:<br>0 or 1 |
| **RFM-6.4**<br>1. Does the video surveillance cover all areas, which are accessible for passengers under normal operating conditions?<br>YES = 1, NO = 0<br>2. Is there a physical protection against the possibility of external intervention in the video surveillance system, including possibility to deactivate video and audio recording and/or to delete recorded material?<br>YES = 1, NO = 0<br>3. Is the video surveillance system equipped with video stream analysis functionalities to identify dangerous situations and automatically inform the on-board staff, e.g. the train manager and/or security services?<br>YES = 2, NO = 1 | Product of the answers:<br>0 or 1 or 2 |

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

--- --- ---

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

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

| | |
|---|---|
| **RFM-6.5**<br>3. Is there a physical protection against the possibility of external intervention in the toilets doors controllers?<br>YES = 1, NO = 0<br>4. Is there a physical protection against the possibility of external intervention in the toilet compartments call for aid devices?<br>YES = 1, NO = 0 | Product of the answers:<br>0 or 1 |
| **RFM-6.6**<br>1. Is there a visual passenger information provided in the passenger areas of the vehicle?<br>YES = 1, NO = 0<br>2. Is there a spoken passenger information provided in the passenger areas of the vehicle?<br>YES = 1, NO = 0<br>3. Is there a physical protection against the possibility of external intervention in the passenger information systems in the vehicle areas accessible for passengers?<br>YES = 1, NO = 0<br>4. Are there passenger safety aids available in suitable types, quantities and locations for the intended use of the vehicle?<br>YES = 1, NO = 0<br>NOTE: As a minimum, the following shall be included: emergency door-opening systems, emergency driver/on-board staff notification systems (call for assistance) and passenger emergency braking systems.<br>5. Is there a physical protection against intervention in the systems referred to in point 4 above, to prevent them being operated and/or to cut-off communication with relevant staff?<br>YES = 1, NO = 0 | Product of the answers:<br>0 or 1 |
| **Aggregate reference value for the group RFM-G06**<br>product of the reference values RFM-6.1 ÷ RFM-6.6 | 0 or 1 or 2 |

--- --- ---

| **Security control sheet RFM-G07**<br>vehicle movement functionalities (RFM-7.1 ÷ RFM-7.4) |
|---|
| **Assumptions:**<br>Safe movement of the vehicle shall be ensured. |

| **Control questions** | **Ref. values** |
|---|---|
| **RFM-7.1**<br>1. Is there a safe automatic control of on-board current collectors (pantographs) provided?<br>YES = 1, NO = 0<br>2. Is there a physical protection against the possibility of external intervention in pantograph controller during standstill and/or run?<br>YES = 1, NO = 0<br>3. Is there a physical protection against the possibility of external intervention in main circuit-breaker during standstill and/or run?,<br>YES = 1, NO = 0<br>NOTE: in the case of diesel traction, battery traction, as well as hydrogen and hybrid traction vehicles, there is a need to reformulate the above questions 1.÷3.<br>4. Is there an electric shock protection provided in the vehicle areas, which are accessible to passengers?<br>YES = 1, NO = 0 | Product of the answers:<br>0 or 1 |
| **RFM-7.2**<br>1. Is there a safe automatic control of on-board energy conversion equipment such as e.g. inverters, motors, converters, hydrogen cells, battery banks, ...) ensured?<br>YES = 1, NO = 0<br>2. Is there a physical protection against the possibility of vehicle power cut-off by unauthorised persons?<br>YES = 1, NO = 0<br>NOTE: excluding interventions on the infrastructure side. | Product of the answers:<br>0 or 1 |

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

--- --- ---

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

| Pytania kontrolne | Wartości ref. |
|---|---|
| **RMF-8.1**<br>1. Czy zastosowane jest fizyczne zabezpieczenie kabiny maszynisty oraz innych pomieszczeń/przestrzeni zamkniętych przed dostępem osób nieupoważnionych?<br>TAK = 1, NIE = 0<br>2. Czy zastosowane zabezpieczenie zapewniające ochronę, o której mowa powyżej, jest zabezpieczone przed możliwością ingerencji przez osoby nieupoważnione?<br>TAK = 1, NIE = 0 | Iloczyn odpowiedzi:<br>0 lub 1 |
| **RMF-8.2**<br>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)?<br>TAK = 1, NIE = 0<br>2. Czy istnieje fizyczne zabezpieczenie przed dostępem osób nieupoważnionych do kabli i sieciowych urządzeń aktywnych wykorzystywanych przez system monitoringu wizyjnego?<br>TAK = 1, NIE = 0<br>3. Czy istnieje fizyczne zabezpieczenie przed dostępem osób nieupoważnionych do kabli i sieciowych urządzeń aktywnych wykorzystywanych przez systemy hamowania?<br>TAK = 1, NIE = 0<br>4. Czy połączenia (kable, urządzenia aktywne, złącza) wykorzystywane przez systemy hamowania są fizycznie odseparowane od pokładowych sieci wykorzystywanych dla wszelkich innych celów?<br>TAK = 1, NIE = 0<br>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?<br>TAK = 2, NIE = 1 | Iloczyn odpowiedzi:<br>0 lub 1 lub 2 |

| | |
|---|---|
| **RFM-7.3**<br>1. Is there a physical protection against the possibility of external intervention by unauthorised persons in propulsion formation control system from outside the train?<br>YES = 1, NO = 0<br>2. Is there a physical protection against the possibility of external intervention by unauthorised persons in propulsion formation control system from inside the train?<br>YES = 1, NO = 0 | Product of the answers:<br>0 or 1 |
| **RFM-7.4**<br>1. Is there a physical protection against the possibility of external intervention by unauthorised persons in braking formation control system?<br>YES = 1, NO = 0<br>2. Is there a physical protection against the possibility of external intervention by unauthorised persons in wheel slide protection systems including sand distributors providing sand in front of vehicle wheels?<br>YES = 1, NO = 0 | Product of the answers:<br>0 or 1 |
| **Aggregate reference value for the group RFM-G07**<br>product of the reference values RFM-7.1 ÷ RFM-7.4 | 0 or 1 |

--- --- ---

| **Security control sheet RFM-G08**<br>functionalities dedicated to vehicle control (RFM-8.1 ÷ RFM-8.4) | |
|---|---|
| **Assumptions:**<br>Safe vehicle control shall be provided. | |
| **Control questions** | **Ref. values** |
| **RFM-8.1**<br>1. Is there a physical protection of the driver's cab and other spaces/areas, which are closed for unauthorised persons access?<br>YES = 1, NO = 0<br>2. Does the protection means providing protection against unauthorised access, see above, protected against intervention by unauthorised persons?<br>YES = 1, NO = 0 | Product of the answers:<br>0 or 1 |
| **RFM-8.2**<br>1. Is there a physical protection against unauthorised access to cables and on-board network active devices used for driver control of the digital systems/sub¬sys¬tems/ components that control, for example, doors, heating, ventilation, air-conditioning, passenger information (devices ensuring spoken and visual information)?<br>YES = 1, NO = 0<br>2. Is there a physical protection against unauthorised access to cables and on-board network active devices used by video surveillance system?<br>YES = 1, NO = 0<br>3. Is there a physical protection against unauthorised access to cables and on board network active devices used by braking systems?<br>YES = 1, NO = 0<br>4. Are the connections (cables, active devices, connectors) used by braking systems physically separated from on-board networks used for any other purpose??<br>YES = 1, NO = 0<br>5. Are the connections (cables, active devices, connectors) used to control the vehicle's speeding-up and to operate external doors (including movable egress steps, if any) physically separated from the on-board networks used for any other purpose?<br>YES = 2, NO = 1 | Product of the answers:<br>0 or 1 or 2 |

| | |
|---|---|
| **RMF-8.3**<br>1. Czy tabor wyposażony jest w systemy diagnostyczne?<br>TAK = 1, NIE = 0<br>2. Czy zastosowane jest fizyczne zabezpieczenie przed dostępem osób nieupoważnionych do systemów/urządzeń/czujników diagnostycznych?<br>TAK = 1, NIE = 0<br>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?<br>TAK = 1, NIE = 0 | Iloczyn odpowiedzi:<br>0 lub 1 |
| **RMF-8.4**<br>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?<br>TAK = 1, NIE = 0<br>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”.<br>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?<br>TAK = 1, NIE = 0 | Iloczyn odpowiedzi:<br>0 lub 1 |
| **Zbiorcza wartość referencyjna dla grupy RMF-G08**<br>iloczyn wartości referencyjnych RMF-8.1 ÷ RMF-8.4 | 0 lub 1 lub 2 |

--- --- ---

| **Karta kontrolna ochrony RMF-G09**<br>funkcjonalności dedykowane dla systemów umożliwiających podejmowanie działań w sytuacjach awaryjnych oraz oferowania „rozrywki” (RMF-9.1 ÷ RMF-9.6) | |
|---|---|
| **Założenia:**<br>1. Należy zapewnić bezpieczeństwo w sytuacjach zagrożeń ruchowych i w nagłych wypadkach.<br>2. Należy zapewnić brak zagrożeń ze strony systemów poprawiających komfort podróży. | |
| **Pytania kontrolne** | **Wartości ref.** |
| **RMF-9.1**<br>1. Czy istnieje fizyczne zabezpieczenie przed możliwością nieuprawnionej ingerencji w systemy alarmowe?<br>TAK = 1, NIE = 0<br>2. Czy działa system awaryjnego otwierania drzwi?<br>TAK = 1, NIE = 0<br>3. Czy istnieje zabezpieczenie przed możliwością nieuprawnionego awaryjnego otwarcia drzwi?<br>TAK = 1, NIE = 0<br>4. Czy działa system hamowania awaryjnego (hamulec bezpieczeństwa pasażera)?<br>TAK = 1, NIE = 0<br>5. Czy istnieje zabezpieczenie przed możliwością nieuprawnionej ingerencji zewnętrznej w system hamowania awaryjnego?<br>TAK = 1, NIE = 0<br>6. Czy działa system łączności wewnętrznej (intercom)?<br>TAK = 1, NIE = 0<br>7. Czy istnieje zabezpieczenie przed możliwością nieuprawnionej ingerencji zewnętrznej w system łączności wewnętrznej (intercom)?<br>TAK = 1, NIE = 0<br>8. Czy pojazd wyposażony jest w urządzenia AED oraz system nadzoru nad ich udostępnianiem z łącznością z kabiną maszynisty lub personelem pokładowym?<br>TAK = 2 NIE = 1 | Iloczyn odpowiedzi:<br>0 lub 1 lub 2 |
| **RMF-9.2**<br>1. Czy pojazd wyposażony jest w system wykrywania pożaru?<br>TAK = 1, NIE = 0<br>2. Czy pojazd wyposażony jest w system gaszenia pożaru?<br>TAK = 1, NIE = 0 | Iloczyn odpowiedzi:<br>0 lub 1 |

| | |
|---|---|
| **RFM-8.3**<br>1. Is the rolling stock equipped with diagnostic systems?<br>YES = 1, NO = 0<br>2. Is there a physical protection against access by unauthorised persons to diagnostic systems/devices/sensors?<br>YES = 1, NO = 0<br>3. Is there a physical protection against access by unauthorised persons to cables and on-board networks active devices used by diagnostic systems/devices/sensors, which are supervising the on-going rolling stock operation?<br>YES = 1, NO = 0 | Product of the answers:<br>0 or 1 |
| **RFM-8.4**<br>1. Is there a physical protection against unauthorised access to the devices that constitute together the on-board measurement system performing the measurement of the traction energy taken from and returned to the overhead contact line as well as connections between those devices?<br>YES = 1, NO = 0<br>NOTE: If the passenger rolling stock of a given type is not equipped with on-board measurement of the energy taken from and returned to the overhead contact line, the value “1” shall be assigned.<br>2. Is there a physical protection against unauthorised access, on the rolling stock side, to the wireless communication equipment used by the on-board energy measurement system performing the measurement of the traction energy taken from and returned to the overhead contact line?<br>YES = 1, NO = 0 | Product of the answers:<br>0 or 1 |
| **Aggregate reference value for the group RFM-G08**<br>product of the reference values RFM-8.1 ÷ RFM-8.4 | 0 or 1 or 2 |

--- --- ---

| **Security control sheet RFM-G09**<br>functionalities dedicated to systems supporting actions foreseen to be taken in emergency situations and to offer “entertainment” (RFM-9.1 ÷ RFM-9.6) | |
|---|---|
| **Assumptions:**<br>1. Safety shall be ensured in case of railway traffic related hazards and in case of emergencies.<br>2. There shall be no risk from systems that improve travel comfort. | |
| **Control questions** | **Ref. values** |
| **RFM-9.1**<br>1. Is there a physical protection against the possibility of unauthorised intervention in the alarm systems?<br>YES = 1, NO = 0<br>2. Does the door emergency opening system work?<br>YES = 1, NO = 0<br>3. Is there a protection against unauthorised emergency opening of the doors?<br>YES = 1, NO = 0<br>4. Does the emergency braking system (passenger emergency brake) work??<br>YES = 1, NO = 0<br>5. Is there a protection against unauthorised external intervention in the emergency braking system?<br>YES = 1, NO = 0<br>6. Does the internal communication system work (intercom)?<br>YES = 1, NO = 0<br>7. Is there a protection against unauthorised external intervention in the internal communication system (intercom)?<br>YES = 1, NO = 0<br>8. Is the vehicle equipped with AED devices and a surveillance system for their provision together with communication with the driver's cab or on-board staff?<br>YES = 2 NO = 1 | Product of the answers:<br>0 or 1 or 2 |
| **RFM-9.2**<br>1. Is the vehicle equipped with a fire detection system?<br>YES = 1, NO = 0<br>2. Is the vehicle equipped with a fire extinguishing system?<br>YES = 1, NO = 0 | Product of the answers:<br>0 or 1 |

| | |
|---|---|
| **RMF-9.3**<br>1. Czy zastosowany jest system wykrywania poślizgu?<br>TAK = 1, NIE = 0<br>2. Czy system wykrywania poślizgu ma zastosowane fizyczne zabezpieczenie przed dostępem osób nieupoważnionych?<br>TAK = 1, NIE = 0 | Iloczyn odpowiedzi:<br>0 lub 1 |
| **RMF-9.4**<br>1. Czy przedziały techniczne i szafy aparaturowe są fizycznie zabezpieczone przed dostępem osób nieuprawnionych?<br>TAK = 1, NIE = 0<br>2. Czy zastosowano zabezpieczenia fizyczne uniemożliwiające podłączenie się do magistrali CAN osobom nieupoważnionym, w tym maszynistom?<br>TAK = 1, NIE = 0<br>3. Czy zastosowano zabezpieczenia fizyczne uniemożliwiające podłączenie się do sieci LAN osobom nieupoważnionym?<br>TAK = 1, NIE = 0 | Iloczyn odpowiedzi:<br>0 lub 1 |
| **RMF-9.5**<br>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?<br>TAK = 1, NIE = 0<br>2. Czy istnieje zabezpieczenie przed możliwością nieuprawnionej ingerencji w pokładową sieć WiFi?<br>TAK = 1, NIE = 0 | Iloczyn odpowiedzi:<br>0 lub 1 |
| **RMF-9.6**<br>1. Czy systemy sprzedaży prasy, artykułów spożywczych i ewentualnie biletów (w tym wykorzystywane kable, urządzenia aktywne, złącza, bufory, itp.) są fizycznie odseparowane od wszelkich systemów i sieci pokładowych z wyjątkiem systemu udostępniania internetu pasażerom?<br>TAK = 1, NIE = 0 | Odpowiedz:<br>0 lub 1 |
| **Zbiorcza wartość referencyjna dla grupy RMF-G09**<br>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 pracujących w pojeździe,
- zagrożenia dla pojazdów dotyczące kanałów komunikacyjnych,
- zagrożenia dla pojazdów dotyczące procedur aktualizacji oprogramowania pojazdów,
- 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 pojazdy nie będą wystarczająco chronione lub jeżeli stosowne mechanizmy zabezpieczające nie zostały odpowiednio 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 sposobu działania,
- zmianę oprogramowania bez wpływu na sposób działania,
- naruszenie integralności danych,
- naruszenie poufności danych,

| | |
|---|---|
| **RFM-9.3**<br>1. Is there a slip detection system?<br>YES = 1, NO = 0<br>2. Does the slip detection system have physical protection against unauthorised access?<br>YES = 1, NO = 0 | Product of the answers:<br>0 or 1 |
| **RFM-9.4**<br>1. Are technical compartments and equipment cabinets physically protected against unauthorised access?<br>YES = 1, NO = 0<br>2. Are there physical protections in place to prevent unauthorised persons, including drivers, from connecting to the CAN bus?<br>YES = 1, NO = 0<br>3. Are there physical protections in place to prevent unauthorised persons from connecting to the LAN network?<br>YES = 1, NO = 0 | Product of the answers:<br>0 or 1 |
| **RFM-9.5**<br>1. Is the system providing internet access to passengers (including system cables, active devices, connectors, buffers, etc.) physically separated from all on-board systems and networks except for sale of press and/or food and possibly except ticketing systems?<br>YES = 1, NO = 0<br>2. Is there a protection against the possibility of unauthorised intervention in the on-board Wi-Fi network?<br>YES = 1, NO = 0 | Product of the answers:<br>0 or 1 |
| **RFM-9.6**<br>1. Are the systems for sale of press and/or food, and ticketing (including systems cables, active devices, connectors, buffers, etc.) physically separated from all on-board systems and networks except the ones providing internet to passengers?<br>YES = 1, NO = 0 | Answer:<br>0 or 1 |
| **Aggregate reference value for the group RFM-G09**<br>product of the reference values RFM-9.1 ÷ RFM-9.6 | 0 or 1 or 2 |

--- --- ---

#### 4.1.5.4. Railway passenger rolling stock type assessment regarding cybersecurity

All microprocessor systems and auxiliary equipment, such as diagnostic systems and all communication equipment, must be designed, tested and delivered with appropriate cybersecurity measures in place to prevent exposure to external threats.

These threats shall be identified as follows:
- threats associated with internal servers working in the vehicle,
- threats to vehicles regarding communication channels,
- threats to vehicles relating to their software update procedures,
- threats to vehicles relating to unintended human actions that facilitate cyberattacks,
- threats to vehicles relating to their external communications and connections,
- threats to vehicle data/code,
- potential vulnerabilities that can be exploited, if vehicles are not sufficiently protected or if the relevant protection means are not sufficiently subjected to hardening.

Possible consequences of an attack shall also be considered in the threats analysis. These can help to determine the severity of the risk and identify additional threats. Possible effects of an attack may include:
- impact on the safe operation of the vehicle,
- stopping the vehicle's functions,
- software modification, change in the way of operation,
- software modification without impact on the way of operation,
- violation of data integrity,
- breach of data confidentiality,

- 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, oraz oprogramowanie, 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. Systemy powinny także zapewniać metodę ochrony przed nieautoryzowaną eskalacją uprawnień.
6. Systemy pojazdowe 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.

- data loss,
- other effects, including those of a criminal nature.

Software that is installed, configured, used and updated in accordance with the requirements of the standards defining software safety, i.e. EN 50128 and EN 50657 [11], which together will be superseded by EN 50716 in 2023, as well as software that is installed, used, monitored and updated in accordance with the requirements of the EN ISO/IEC 62443 [14] series of standards for digital systems/ sub¬sys¬tems/components, which are intended for use in industrial control and automation systems, are assumed to provide an adequate level of functional safety. At the same time, it is recognised that functional safety may nevertheless be subject to actions, leading to threats to it. It is therefore necessary to follow to the requirements indicated below, which are verified using control sheets G9 to G14.

**Generic requirements regarding cybersecurity of the railway passenger rolling stock:**

1. A threat and vulnerability assessment of the Supplier's subsystem shall be carried out by determining the impact/probability for the following attack vectors taking into account detail characteristics of the subsystem:
    a. vandalism,
    b. eavesdropping,
    c. device/user impersonation,
    d. dictionary attacks,
    e. message modifications,
    f. session hijacking,
    g. buffer overflow,
    h. denial of service,
    i. jamming (denial of service at the physical layer),
    j. virus/worm infection,
    k. unauthorised installation of software, as well as
    l. unauthorised root/administrator access.
2. System shall be designed to be essentially cybersecured in accordance with the best IEC 62443 generic approach to cybersecurity practices.
3. Used encryption and authentication schemes shall be approved for active use (e.g. not superseded or obsolete) by the relevant governing bodies. Protocols with known defects or broken security means (e.g. WEP) are prohibited.
4. Unused functionalities that are not required for the operation or maintenance of the network node or end device shall be removed (e.g. software libraries, communication ports). If removal is not technically feasible, they shall be deactivated.

    Features that are not required shall be documented, including the method to remove or disable them. If any functions cannot be removed or disabled, the technical reason shall be explained and any associated risks shall be assessed, as well as how the risks can be mitigated.
5. Systems shall apply the principle of least privilege to enable access when providing a hierarchy of user account privileges to allow each user account to access only the required functionalities. Systems shall provide also method to protect against unauthorised privilege escalation.
6. Vehicle systems shall be designed taking into account planned future opportunities for safety improvements so that, over the lifetime of the vehicles, any protocols in use that become obsolete can be updated or replaced.

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 odpowiednie 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 pojazdowe 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.

7. System related documentation confirming that unauthorised recording devices (e.g. key recorders, cameras and microphones) have not been installed in the system after delivery to the Purchaser shall be verified and submitted.
8. Inbound/outbound rate limiting shall be applied on end device ports if necessary.
9. Common Vulnerabilities and Exposures (CVE) list shall be monitored for all relevant records before the software is delivered.

Any applicable CVEs from the Common Vulnerability Scoring System (CVSS) of medium severity or higher severity shall be mitigated prior to vehicle acceptance.

10. All user logins shall be authenticated and authorised by the terminal device before allowing access to the system. PTU-only verified logins are prohibited.
11. Communications requiring the transfer of passwords or session tokens over the network (e.g. PTU logins or file transfers) shall use an encrypted connection (e.g. HTTPS, FTPS, SFTP).
12. Passwords shall be stored in an approved one-way hashed format; passwords may not be stored in plain text, logged or permanently encoded in software or scripts. Obsolete hash protocols are prohibited (e.g. SHA1).
13. Any factory passwords that may be publicly available shall be replaced by passwords that meet the requirements set out above.
14. Physical ports and network node services not used for vehicle operation or maintenance shall be disabled.
15. Systems shall implement an appropriate approach to the collection and storage of security log files.
    a. Security log files shall contain timestamped events to enable audits and investigations, similar to syslogs.
    b. Security log files shall be read-only for all user accounts, including administrator accounts, and provide a method for checking the integrity of the log.
    c. Approach shall include at least the following events (as appropriate to their function):
        i. requests for information and response from equipment
        ii. successful and unsuccessful authentication and access attempts
        iii. account changes
        iv. privileged uses
        v. timestamp audit trails and log files in Coordinated Universal Time (UTC).
16. Systems shall provide means to access the system, taking into account physical access to the device, in order to prevent the system from being locked if passwords are lost. Such action shall be recorded and capable of being audited.
17. Vehicle systems shall be designed taking into account planned future opportunities for safety improvements so that, over the lifetime of the vehicles, any protocols in use that become obsolete can be updated or replaced.
18. Where applicable, all delivered software shall be configured in accordance with the national checklist programme. This requirement shall apply to all software components to which national checklists apply.

**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 pojazd 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 (cybersecurity)

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**<br>bezpieczne tworzenie oprogramowania |
|---|
| **Założenia:**<br>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**<br>1. Czy jest wprowadzony proces bezpieczeństwa zgodnie z normą IEC 62443-2-1?<br>TAK = 1, NIE = 0<br>2. Czy wymagane właściwości zostały wykazane przez analizę/testowanie?<br>TAK = 1, NIE = 0 | Iloczyn odpowiedzi:<br>0 lub 1 |

**Additional requirements, regarding cybersecurity of the railway passenger rolling stock, for systems with wireless access:**
If the offered system has wireless or trackside/side/ground access, the following requirements shall be fulfilled according to the technical specifications:

1. Wireless communication from the on-board network outside the vehicle to wayside services shall be via a VPN connection.
2. Communications shall be secured and encrypted to prevent unauthorised users from accessing data or the system. Communications shall use both secured wireless communications and a VPN tunnel to the Wayside Monitoring and Diagnostic System (WMDS). All traffic other than VPN shall be automatically rejected.
3. Information on all communication (e.g. protocols) required between the on-board network and wayside services - both incoming and outgoing - is required, together with the identification of each of them.
4. An assessment of vulnerability to intrusion via wireless access shall be documented in the Supplier Cybersecurity Assurance Plan (SCAP).

#### 4.1.5.5. Control sheets for passenger rolling stock type assessment in relation to cybersecurity (cybersecurity sheets)

These control sheets shall be completed, for the type of the rolling stock, which is under consideration, by assigning values to the answers according to the templates. It is underlined that the SSC case proving safety, security and cybersecurity integrity shall include all information necessary to verify the answers. Relevant data may be included in full in the SSC case, and can also be partly based on referenced documents, which then shall be made available to the body assessing SSC case.

Following four control sheets G10 to G13 shall be completed separately for each digital system/sub¬sys¬tem/component excluding only those systems/sub¬sys¬tems/components that are dedicated to railway safety functionalities, which are full covered by an adequate and reliable SIL-4 Specific Application Safety Case (SASC) developed and verified according to RAMS standards [9÷13].

NOTE: Control sheets G10 to G13 refer to the 27000 series standards and to the 62443 series standards. It is possible to use digital systems/sub¬sys¬tems/components that have been verified against other similar standards, e.g. the American ones, but in such cases it is necessary to carry out a comparison of requirements and develop a risk assessment that takes into account all risks arising from possible differences in requirements.

| **Cybersecurity control sheet RFM-G10**<br>safe software development | |
|---|---|
| **Assumptions:**<br>Software development shall take place in a coordinated manner, with full software safety oversight and in accordance with the relevant normative documents. | |
| **Control questions** | **Ref. values** |
| **RFM-10.1 – safety process in software development**<br>1. Is a safety process in place in accordance with the standard IEC 62443-2-1?<br>YES = 1, NO = 0<br>2. Have the required properties been demonstrated by analysis/testing?<br>YES = 1, NO = 0 | Product of the answers:<br>0 or 1 |

| | |
|---|---|
| **RMF-10.2 – analiza zagrożeń**<br>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?<br>TAK = 1, NIE = 0<br>2. Czy przeprowadzono test bezpieczeństwa IT, co najmniej test podatności z zgodnie z IEC 62443-4-1 rozdział 9.4?<br>TAK = 1, NIE = 0<br>3. Czy jest wdrożony proces usuwania luk w zabezpieczeniach zgodnie z normą IEC 62443-4-1 rozdział 10?<br>TAK = 1, NIE = 0<br>4. Czy jest wdrożony interfejs dla powiadomień o stwierdzonych lukach w zabezpieczeniach?<br>TAK = 1, NIE = 0<br>5. Czy wymagane właściwości zostały wykazane przez analizę/testowanie?<br>TAK = 1, NIE = 0 | Iloczyn odpowiedzi: 0 lub 1 |
| **RMF-10.3 – osoba odpowiedzialna za bezpieczeństwo oprogramowania**<br>1. Czy jest wyznaczona osoba kontaktowa odpowiedzialną za bezpieczeństwo IT dla zakresu danego systemu/podsystemu/komponentu z oprogramowaniem?<br>TAK = 1, NIE = 0<br>2. Czy jest zapewniony odpowiedni personel, posiadający wystarczającą wiedzę w zakresie bezpieczeństwa IT?<br>TAK = 1, NIE = 0<br>3. Czy jest wdrożony proces powiadamiania o zmianach personelu odpowiedzialnego za bezpieczeństwo IT?<br>TAK = 1, NIE = 0<br>4. Czy wymagane właściwości zostały wykazane przez analizę/testowanie?<br>TAK = 1, NIE = 0 | Iloczyn odpowiedzi: 0 lub 1 |
| **RMF-10.4 – wrażliwe dane systemu/podsystemu/komponentu zawierającego elementy programowe**<br>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)?<br>TAK = 1, NIE = 0<br>2. Czy wymagane właściwości zostały wykazane przez analizę/testowanie?<br>TAK = 1, NIE = 0 | Iloczyn odpowiedzi: 0 lub 1 |
| **RMF-10.5 – dostępność wsparcia technicznego dla oprogramowania**<br>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?<br>TAK = 1, NIE = 0<br>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?<br>TAK = 1, NIE = 0<br>3. Czy wymagane właściwości zostały wykazane przez analizę/testowanie?<br>TAK = 1, NIE = 0 | Iloczyn odpowiedzi: 0 lub 1 |
| **RMF-10.6 – cyberbezpieczeństwo w całym okresie eksploatacji**<br>1. Czy Dostawca systemów i komponentów podłączanych do dowolnej pociągowej sieci łączności zaproponował plan SCAP mający na celu zapewnienie cyberbezpieczeństwa systemu przez cały okres jego eksploatacji?<br>TAK = 1, NIE = 0<br>2. Czy wymagane właściwości zostały wykazane przez analizę/testowanie?<br>TAK = 1, NIE = 0<br>3. Czy jeśli system zostanie dotknięty nową luką w zabezpieczeniach, dostawca powiadomi zamawiającego/użytkownika i dostarczy odpowiednią poprawkę bezpieczeństwa?<br>TAK = 1, NIE = 0<br>4. Czy te rozwiązania i warunki są opisane w planie zapewniania cyberbezpieczeństwa SCAP?<br>TAK = 1, NIE = 0<br>5. Czy wymagane właściwości zostały wykazane przez analizę/testowanie?<br>TAK = 1, NIE = 0 | Iloczyn odpowiedzi: 0 lub 1 |
| **Zbiorcza wartość referencyjna dla grupy RMF-G10 dla danego systemu/podsystemu/komponentu z oprogramowaniem**<br>iloczyn wartości referencyjnych RMF-10.1 ÷ RMF-10.6 | Iloczyn odpowiedzi: 0 lub 1 |

--- --- ---

| | |
|---|---|
| **RFM-10.2 – threats analysis**<br>1. Has a safety threats and risks analysis been carried out, e.g. in accordance with the standard ISO 27005 based on the threat model in IEC 62443-4-1 Chapter 6.3?<br>YES = 1, NO = 0<br>2. Has an IT security test been carried out, at least a vulnerability testing in accordance with IEC 62443-4-1 Chapter 9.4?<br>YES = 1, NO = 0<br>3. Is there a process in place to address vulnerabilities in accordance with IEC 62443-4-1 Chapter 10?<br>YES = 1, NO = 0<br>4. Is there an interface in place for notifications of identified vulnerabilities?<br>YES = 1, NO = 0<br>5. Have the required properties been demonstrated by analysis/testing?<br>YES = 1, NO = 0 | Product of the answers:<br>0 or 1 |
| **RFM-10.3 – person responsible for software safety**<br>1. Is there a designated contact person responsible for IT security for the scope of the given digital system/subsystem/component?<br>YES = 1, NO = 0<br>2. Is there an adequate staffing in place with sufficient knowledge of IT security?<br>YES = 1, NO = 0<br>3. Is there a process in place to notify IT security personnel of changes?<br>YES = 1, NO = 0<br>4. Have the required properties been demonstrated by analysis/testing?<br>YES = 1, NO = 0 | Product of the answers:<br>0 or 1 |
| **RFM-10.4 – digital system/subsystem/component sensitive data**<br>1. Is there a process in place to specify that sensitive project data (e.g. IT security documents, data, software configurations, confidential documents), which shall be processed and transmitted in a secure manner (e.g. cannot be transmitted by email and other electronic technologies without encryption)?<br>YES = 1, NO = 0<br>2. Have the required properties been demonstrated by analysis/testing?<br>YES = 1, NO = 0 | Product of the answers:<br>0 or 1 |
| **RFM-10.5 – availability of technical support for the software**<br>1. Is there a process in place to determine that used software and firmware is not retired from support (end of life not yet reached) at the time of delivery?<br>YES = 1, NO = 0<br>2. Is there a written confirmation that the software and firmware used are not withdrawn from support (end of period not yet reached) at the time of delivery?<br>YES = 1, NO = 0<br>3. Have the required properties been demonstrated by analysis/testing?<br>YES = 1, NO = 0 | Product of the answers:<br>0 or 1 |
| **RFM-10.6 – cybersecurity over the entire lifetime**<br>1. Has the Supplier of the systems and components, which are to be connected to any train communication network, proposed a Supplier Cybersecurity Assurance Plan SCAP for the system throughout its lifetime?<br>YES = 1, NO = 0<br>2. Have the required properties been demonstrated by analysis/testing?<br>YES = 1, NO = 0<br>3. If the system is affected by a new vulnerability, will the supplier notify the purchaser/user and provide an appropriate security patch?<br>YES = 1, NO = 0<br>4. Are these solutions and conditions described in Cybersecurity Assurance Plan SCAP?<br>YES = 1, NO = 0<br>5. Have the required properties been demonstrated by analysis/testing?<br>YES = 1, NO = 0 | Product of the answers:<br>0 or 1 |
| **Aggregate reference value for the group RFM-G10 for a given digital system/subsystem/component**<br>product of the reference values RFM-10.1 ÷ RFM-10.6 | Product of the answers:<br>0 or 1 |

--- --- ---

| **Karta kontrolna cyberbezpieczeństwa RMF-G11**<br>kontrola dostępu |
|---|
| **Założenia:**<br>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**<br>1. Czy systemy/podsystemy/komponenty z oprogramowaniem podłączane do dowolnej sieci łączności pociągowej zapobiegają lub odpowiednio ograniczają korzystanie z niepotrzebnych funkcji, portów, protokołów i/lub usług?<br>TAK = 1, NIE = 0<br>2. Czy używane porty, protokoły lub usługi są udokumentowane w specyfikacji zabezpieczeń?<br>TAK = 1, NIE = 0<br>3. Czy wymagane właściwości zostały wykazane przez analizę/testowanie?<br>TAK = 1, NIE = 0 | Iloczyn odpowiedzi: 0 lub 1 |
| **RMF-11.2 – wyłączanie niewykorzystywanych portów fizycznych**<br>1. Czy systemy/podsystemy/komponenty z oprogramowaniem podłączane do dowolnej sieci komunikacyjnej pociągu zostały poddane procesowi wzmocnienia/utwardzania (hardening) w celu wyłączenia niepotrzebnych portów fizycznych?<br>TAK = 1, NIE = 0<br>2. Czy istniejące porty fizyczne, porty włączone i porty wyłączone zostały określone w planie zapewniania cyberbezpieczeństwa SCAP?<br>TAK = 1, NIE = 0<br>3. Czy wymagane właściwości zostały wykazane przez analizę/testowanie?<br>TAK = 1, NIE = 0 | Iloczyn odpowiedzi: 0 lub 1 |
| **RMF-11.3 – zapewnienie braku dostępność niepotrzebnych zasobów**<br>1. Czy systemy/podsystemy/komponenty z oprogramowaniem mają wyłączone niepotrzebne funkcje, porty, protokoły i/lub usługi?<br>TAK = 1, NIE = 0<br>2. Czy zastosowano zasady zgodne z IEC 62443-3-3: FR 7: Dostępność zasobów?<br>TAK = 1, NIE = 0<br>3. Czy w odniesieniu do systemów, których restart może być obserwowany przez pasażerów zastosowano zasadę bootowania systemów z ukrytym ciągiem zdarzeń (tzw. silent boot)?<br>TAK = 1, NIE = 0<br>4. Czy wymagane właściwości zostały wykazane przez analizę/testowanie?<br>TAK = 1, NIE = 0 | Iloczyn odpowiedzi: 0 lub 1 |
| **RMF-11.4 – wymagania informacyjne w planie zapewniania cyberbezpieczeństwa SCAP**<br>1. Czy dla każdego wcześniej zidentyfikowanego portu logicznego/usługi/protokołu określono następujące informacje w planie zapewniania cyberbezpieczeństwa SCAP:<br>- port fizyczny<br>- numer logicznego portu IP (jeśli sieć Ethernet)<br>- protokół komunikacyjny<br>- opis funkcji/uzasadnienie?<br>TAK = 1, NIE = 0<br>2. Czy wymagane właściwości zostały wykazane przez analizę/testowanie?<br>TAK = 1, NIE = 0 | Iloczyn odpowiedzi: 0 lub 1 |
| **RMF-11.5 – identyfikacja i uwierzytelnianie na interfejsach**<br>1. Czy systemy/podsystemy/komponenty z oprogramowaniem podłączane do dowolnej sieci łączności pociągowej wymuszają identyfikację i uwierzytelnianie we wszystkich interfejsach zarządzania, konfiguracji lub diagnostyki wszystkich użytkowników, oprogramowania procesów i urządzeń?<br>TAK = 1, NIE = 0<br>2. Czy wymuszanie takiej identyfikacji i uwierzytelniania ma miejsce na wszystkich interfejsach zapewniających dostęp do systemu?<br>TAK = 1, NIE = 0<br>3. Czy jest wymuszone szyfrowanie danych uwierzytelniających?<br>TAK = 1, NIE = 0<br>4. Czy nieużywane interfejsy fizyczne (np. USB, Ethernet / Profinet, Wi-Fi, Bluetooth), jak również porty debugowania są dezaktywowane lub mechanicznie zablokowane?<br>TAK = 1, NIE = 0 | |

| **Cybersecurity control sheet RFM-G11**<br>access control |
|---|
| **Assumptions:**<br>Digital systems/subsystems/components shall be adequately protected against unauthorised access. During the period of operation, access control shall be performed by the railway undertaking or entity in charge of maintenance of rolling stock. Such control may be delegated to manufacturer, but in this case the railway undertaking or entity in charge of maintenance shall supervise it. |

| Control questions | Ref. values |
|---|---|
| **RFM-11.1 – restricting access to unused functions, ports, protocols and/or services**<br>1. Do the digital systems/sub¬sys¬tems/components, which are to be connected to any train communication network, prevent or appropriately limit the use of unnecessary functions, ports, protocols and/or services?<br>YES = 1, NO = 0<br>2. Are the ports, protocols or services used documented in the security specification?<br>YES = 1, NO = 0<br>3. Have the required properties been demonstrated by analysis/testing?<br>YES = 1, NO = 0 | Product of the answers:<br>0 or 1 |
| **RFM-11.2 – disabling unused physical ports**<br>1. Have the digital systems/sub¬sys¬tems/components, which are to be connected to any of the train communication network, been subjected to a hardening process to exclude unnecessary physical ports?<br>YES = 1, NO = 0<br>2. Are the existing physical ports, enabled ports and disabled ports specified in the Cybersecurity Assurance Plan SCAP?<br>YES = 1, NO = 0<br>3. Have the required properties been demonstrated by analysis/testing?<br>YES = 1, NO = 0 | Product of the answers:<br>0 or 1 |
| **RFM-11.3 – ensuring that unnecessary resources are not available**<br>1. Do digital systems/sub¬sys¬tems/components have unnecessary functions, ports, protocols and/or services disabled?<br>YES = 1, NO = 0<br>2. Have the rules been applied in accordance with IEC 62443-3-3: FR 7: Resource availability?<br>YES = 1, NO = 0<br>3. Has the principle of silent boot (with hidden sequence of events) been applied to systems whose restart can be observed by passengers?<br>YES = 1, NO = 0<br>4. Have the required properties been demonstrated by analysis/testing?<br>YES = 1, NO = 0 | Product of the answers:<br>0 or 1 |
| **RFM-11.4 – information requirements in Cybersecurity Assurance Plan SCAP**<br>1. Has the following information been specified for each previously identified logical port/service/protocol in the Cybersecurity Assurance Plan SCAP:<br>- physical port,<br>- logical IP port number (if Ethernet),<br>- communication protocol,<br>- function description/reason?<br>YES = 1, NO = 0<br>2. Have the required properties been demonstrated by analysis/testing?<br>YES = 1, NO = 0 | Product of the answers:<br>0 or 1 |
| **RFM-11.5 – identification and authentication at the interfaces**<br>1. Do digital systems/sub¬sys¬tems/components, which are to be connected to any of the train communication network, enforce identification and authentication across all management, configuration and diagnostic interfaces for all users, process software and equipment?<br>YES = 1, NO = 0<br>2. Does enforcing of such identification and authentication take place at all interfaces providing access to the system?<br>YES = 1, NO = 0<br>3. Is there enforced encryption of credentials?<br>YES = 1, NO = 0<br>4. Are unused physical interfaces (e.g. USB, Ethernet / Profinet, Wi-Fi, Bluetooth) as well as debug ports deactivated or mechanically locked?<br>YES = 1, NO = 0 | |

| | |
|---|---|
| 5. Czy mechanizmy automatycznego uruchamiania są chronione (np. hasłem) lub dezaktywowane?<br>TAK = 1, NIE = 0<br>6. Czy w przypadku każdego interfejsu zarządzania, konfiguracji i diagnostyki w planie zapewniania cyberbezpieczeństwa SCAP określono następujące informacje:<br>- mechanizm uwierzytelniania,<br>- protokół mechanizmu uwierzytelniania?<br>TAK = 1, NIE = 0<br>7. Czy wymagane właściwości zostały wykazane przez analizę/testowanie?<br>TAK = 1, NIE = 0 | Iloczyn odpowiedzi:<br>0 lub 1 |
| **RMF-11.6 – hasła i/lub zabezpieczenie alternatywne zapewniające taki sam lub wyższy poziom zabezpieczenia**<br>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?<br>TAK = 1, NIE = 0<br>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)?<br>TAK = 1, NIE = 0<br>3. Czy mechanizm uwierzytelniania wymusza ustanowienie silnego hasła opartego na wielkich i małych literach, znakach niealfanumerycznych (tj. $, %, &, @, ...) i długości co najmniej 12 znaków?<br>TAK = 1, NIE = 0<br>4. Czy systemy, podsystemy, komponenty są dostarczane z hasłami, które odpowiadają regułom złożoności ustalonym przez integratora w zakresie długości hasła i typów znaków?<br>TAK = 1, NIE = 0<br>5. Czy integrator ma możliwość zmiany haseł i kluczy (czy brak jest zakodowanych sekretów w obrazie oprogramowania/oprogramowania układowego (SW/FW))?<br>TAK = 1, NIE = 0<br>6. Czy hasła i klucze są chronione przed nieautoryzowaną modyfikacją i ujawnieniem w spoczynku i podczas transportu?<br>TAK = 1, NIE = 0<br>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?<br>TAK = 1, NIE = 0<br>8. Czy hasła zostały przekazane integratorowi przed rozpoczęciem rozruchu statycznego?<br>TAK = 1, NIE = 0<br>9. Czy wymagane właściwości zostały wykazane przez analizę/testowanie?<br>TAK = 1, NIE = 0 | Iloczyn odpowiedzi:<br>0 lub 1 |
| **RMF-11.7 – dzienniki logowania**<br>1. Czy systemy/podsystemy/komponenty z oprogramowaniem podłączane do dowolnej sieci łączności pociągów zapewniają możliwość generowania dzienników istotnych dla bezpieczeństwa dla kategorii: próby logowania?<br>TAK = 1, NIE = 0<br>2. Czy Dzienniki te są dostępne dla przewoźnika lub podmiotu odpowiedzialnego za utrzymanie taboru?<br>TAK = 1, NIE = 0<br>3. Czy w planie zapewniania cyberbezpieczeństwa SCAP określono następujące informacje:<br>- mechanizm/procedura dostępu do pliku dziennika,<br>- plik dziennika zawierający zdarzenie próby logowania,<br>- format pliku dziennika i informacje w nim zawarte?<br>TAK = 1, NIE = 0<br>4. Czy wymagane właściwości zostały wykazane przez analizę/testowanie?<br>TAK = 1, NIE = 0 | Iloczyn odpowiedzi:<br>0 lub 1 |
| **RMF-11.8 – wykluczanie prostych haseł**<br>1. Czy systemy/podsystemy/komponenty z oprogramowaniem, które wymagają uwierzytelniania hasłem, stosują wytyczne dotyczące najlepszych praktyk w zakresie konfiguracji haseł i wykluczają hasła domyślne?<br>TAK = 1, NIE = 0 | |

| | |
|---|---|
| 5. Are the automatic start-up mechanisms protected (e.g. by password) or deactivated?<br>YES = 1, NO = 0<br>6. Are the following information specified for each management, configuration and diagnostic interface in the Cybersecurity Assurance Plan SCAP:<br>- authentication mechanism,<br>- authentication mechanism protocol?<br>YES = 1, NO = 0<br>7. Have the required properties been demonstrated by analysis/testing?<br>YES = 1, NO = 0 | Product of the answers:<br>0 or 1 |
| **RFM-11.6 – passwords and/or alternative protection neans providing the same or a higher level of security**<br>1. Are the digital systems/sub¬sys¬tems/components and their components, which are to be connected to any of the train communication network, using default password changes and applying a strong password policy?<br>YES = 1, NO = 0<br>2. Has a condition been applied in digital systems/sub¬sys¬tems/components and their digital components, which are to be connected to any of the train communication network, that unaltered default passwords (e.g. SSH host key, private key of self-signed certificates) shall not be used?<br>YES = 1, NO = 0<br>3. Does the authentication mechanism force the establishment of a strong password based on upper and lower case letters, non-alphanumeric characters (i.e. $, %, &, @, ...) with a length of at least 12 characters?<br>YES = 1, NO = 0<br>4. Are the systems, subsystems, components supplied with passwords that comply with complexity rules set by integrator in terms of password length and character types?<br>YES = 1, NO = 0<br>5. Does the integrator have the ability to change passwords and keys (are there no encoded secrets in the software/firmware image (SW/FW))?<br>YES = 1, NO = 0<br>6. Are passwords and keys protected against unauthorised modification and disclosure during warehousing and transport?<br>YES = 1, NO = 0<br>7. Is there a requirement for digital systems/sub¬sys¬tems/components, which are to be connected to any of the train communication network, to provide to the system/network integrator a list of passwords, mechanisms for changing credentials, also resetting and recovering passwords for all accounts (of the users and components)?<br>YES = 1, NO = 0<br>8. Have passwords been communicated to the integrator prior to the start of the standstill commissioning?<br>YES = 1, NO = 0<br>9. Have the required properties been demonstrated by analysis/testing?<br>YES = 1, NO = 0 | Product of the answers:<br>0 or 1 |
| **RFM-11.7 – logging logs**<br>1. Do digital systems/sub¬sys¬tems/components, which are to be connected to any of the train communication network, provide the ability to generate security relevant logs for the category: login attempts?<br>YES = 1, NO = 0<br>2. Are these logs available to the railway undertaking or entity in charge of maintenance of rolling stock?<br>YES = 1, NO = 0<br>3. Has the following information been specified in the Cybersecurity Assurance Plan SCAP:<br>- log file access mechanism/procedure,<br>- log file containing the logon attempt event,<br>- format of the log file and the information contained therein?<br>YES = 1, NO = 0<br>4. Have the required properties been demonstrated by analysis/testing?<br>YES = 1, NO = 0 | Product of the answers:<br>0 or 1 |
| **RFM-11.8 – excluding simple passwords**<br>1. Do digital systems/sub¬sys¬tems/components that require password authentication follow best practice guidelines for password configuration and exclude default passwords?<br>YES = 1, NO = 0 | |

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

--- --- ---

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

| Pytania kontrolne | Wartości ref. |
|---|---|
| **RMF-12.1 – integralność oprogramowania**<br>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?<br>TAK = 1, NIE = 0<br>2. Czy jest stosowane sprawdzenie podpisu cyfrowego oprogramowania po załadowaniu do komponentu w oparciu o algorytmy podpisu oparte na kryptografii asymetrycznej lub algorytmach HMAC?<br>TAK = 1, NIE = 0<br>3. Czy wymagane właściwości zostały wykazane przez analizę/testowanie?<br>TAK = 1, NIE = 0 | Iloczyn odpowiedzi:<br>0 lub 1 |
| **RMF-12.2 – dzienniki zmiany konfiguracji**<br>1. Czy systemy/podsystemy/komponenty z oprogramowaniem podłączane do dowolnej sieci łączności pociągowej zapewniają możliwość generowania dzienników związanych z bezpieczeństwem następujących kategorii: zmiany konfiguracji?<br>TAK = 1, NIE = 0<br>2. Czy Dzienniki te są dostępne dla przewoźnika lub podmiotu odpowiedzialnego za utrzymanie?<br>TAK = 1, NIE = 0<br>3. Czy w planie zapewniania cyberbezpieczeństwa SCAP określono następujące informacje:<br>- mechanizm/procedura dostępu do pliku dziennika,<br>- plik dziennika zawierający zdarzenie zmiany konfiguracji,<br>- format pliku dziennika i informacje w nim zawarte?<br>TAK = 1, NIE = 0<br>4. Czy wymagane właściwości zostały wykazane przez analizę/testowanie?<br>TAK = 1, NIE = 0 | Iloczyn odpowiedzi:<br>0 lub 1 |
| **RMF-12.3 – możliwość współpracy z zewnętrznym nadzorem nad dziennikami**<br>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)? | |

| | |
|---|---|
| 2. Are passwords configurable by the railway undertaking?<br>YES = 1, NO = 0<br>3. Is the identification and authentication control implemented in accordance with IEC 62443-3-3: FR 1: Identification and authentication control?<br>YES = 1, NO = 0<br>4. Have the required properties been demonstrated by analysis/testing?<br>YES = 1, NO = 0 | Product of the answers:<br>0 or 1 |
| **RFM-11.9 – authentication**<br>1. Is access to digital systems/subsystems/components provided via authentication?<br>YES = 1, NO = 0<br>2. Have the required properties been demonstrated by analysis/testing?<br>YES = 1, NO = 0 | Product of the answers:<br>0 or 1 |
| **RFM-11.10 – encryption**<br>1. Are digital systems/subsystems/components, which are using encryption, compliant with best practice and standards for their cryptographic mechanisms?<br>YES = 1, NO = 0<br>2. Are the confidentiality requirements applied as defined in IEC 62443-3-3: FR 4: Data Confidentiality?<br>YES = 1, NO = 0<br>3. Have the required properties been demonstrated by analysis/testing?<br>YES = 1, NO = 0 | Product of the answers:<br>0 or 1 |
| **Aggregate reference value for the group RFM-G11 for a given digital system/subsystem/component**<br>product of the reference values RFM-11.1 ÷ RFM-11.10 | Product of the answers:<br>0 or 1 |

--- --- ---

| **Cybersecurity control sheet RFM-G12**<br>configuration management |
|---|
| **Assumptions:**<br>Digital processes/subsystems/components shall be configured appropriately. |

| Control questions | Ref. values |
|---|---|
| **RFM-12.1 – software integrity**<br>1. Does the Supplier guarantee that the integrity of the software and firmware for its components includes protection against targeted manipulation of software or firmware that may be loaded into the system/subsystem/component?<br>YES = 1, NO = 0<br>2. Is it practiced to check the digital signature of the software, when loaded into the component, based on signature algorithms based on asymmetric cryptography or HMAC algorithms?<br>YES = 1, NO = 0<br>3. Have the required properties been demonstrated by analysis/testing?<br>YES = 1, NO = 0 | Product of the answers:<br>0 or 1 |
| **RFM-12.2 – configuration change logs**<br>1. Do digital systems/sub¬sys¬tems/components, which are to be connected to any of the train communication network, provide the ability to generate security-related logs for the following categories: configuration changes?<br>YES = 1, NO = 0<br>2. Are these logs available to the railway undertaking or entity in charge of maintenance of rolling stock?<br>YES = 1, NO = 0<br>3. Has the following information been specified in the Cybersecurity Assurance Plan SCAP:<br>- log file access mechanism/procedure,<br>- log file containing the configuration change event,<br>- format of the log file and the information contained therein?<br>YES = 1, NO = 0<br>4. Have the required properties been demonstrated by analysis/testing?<br>YES = 1, NO = 0 | Product of the answers:<br>0 or 1 |
| **RFM-12.3 – ability to cooperate with external surveillance of logs**<br>1. Do digital systems/sub¬sys¬tems/components and their components provide the ability to automatically and immediately transfer generated logs to external log management systems using industry-leading protocols (for example, syslog)? | |

| | |
|---|---|
| TAK = 1, NIE = 0<br>2. Czy wymagane właściwości zostały wykazane przez analizę/testowanie?<br>TAK = 1, NIE = 0 | Iloczyn odpowiedzi: 0 lub 1 |
| **RMF-12.4 – znane luki w zabezpieczeniach**<br>1. Czy systemy/podsystemy/komponenty z oprogramowaniem podłączane do dowolnej sieci łączności pociągów są wolne od znanych luk w zabezpieczeniach?<br>TAK = 1, NIE = 0<br>2. Czy w planie zapewniania cyberbezpieczeństwa SCAP określono następujące informacje:<br>- Raport ze skanowania pod kątem luk we wszystkich fizycznych portach Ethernet?<br>TAK = 1, NIE = 0<br>3. Czy wymagane właściwości zostały wykazane przez analizę/testowanie?<br>TAK = 1, NIE = 0 | Iloczyn odpowiedzi: 0 lub 1 |
| **RMF-12.5 – alerty dla zmian konfiguracji**<br>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?<br>TAK = 1, NIE = 0<br>2. Czy odpowiadająca za to funkcjonalność jest zgodna z wymaganiami IEC 62443-3-3: FR 2: Kontrola użytkowania, lub podobną normą?<br>TAK = 1, NIE = 0<br>3. Czy wymagane właściwości zostały wykazane przez analizę/testowanie?<br>TAK = 1, NIE = 0 | Iloczyn odpowiedzi: 0 lub 1 |
| **RMF-12.6 – ochrona przed ujawnieniem i modyfikacją danych**<br>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?<br>TAK = 1, NIE = 0<br>2. Czy wymagane właściwości zostały wykazane przez analizę/testowanie?<br>TAK = 1, NIE = 0 | Iloczyn odpowiedzi: 0 lub 1 |
| **RMF-12.7 – aktualizacje i uaktualnienia poprawkami bezpieczeństwa**<br>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)?<br>TAK = 1, NIE = 0<br>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.<br>2. Czy funkcje realizujące te procesy są zgodne z wymaganiami IEC 62443-4-2: FR 3: Integralność systemu, lub podobnymi normami?<br>TAK = 1, NIE = 0<br>3. Czy wymagane właściwości zostały wykazane przez analizę/testowanie?<br>TAK = 1, NIE = 0 | Iloczyn odpowiedzi: 0 lub 1 |
| **RMF-12.8 – dokumentowanie bezpiecznej konfiguracji**<br>1. Czy systemy/podsystemy/komponenty z oprogramowaniem mają udokumentowaną bezpieczną konfigurację?<br>TAK = 1, NIE = 0<br>2. Czy konfiguracja opiera na zalecanych ustawieniach bezpieczeństwa i najlepszych praktykach?<br>TAK = 1, NIE = 0<br>3. Czy jest zgodna z wymaganiami IEC 62443-3-3: FR 7: Dostępność zasobów?<br>TAK = 1, NIE = 0<br>4. Czy wymagane właściwości zostały wykazane przez analizę/testowanie?<br>TAK = 1, NIE = 0 | Iloczyn odpowiedzi: 0 lub 1 |
| **RMF-12.9 – przywracanie znanego stanu bezpiecznego**<br>1. Czy systemy/podsystemy/komponenty z oprogramowaniem umożliwiają odzyskanie i przywracanie do znanego stanu bezpiecznego po zakłóceniu lub awarii?<br>TAK = 1, NIE = 0<br>2. Czy odbywa się to zgodnie z IEC 62443-3-3: FR 7: Dostępność zasobów?<br>TAK = 1, NIE = 0<br>3. Czy wymagane właściwości zostały wykazane przez analizę/testowanie?<br>TAK = 1, NIE = 0 | Iloczyn odpowiedzi: 0 lub 1 |

| | |
|---|---|
| YES = 1, NO = 0<br>2. Have the required properties been demonstrated by analysis/testing?<br>YES = 1, NO = 0 | Product of the answers:<br>0 or 1 |
| **RFM-12.4 – known vulnerabilities**<br>1. Do digital systems/sub¬sys¬tems/components, which are to be connected to any of the train communication network, remain free of known vulnerabilities?<br>YES = 1, NO = 0<br>2. Has the following information been specified in the Cybersecurity Assurance Plan SCAP:<br>- Scanning report for vulnerabilities on all physical Ethernet ports?<br>YES = 1, NO = 0<br>3. Have the required properties been demonstrated by analysis/testing?<br>YES = 1, NO = 0 | Product of the answers:<br>0 or 1 |
| **RFM-12.5 – alerts for configuration changes**<br>1. Are digital systems/sub¬sys¬tems/components, in case of which human access is possible (e.g. to perform software updates, configuration changes), generating alerts that can be provided to the external system in the event of access and/or change?<br>YES = 1, NO = 0<br>2. Does the corresponding functionality comply with the requirements of the IEC 62443-3-3: FR 2: Use control, or similar standards?<br>YES = 1, NO = 0<br>3. Have the required properties been demonstrated by analysis/testing?<br>YES = 1, NO = 0 | Product of the answers:<br>0 or 1 |
| **RFM-12.6 – protection against disclosure and modification of data**<br>1. Whether digital systems/sub¬sys¬tems/components have the ability to protect data from unauthorised disclosure or modification, as well as procedural measures to enable data to be deleted by replacement or deactivation?<br>YES = 1, NO = 0<br>2. Have the required properties been demonstrated by analysis/testing?<br>YES = 1, NO = 0 | Product of the answers:<br>0 or 1 |
| **RFM-12.7 – updates and upgrades with security patches**<br>1. Do digital systems/sub¬sys¬tems/components, have the ability to update and upgrade all parts of the solution (e.g. firmware, application software, middleware) with security patches?<br>YES = 1, NO = 0<br>NOTE: It is not required that all the digital systems/sub¬sys¬tems/components support such elements as: automatic updates, regular security patching processes or vulnerability scanning.<br>2. Does the corresponding functionality comply with the requirements of the IEC 62443-4-2: FR 3: System integrity, or similar standards?<br>YES = 1, NO = 0<br>3. Have the required properties been demonstrated by analysis/testing?<br>YES = 1, NO = 0 | Product of the answers:<br>0 or 1 |
| **RFM-12.8 – documenting security-related configuration**<br>1. Whether digital systems/sub¬sys¬tems/components have a documented security-related configuration?<br>YES = 1, NO = 0<br>2. Is the configuration based on recommended security settings and best practices?<br>YES = 1, NO = 0<br>3. Does it comply with the requirements of the IEC 62443-3-3: FR 7: Resource availability?<br>YES = 1, NO = 0<br>4. Have the required properties been demonstrated by analysis/testing?<br>YES = 1, NO = 0 | Product of the answers:<br>0 or 1 |
| **RFM-12.9 – restoration of a known safe state**<br>1. Do digital systems/sub¬sys¬tems/components allow recovery and restoration to known safe state after a disruption or failure??<br>YES = 1, NO = 0<br>2. Is this done in accordance with IEC 62443-3-3: FR 7: Resource availability?<br>YES = 1, NO = 0<br>3. Have the required properties been demonstrated by analysis/testing?<br>YES = 1, NO = 0 | Product of the answers:<br>0 or 1 |

| | |
|---|---|
| **RMF-12.10 – generowanie zdarzeń**<br>1. Czy systemy/podsystemy/komponenty z oprogramowaniem mają możliwość generowania zdarzeń związanych z bezpieczeństwem i przesyłania ich do aplikacji zewnętrznych?<br>TAK = 1, NIE = 0<br>UWAGA: Zdolność ta może być zapewniana bezpośrednio przez systemy/ podsystemy/komponenty lub pośrednio poprzez alternatywne środki?<br>2. Czy jest ona realizowana zgodnie z wymaganiami IEC 62443-3-3: FR 2: Kontrola użytkowania, lub podobnych norm.<br>TAK = 1, NIE = 0<br>3. Czy wymagane właściwości zostały wykazane przez analizę/testowanie?<br>TAK = 1, NIE = 0 | Iloczyn odpowiedzi: 0 lub 1 |
| **RMF-12.11 – egzekwowanie ograniczeń użytkownika**<br>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)?<br>TAK = 1, NIE = 0<br>2. Czy odbywa się to zgodnie z wymaganiami IEC 62443-3-3: FR-2: Kontrola użytkowania, lub innych podobnych norm?<br>TAK = 1, NIE = 0<br>3. Czy wymagane właściwości zostały wykazane przez analizę/testowanie?<br>TAK = 1, NIE = 0 | Iloczyn odpowiedzi: 0 lub 1 |
| **RMF-12.12 – nieudane instalacje aktualizacji**<br>1. Czy systemy/podsystemy/komponenty z oprogramowaniem posiadają mechanizmy zapewniające bezpieczny powrót do poprzedniego stanu w przypadku nieudanej instalacji aktualizacji?<br>TAK = 1, NIE = 0<br>2. Czy wymagane właściwości zostały wykazane przez analizę/testowanie?<br>TAK = 1, NIE = 0 | Iloczyn odpowiedzi: 0 lub 1 |
| **RMF-12.13 – wykrywanie nieautoryzowanych zmian oprogramowania**<br>1. Czy wykrywane są nieautoryzowane zmiany w oprogramowaniu i oprogramowaniu układowym (firmware) używanym przez systemy/podsystemy/komponenty z oprogramowaniem?<br>TAK = 1, NIE = 0<br>2. Czy wymagane właściwości zostały wykazane przez analizę/testowanie?<br>TAK = 1, NIE = 0 | Iloczyn odpowiedzi: 0 lub 1 |
| **RMF-12.14 – wykrywanie złośliwego oprogramowania (malware'u)**<br>1. Czy systemy/podsystemy/komponenty z oprogramowaniem mają możliwość wykrywania i zgłaszania złośliwego lub nieautoryzowanego oprogramowania?<br>TAK = 1, NIE = 0<br>2. Czy odbywa się to zgodnie z wymaganiami IEC 62443-3-3: FR 3: Integralność systemu, lub innych podobnych norm?<br>TAK = 1, NIE = 0<br>3. Czy wymagane właściwości zostały wykazane przez analizę/testowanie?<br>TAK = 1, NIE = 0 | Iloczyn odpowiedzi: 0 lub 1 |
| **RMF-12.15 – fizyczne zabezpieczenie złącz**<br>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?<br>TAK = 1, NIE = 0<br>2. Czy wymagane właściwości zostały wykazane przez analizę/testowanie?<br>TAK = 1, NIE = 0 | Iloczyn odpowiedzi: 0 lub 1 |
| **RMF-12.16 – odporność na przeciążenia**<br>1. Czy systemy/podsystemy/komponenty z oprogramowaniem są odporne na przeciążenia i reagują w określony sposób?<br>TAK = 1, NIE = 0<br>2. Czy uwzględniono różne protokoły i warstwy np. aplikacje internetowe, zastrzeżone protokoły i warstwę sieciową?<br>TAK = 1, NIE = 0<br>3. Czy wymagane właściwości zostały wykazane przez analizę/testowanie?<br>TAK = 1, NIE = 0 | Iloczyn odpowiedzi: 0 lub 1 |
| **Zbiorcza wartość referencyjna dla grupy RMF-G12 dla danego systemu/podsystemu/komponentu z oprogramowaniem**<br>iloczyn wartości referencyjnych RMF-12.1 ÷ RMF-12.16 | Iloczyn odpowiedzi: 0 lub 1 |

--- --- ---

| | |
|---|---|
| **RFM-12.10 – generating events**<br>1. Do digital systems/sub¬sys¬tems/components have the ability to generate security events and send them to external applications?<br>YES = 1, NO = 0<br>NOTE: This ability can be provided directly by systems/ sub¬sys¬tems/ components or indirectly through alternative means?<br>2. Is it carried out in accordance with the requirements of the IEC 62443-3-3: FR 2: Use control, or similar standards.<br>YES = 1, NO = 0<br>3. Have the required properties been demonstrated by analysis/testing?<br>YES = 1, NO = 0 | Product of the answers:<br>0 or 1 |
| **RFM-12.11 – enforcement of user restrictions**<br>1. Do digital systems/sub¬sys¬tems/components and networks have the ability to enforce usage restrictions (e.g. usage restrictions on disabling unused USB ports, whitelisting and network access control)?<br>YES = 1, NO = 0<br>2. Is it carried out in accordance with the requirements of the IEC 62443-3-3: FR-2: Use control, or similar standards?<br>YES = 1, NO = 0<br>3. Have the required properties been demonstrated by analysis/testing?<br>YES = 1, NO = 0 | Product of the answers:<br>0 or 1 |
| **RFM-12.12 – unsuccessful update installations**<br>1. Do digital systems/sub¬sys¬tems/components have mechanisms in place to ensure safe recovery in the event of a failed update installation?<br>YES = 1, NO = 0<br>2. Have the required properties been demonstrated by analysis/testing?<br>YES = 1, NO = 0 | Product of the answers:<br>0 or 1 |
| **RFM-12.13 – detection of unauthorised software changes**<br>1. Are unauthorised changes to software and firmware used by digital systems/sub¬sys¬tems/components detected?<br>YES = 1, NO = 0<br>2. Have the required properties been demonstrated by analysis/testing?<br>YES = 1, NO = 0 | Product of the answers:<br>0 or 1 |
| **RFM-12.14 – malware detection**<br>1. Do digital systems/sub¬sys¬tems/components have the ability to detect and report malicious or unauthorised software?<br>YES = 1, NO = 0<br>2. Is it carried out in accordance with the requirements of the IEC 62443-3-3: FR 3: System integrity, or similar standards?<br>YES = 1, NO = 0<br>3. Have the required properties been demonstrated by analysis/testing?<br>YES = 1, NO = 0 | Product of the answers:<br>0 or 1 |
| **RFM-12.15 – physical protection of connectors**<br>1. Are digital systems/sub¬sys¬tems/components that have connectors that form an entry point to the system/sub¬sys¬tem/component itself and/or to the network (in addition to their own connection to the network) physically secured?<br>YES = 1, NO = 0<br>2. Have the required properties been demonstrated by analysis/testing?<br>YES = 1, NO = 0 | Product of the answers:<br>0 or 1 |
| **RFM-12.16 – overload resistance**<br>1. Are digital systems/sub¬sys¬tems/components resistant to overload and responsive in certain ways?<br>YES = 1, NO = 0<br>2. Have the different protocols and layers been considered, e.g. web applications, proprietary protocols and the network layer?<br>YES = 1, NO = 0<br>3. Have the required properties been demonstrated by analysis/testing?<br>YES = 1, NO = 0 | Product of the answers:<br>0 or 1 |
| **Aggregate reference value for the group RFM-G12**<br>**for a given digital systems/subsystems/components**<br>product of the reference values RFM-12.1 ÷ RFM-12.16 | Product of the answers:<br>0 or 1 |

--- --- ---

| **Karta kontrolna cyberbezpieczeństwa RMF-G13**<br>oprogramowanie wspomagające eksploatację i utrzymanie |
|---|
| **Założenia:**<br>Konieczne jest zapewnienie bezpieczeństwa korzystania z oprogramowania narzędziowego i serwisowego. |

| Pytania kontrolne | Wartości ref. |
|---|---|
| **RMF-13.1 – złośliwe oprogramowanie w oprogramowaniu narzędziowym**<br>1. Czy oprogramowanie narzędziowe i serwisowe jest wolne od złośliwego oprogramowania w momencie przekazania integratorowi?<br>TAK = 1, NIE = 0<br>2. Czy wymagane właściwości zostały wykazane przez analizę/testowanie?<br>TAK = 1, NIE = 0 | Iloczyn odpowiedzi: 0 lub 1 |
| **RMF-13.2 – ograniczanie praw użytkownikowi oprogramowania narzędziowego**<br>1. Czy oprogramowanie narzędziowe i serwisowe działa z najmniejszymi możliwymi uprawnieniami (np. użytkownik zamiast uprawnień administratora)?<br>TAK = 1, NIE = 0<br>2. Czy wymagane właściwości zostały wykazane przez analizę/testowanie?<br>TAK = 1, NIE = 0 | Iloczyn odpowiedzi: 0 lub 1 |
| **Zbiorcza wartość referencyjna dla grupy RMF-G13**<br>**dla danego systemu/podsystemu/komponentu z oprogramowaniem**<br>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 oprogramowaniem, 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.

| **Zbiorcza karta kontrolna cyberbezpieczeństwa RMF-G14**<br>komplet funkcjonalności dedykowanych cyberbezpieczeństwu |
|---|
| **Założenia:**<br>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.<br>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.<br>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.<br>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**<br>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”?)<br>TAK = 1, NIE = 0 | Iloczyn zbiorczych wartości referencyjnych z kart G10 dla wszystkich systemów/podsystemów/ komponentów<br>0 lub 1 |
| **RMF-14.2 – kontrola dostępu**<br>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”?)<br>TAK = 1, NIE = 0 | Iloczyn zbiorczych wartości referencyjnych z kart G10 dla wszystkich systemów/podsystemów/ komponentów<br>0 lub 1 |

| Cybersecurity control sheet RFM-G13<br>software supporting operation and maintenance |
|---|
| **Assumptions:**<br>It is necessary to ensure the security of the use of software tools and service software. |

| Control questions | Ref. values |
|---|---|
| **RFM-13.1 – malware in software tools**<br>1. Are the software tools and service software free of malware at the time of handover to the integrator?<br>YES = 1, NO = 0<br>2. Have the required properties been demonstrated by analysis/testing?<br>YES = 1, NO = 0 | Product of the answers:<br>0 or 1 |
| **RFM-13.2 – limiting the rights of the software tools user**<br>1. Does the software tools and service software run with the least possible rights (e.g. user instead of administrator rights)?<br>YES = 1, NO = 0<br>2. Have the required properties been demonstrated by analysis/testing?<br>YES = 1, NO = 0 | Product of the answers:<br>0 or 1 |
| **Aggregate reference value for the group RFM-G13 for a given digital system/subsystem/component**<br>product of the reference values RFM-13.1 ÷ RFM-13.2 | Product of the answers:<br>0 or 1 |

--- --- ---

The next control sheet (sheet G14) has an aggregate nature. Control sheets G10 to G13 apply to individual digital systems/sub¬sys¬tems/components, while sheet G14 applies to the aggregate assessment of the cyber-security of a given type of railway passenger rolling stock and, as such, is based, inter alia, on the systems/sub¬sys-tems/components sheets.

| Overall cybersecurity control sheet RFM-G14<br>a set of functionalities dedicated to cyber security |
|---|
| **Assumptions:**<br>1. Systems/sub¬sys¬tems/components performing vehicle movement safety related functionalities shall be covered by a Specific Application Safety Case (SASC) proving SIL-4, which is developed and verified according to RAMS standards [9÷13]. Their re-verification using control sheets G10 to G13 is considered redundant and therefore unnecessary.<br>2. All other systems/subsystems/components shall be included in the analysis using control sheets G10 to G13; The relationships between all separated digital systems/sub¬sys¬tems/components shall be presented at the beginning of Chapter 4 of the **SSC case proving safety, security and cybersecurity integrity** for a given rolling stock type.<br>3. Protection against cyberattacks shall be provided for all wired and wireless data transmission systems that are utilised for the purpose of the railway traffic safety, including those included in the safety case referred to in point 1. above.<br>4. Protection against cyberattacks shall be provided for all wired and wireless data transmission systems that are utilised for the purpose of the railway transport security (transport safety). |

| Control questions | Ref. values |
|---|---|
| **RFM-14.1 – safe software development**<br>1. Whether for all digital systems/sub¬sys¬tems/components, software was developed in a secure manner?<br>(Whether answers to all questions for all digital systems/sub¬sys¬tems/components in RFM G10 sheets, have assigned value “1” as appropriate?)<br>YES = 1, NO = 0 | Product of the aggregate reference values of the control sheets G10 of all systems/subsystems/components:<br>0 or 1 |
| **RFM-14.2 – access control**<br>1. Whether all digital systems/sub¬sys¬tems/components have appropriate access control?<br>(Whether answers to all questions for all digital systems/sub¬sys¬tems/components in RFM G11 sheets, have assigned value “1” as appropriate?)<br>YES = 1, NO = 0 | Product of the aggregate reference values of the control sheets G10 of all systems/subsystems/components:<br>0 or 1 |

| | |
|---|---|
| **RMF-14.3 – zarządzanie konfiguracją**<br>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”?)<br>TAK = 1, NIE = 0 | Iloczyn zbiorczych wartości referencyjnych z kart G10 dla wszystkich systemów/podsystemów/ komponentów<br>0 lub 1 |
| **RMF-14.4 – oprogramowanie wspomagające eksploatację i utrzymanie**<br>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”?)<br>TAK = 1, NIE = 0 | Iloczyn zbiorczych wartości referencyjnych z kart G10 dla wszystkich systemów/podsystemów/ komponentów<br>0 lub 1 |
| **RMF-14.5 – zasilanie awaryjne**<br>**1.** Czy pokładowe systemy bezpiecznej kontroli jazdy oraz łączności głosowej (maszynisty z dyżurnym ruchu) mają zapewnione zasilanie rezerwowe w przypadku utraty 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)?<br>TAK = 2, NIE = 1<br>**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 utraty głównego źródła zasilania pozwalające na dalszą pracę w normalnym trybie przez minimum 2 godziny?<br>TAK = 2, NIE = 1<br>**3.** Czy system monitoringu wizyjnego ma zapewnione zasilanie w przypadku utraty 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?<br>TAK = 1, NIE = 0 | Iloczyn odpowiedzi:<br>0 lub 1 lub 2 lub 4 |
| **RMF-14.6 – aktywna kopia oprogramowania układowego (firmwaru)**<br>**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?<br>TAK = 2, NIE = 1 | Odpowiedź:<br>1 lub 2 |
| **Zbiorcza wartość referencyjna dla grupy RMF-G14**<br>iloczyn wartości referencyjnych RMF-14.1 ÷ RMF-14.6 | 0 lub 1 lub 2 lub 4 lub 8 |

--- --- ---

| | |
|---|---|
| **RFM-14.3 – configuration management**<br>1. Whether all digital systems/sub¬sys¬tems/components have appropriate configuration management?<br>(Whether answers to all questions for all digital systems/sub¬sys¬tems/components in RFM G12 sheets, have assigned value “1” as appropriate?)<br>YES = 1, NO = 0 | Product of the aggregate reference values of the control sheets G10 of all systems/subsystems/ components:<br>0 or 1 |
| **RFM-14.4 – software supporting operation and maintenance**<br>1. Whether for all digital systems/sub¬sys¬tems/components security of the software tools and service software is ensured?<br>(Whether answers to all questions for all digital systems/sub¬sys¬tems/components in RFM G13 sheets, have assigned value “1” as appropriate?)<br>YES = 1, NO = 0 | Product of the aggregate reference values of the control sheets G10 of all systems/subsystems/ components:<br>0 or 1 |
| **RFM-14.5 – backup power supply**<br>**1.** Do the on-board control-command system and voice communication system (ensuring communication between driver and traffic controller) have backup power supply, which in the event of loss of the main power supply, allows further normal operation for a minimum of 30 minutes, and informs the driver about activation of the backup power supply and the need to stop, before the end of 30 minutes (the guaranteed back-up power supply time), at a location, which is convenient for (technical, rescue, safety) service activities and evacuation?<br>YES = 2, NO = 1<br>**2.** Do the digital systems/sub¬sys¬tems/components, that control braking systems, door and movable egress steps, ventilation, fire detection and fire extinguishing systems as well as passenger information systems (ensuring at least spoken information) and passenger safety aids (emergency door-opening, emergency driver/on-board staff notification systems (call for assistance) and passenger emergency braking systems) as well as driver desk, cables and active network equipment utilised for driver control of these digital systems/sub¬sys¬tems/components, have backup power supply, which in the event of loss of the main power supply, allows further normal operation for a minimum of 2 hours?<br>YES = 2, NO = 1<br>**3.** Does the video surveillance system have backup power supply, which in the event of loss of the main power supply, ensures further normal operation for a minimum of 30 minutes and retain of the records both from before the loss of the main power supply and for a minimum of 30 minutes afterwards?<br>YES = 1, NO = 0 | Product of the answers:<br>0 or 1 or 2 or 4 |
| **RFM-14.6 – active firmware copy**<br>**1.** Is there available copy of the firmware of the digital systems/sub¬sys¬tems/ components that control braking systems, door and movable egress steps, ventilation, fire detection and fire extinguishing systems as well as passenger information systems (ensuring at least spoken information) and passenger safety aids (emergency door-opening, emergency driver/on-board staff notification systems (call for assistance) and passenger emergency braking systems), and a firmware intervention detection system, based e.g. on a hash function, that detects firmware changes, and informs driver (or ATS system in case of an autonomous rolling stock) in case firmware change is detected, and replaces the firmware after driver/ATS system operator confirmation?<br>YES = 2, NO = 1 | Answer:<br>1 or 2 |
| **Aggregate reference value for the group RFM-G14**<br>product of the reference values RFM-14.1 ÷ RFM-14.6 | 0 or 1 or 2<br>or 4 or 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 taboru prowadzonego prze maszynistów, obejmuje funkcjonalności wskazane w kartach kontrolnych RMF-G01 -G02, -G03 oraz RMF-G04, a dla taboru autonomicznego poruszającego się bez maszynistów, pod nadzorem systemów automatycznego prowadzenia ruchu (systemów klasy ATO – ang. Automatic Train Operation), funkcjonalności wskazane w kartach kontrolnych RMF-G01, -G02, -G03, -G04 oraz RMF-G05. Skumulowana wartość referencyjna dla ochrony obejmuje funkcjonalności wskazane w kartach kontrolnych RMF-G06, -G07, -G08 oraz RMF-G09, natomiast skumulowaną wartość referencyjną dla cyberbezpieczeństwa uzyskuje się z karty kontrolnej RMF-G14 odwołującej się do indywidualnych kart kontrolnych cyberbezpieczeństwa RMF-G10, -G11, -G12 oraz RMF-G13.

Dopuszcza się stosowanie przez **wykonawców** koncepcji i projektów oraz **wykonawców** realizujących budowę lub przebudowę taboru innych pytań różnicujących. Jednak zastosowanie innego pytania różnicującego wymaga każdorazowo uzyskania pisemnej zgody od 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 (poziom bezpieczeństwa),
*SC* – skumulowana wartość referencyjna dla ochrony (poziom ochrony),
*CS* – skumulowana wartość referencyjna dla cyberbezpieczeństwa (poziom cyberbezpieczeństwa).

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

$$[G01 \times G02 \times G03 \times G04\,,\ G06 \times G07 \times G08 \times G09\,,\ G14] \tag{4.3}$$

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:

$$[G01 \times G02 \times G03 \times G04 \times G05\,,\ G06 \times G07 \times G08 \times G09\,,\ G14] \tag{4.4}$$

By distinguishing through the questions, the issues for which it is possible to assign a value of “2” some technical solutions were selected, as the ones which in case of their application significantly enhance safety or security or cybersecurity. The number of questions for which a value of “2” can be assigned has been chosen so, that the maximum aggregate reference values for safety, security and cybersecurity are equal; The aggregate reference value for safety for driver-operated rolling stock includes the functionalities indicated in the control sheets RMF-G01, -G02, -G03 and RMF-G04, and for autonomous rolling stock, running without drivers, under the supervision of an automatic train operation (ATO) system, the functionalities indicated in the control sheets RMF-G01, -G02, -G03, -G04 and RMF-G05. The aggregate reference value for security includes the functionalities indicated in the control sheets RMF-G06, -G07, -G08 and RMF-G09; The aggregate reference value for cybersecurity is obtained from the control sheet RMF-G14, which refers to individual cybersecurity control sheets RMF-G10, -G11, -G12 and RMF-G13.

The use of other differentiating questions by **contractors** providing concepts and designs and by **contractors** carrying out rolling stock construction or modification is permitted. However use of another differentiating question requires obtaining written approval from the contracting authority in each case. For this, **contractor** shall contact the **internal safety coordinator**. At the same time, changes to disqualifying knock-out questions are not permitted.

For the differentiating questions, partially affirmative answers with the assignment of values from the open interval (1, 2), i.e. values greater than 1 and at the same time less than 2, are allowed.

#### 4.1.6. Determination of the level of safety, security and cybersecurity and their functional integrity level

Aggregate reference values for groups of functionalities allow the determination of aggregate reference values for safety, for security, and for cybersecurity. As stated above, each of those three aggregate values can reach a maximum of “8”. However, they can only take following values: “0”, “1”, “2”, “4”, and “8”. The aggregate reference values for safety, for security and for cybersecurity determined this way may be represented in vector form as follows:

$$[safety\,,\ security\,,\ cybersecurity] \tag{4.1}$$

that is

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

where:
*SF* – aggregate reference value for safety (safety level),
*SC* – aggregate reference value for security (security level),
*CS* – aggregate reference value for cybersecurity (cybersecurity level).

For systems, where the trains are operated by drivers, the vector takes the form of:

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

For systems, where trains are capable to run without drivers, using ATO class systems and exchanging data with ATS class systems, the vector takes the form of:

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

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

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

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.

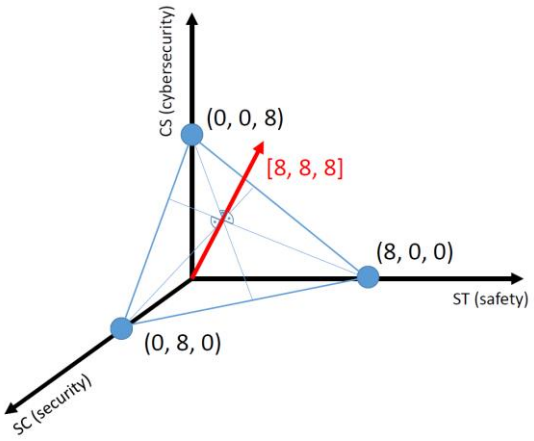
Wektorowa reprezentacja skumulowanych wartości (4.3) i (4.4) pozwala na szacunkowe określanie poziomu spójności funkcjonalnej skumulowanych wartości referencyjnych bezpieczeństwa i ochrony oraz skumulowanej wartości referencyjnej cyberbezpieczeństwa. Jeśli skumulowane wartości referencyjne są takie same, 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 celu odwzorowania takiej zależności zdefiniowano płaszczyznę odniesienia, dla której wektor (4.5) jest tzw. wektorem normalnym, tzn. prostopadłym do tej płaszczyzny, oraz przyjęto 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 $\Pi_{odn}$ 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

Poziom spójności funkcjonalnej bezpieczeństwa, ochrony i cyberbezpieczeństwa będzie wówczas obliczany z następującego wzoru:

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

In both cases (4.3) and (4.4), the maximum levels reached for vector (4.2) are:

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

For new passenger rolling stock, it is required that the safety, security and cybersecurity levels are at least 4. This means that for both safety, security and cybersecurity, at least two positive answers to the differentiating questions shall be demonstrated. At the same time, it is required that the number of positive answers for two elements of the vector [ GB, GO, CB ] shall be equal and that the third cannot differ by more than one.

Vector representation of the aggregate values (4.3) and (4.4) allows estimation of the functional integrity level of the aggregate reference values for safety and security and the aggregate reference value for cybersecurity. When the aggregate reference values are the same, their functional integrity is defined as 1.

If there are differences between these values, the integrity decreases non-linearly, first gently and then more rapidly, but does not fall to zero. In order to mimic such relationship, a reference plane was defined, for which vector (4.5) is the normal vector, i.e. perpendicular to this plane, and the sine of the angle between this plane and vector (4.3) or (4.4) was taken as a measure of the functional integrity of safety, security and cybersecurity.

Each plane in three-dimensional space is defined by three points. The plane $\Pi_{ref}$ defined by the following matrix has been taken as a reference plane:

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

in which the rows represent points and the columns their coordinates in three-dimensional space, and for which the vector (4.5) is the normal vector, as shown in Figure 6.

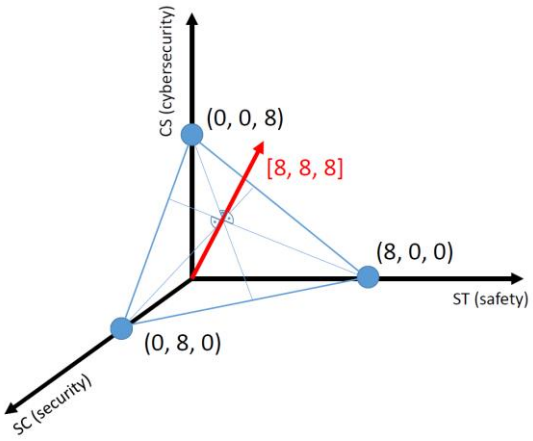



Figure 6. Reference plane normal vector

The safety, security and cybersecurity functional integrity level will then be calculated from the following formula:

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

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 powtórzeniami 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.

where:

$FIL_{SS\&C}$ – safety, security and cybersecurity functional integrity level.

Adoption of the *FIL* designation is intended to correspond with *SIL* (*Safety Integrity Level*) and shall be understood as the level of the functional integrity of safety, security and cybersecurity $FIL_{SS\&C}$ (*Functional Integrity Level for safety, security and cybersecurity*).

#### 4.1.6.1. Determining FIL value for SF, SC, CS levels expressed as integer values

The [SF, SC, CS] vector is an ordered set; Such sets composed of sets' elements are the matter of concern of combinatorics, which is defining permutations with and without repetitions as well as combinations with and without repetitions. In case of [SF, SC, CS] vector, the initial point of the vector (base) is always the point (0, 0, 0), while the terminal point representing the end of the vector (head) is the point (SF, SC, CS). Thus, we are dealing with a three-element ordered set in which each element can take any value from the set {0, 1, 2, 4, 8}. All cases in which one or more elements of the [SF, SC, CS] vector have the value "0" are the ones which disqualify the technical solution due to the lack of provision of at least one functionality, which is required from the safety, security or cybersecurity point of view. The FIL values are therefore calculated only if the coordinates of the end of the vector (head) take values from the set {1, 2, 4, 8}. We are therefore dealing with a three-element set, where the order of the elements is important and each element can take four different values.

Number of k-element combinations with repetitions from an n-element set is expressed by the formula:

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

Whereby *L* takes into account the possibility of multiple occurrences of the same value from an *n*-element set, but not the order in which they occur in a *k*-element vector.

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

It is therefore necessary to identify 20 combinations, out of which single combinations correspond to one, three or six vectors, depending on the diversity of the elements. At the same time, it shall be noted that the functional coherence of safety, security and cybersecurity do not depend on the individual vector but on the combination since all three elements are treated the same way as they are considered to be equally important. A summary of the possible FIL values is presented in the table below.

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 tablica 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 (jako wdrożonych nie w pełnym zakresie) 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 a wektorem normalnym do płaszczyzny odniesienia.

Znając wektor kierunkowy prostej $\vec{v} =$ [A, B, C] oraz wektor normalny płaszczyzny odniesienia $\overrightarrow{u} =$ [X, Y, Z], można wyliczyć kąt pomiędzy prostą i wektorem wykorzystując własności iloczynu wektorowego tych wektorów:

Table 4.1. FIL values for SF, SC, CS levels expressed as integer values

| Nº | combination | vectors | FIL values |
|---|---|---|---|
| 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 |

The table above presents FIL values for the SF, SC, CS levels expressed as integer values. However, the answers to the differentiating questions are not always fully obvious and may be partly affirmative.

#### 4.1.6.2. Determining the SF, SC, CS levels with values from an open interval (1, 2)

Relying on fully unambiguous answers to the differentiating questions is not always possible and could potentially lead to decisions not to take into account in assessment some important applied protection means (as not fully implemented) and to suggestions to consider application of some protection means safeguards also where, in the opinion of the manufacturer, they are not justified. For this reason, it is reasonable and possible to use values from an open interval (1, 2) for differentiating questions.

Determining such values requires taking into account the scale of protection ensured by protection mean and/or the scale of application of the protection mean to which the differentiating question is assigned. Both, the scale of protection and the scale of application may be less than 100%. The answer to the differentiating question shall be 1 plus percentage of protection or 1 plus percentage of application or, if both the scale of protection and the scale of application are not full from the point of view of the differentiating question, shall be 1 plus the product of the percentage of protection and percentage of application.

Consent to the use of fractional values shall be confirmed by the entity contracting the rolling stock. On the other hand, the values adopted shall be well justified as they are subject to verification as part of the assessment referred to in Chapter 4.2.

#### 4.1.6.3. Determining FIL value for SF, SC, CS levels expressed as values from an open interval (1, 2)

For the SF, SC, CS levels expressed as values from an open interval (1, 2) it is proposed to determine the sine value of an angle between vector and the reference plane on the basis of the value of an angle between the vector and the vector normal to the reference plane.

Knowing the direction vector of the straight line $\vec{v} = [A, B, C]$ and the normal vector of the reference plane $\vec{u} = [X, Y, Z]$, the angle between the line and the vector can be calculated using the cross product of these vectors.

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

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 (4.7) otrzymujemy wzór na określanie wartości FIL dla poziomów SF, SC, CS wyrażonych w postaci wartości z przedziału otwartego (1, 2).

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

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, SC i CS oraz wymaganej wartości ich spójności może opierać się zarówno na:

- bezpośrednim wskazaniu minimalnych wartości poziomów SF, SC i CS oraz spójności FIL, lub
- 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 (PVDSI – passenger vehicle digital safety index) zgodne z poniższą tablicą.

Tablica 2. Indeks cyfrowego bezpieczeństwa taboru pasażerskiego (PVDSI)

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

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

In our case, the direction vector is the vector [SF, SC, CS]. Whereas the vector normal to the reference plane can be defined for example as [8, 8, 8]. Thus, the angle between these vectors expressed in radians is:

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

The angle between the vector [SF, SC, CS] and the reference plane is $\frac{\pi}{2} - \measuredangle(\vec{v},\vec{u})$, since the angle between the vector normal to the plane and the plane is $90^o$ which is exactly $\frac{\pi}{2}$ in radians. After substituting that into formula (4.7), we obtain the formula for determining the FIL values for SF, SC, CS levels expressed as values from an open interval (1, 2).

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

The above formula allows the calculation of the *FIL* value using scientific calculators or spreadsheets, while maintaining both compliance with the general formula (4.7) and taking into account partially affirmative answers to the differentiating questions used to determine the values of the levels of safety, security and cybersecurity, presented together as a vector ( 4.2).

#### 4.1.6.4. Determining requirements for SF, SC, CS levels and their integrity by rolling stock users – passenger rolling stock digital safety index

The SF, SC and CS levels required by future user of the railway passenger rolling stock and their required integrity level can be defined on the basis of:

- expressing directly the minimum values for the SF, SC and CS levels and FIL integrity, or
- expressing directly the minimum values for the SF, SC and CS levels together with expressing maximum acceptable differentiation of the SF, SC and CS levels and minimum FIL integrity, or
- expressing the average value of the SF, SC and CS levels together with expressing maximum acceptable differentiation of the SF, SC and CS levels and minimum FIL integrity, or
- expressing required value of the PVDSI (Passenger Vehicle Digital Safety Index) in accordance with following table.

Table 2. Passenger Vehicle Digital Safety Index (PVDSI)

| PVDSI | | | | |
|---|---|---|---|---|
| PVDSI basic integrity (**FIL BI**) | SF ≥ 1 | SC ≥ 1 | CS ≥ 1 | FIL ≥ 0,7 |
| PVDSI 1 (**FIL index 1**) | SF ≥ 2 | SC ≥ 2 | CS ≥ 2 | FIL ≥ 0,8 |
| PVDSI 2 (**FIL index 2**) | SF ≥ 4 | SC ≥ 4 | CS ≥ 4 | FIL ≥ 0,9 |
| PVDSI 3 (**FIL index 3**) | SF ≥ 6 | SC ≥ 6 | CS ≥ 6 | FIL ≥ 0,9 |
| PVDSI 4 (**FIL index 4**) | SF = 8 | SC = 8 | CS = 8 | FIL = 1 |

For example, a future user of the railway passenger rolling stock may require the manufacturer to offer rolling stock characterised by a minimum value of the SF, SC, CS levels equal to the value of 2 and the FIL integrity of at least 0.88, or may require average value of the SF, SC, CS levels equal to the value of 2 and the FIL integrity of at least 0.85. However, it is recommended to define the requirements by expressing the required value of the Passenger Vehicle Digital Safety Index (PVDSI).

#### 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 [SF, SC, CS] oraz poziomu FIL funkcjonalnej spójności bezpieczeństwa, ochrony i cyberbezpieczeństwa. Rozdział ten powinien odnosić się do wszystkich ewentualnych częściowo twierdzących odpowiedzi wykorzystanych przy określaniu tych wartości.

#### 4.1.7. Conclusion of the SSC cases proving safety, security and cybersecurity integrity

Each **SSC case proving safety, security and cybersecurity integrity** shall contain a separate dedicated chapter in which contractor provides the scope of the system being assessed, as well as the resulting levels of safety, security and cybersecurity and the resulting level of safety, security and cybersecurity integrity, and the resulting PVDSI Passenger Vehicle Digital Safety Index for the rolling stock under consideration.

### 4.2. Rules regarding assessment of the railway passenger rolling stock safety, security and cybersecurity integrity

Verification of the '**SSC case proving safety, security and cybersecurity integrity**' shall be carried out by a **competent independent inspection body** accredited by the National Centre for Accreditation (recognised by EA European Accreditation) as a body assessing risk analyses and evaluations carried out in accordance with the Regulation on evaluation and assessment [6, 7] for all five structural subsystems i.e. for the "Infrastructure", "Energy", "Command and Signalling – Trackside" and "Rolling Stock" and "Command and Signalling - On-Board" subsystems. Additionally, accreditation shall cover the competence to assess safe integration in the above-mentioned areas.

The **competent independent inspection body** prepares the 'Report on the independent assessment of the SSC case proving safety, security and cybersecurity integrity'; Assessment body, assessment itself and report shall respect requirements defined in the CSM Regulation for risk assessment and evaluation [6, 7], the National Centre for Accreditation guidelines, the National Safety Authority guidelines and shall respect requirements for the report defined in this chapter.

'Report on the independent assessment of the SSC case proving safety, security and cybersecurity integrity' for the concept/design or rolling stock construction or rolling stock modification shall include following five chapters:

1. Assessment of the analysis of technical means related to ensuring traffic safety
2. Assessment of the analysis of technical means related to ensuring transport security
3. Assessment of the analysis of protection means against cyberthreats
4. Assessment of the way the level of safety, security, and cybersecurity integrity is determined
5. Conclusions from assessment of the SSC case proving safety, security and cybersecurity integrity

Chapter 1 shall include an assessment of the analysis of the technical protection means related to ensuring traffic safety, including a reference to the following aspects of the essential requirement safety: 1.1.1., 1.1.4., 1.1.5., 1.1.6., 1.1.7., 1.1.8., 1.1.10. and 1.1.11. All detailed requirements of the Technical Specifications for Interoperability related to these aspects of the essential requirement safety and all requirements of the contracting entity that are related to these aspects shall be taken into account.

Chapter 2 shall include an assessment of the analysis of the technical protection means related to ensuring transport security, including references to the following aspects of the essential requirement security: 1.1.12. and 1.1.13 defined for new passenger rolling stock.

Chapter 3 shall include an assessment of the analysis of protection means against cyberthreats, including an analysis of the full application of the principles of the Information Security Management System adopted by the railway undertaking in accordance with the EN ISO/IEC 27001 standard [8].

Chapter 4 shall confirm correctness of the calculation of the [SF, SC, CS] vector values and correct calculation of the FIL safety, security and cybersecurity functional integrity level. This chapter shall refer to all partially affirmative answers used in determining these values, if any.

**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 fazy definiowania ‘koncepcji’ taboru kolejowego 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.

The **competent independent inspection body**, which is elaborating the ‘Report on the independent assessment of the SSC case proving safety, security and cybersecurity integrity’ is obliged to include a separate chapter at the end of the report containing clear conclusions indicating a positive or a negative result of the report.

For the 'concept' phase of the rolling stock development, the verification of the ‘**SSC case proving safety, security and cybersecurity integrity**’ may be carried out by contracting entity. For this purpose contractor shall contact the internal safety coordinator of the contracting party.

The ‘Report on the assessment of the SSC case proving safety, security and cybersecurity integrity’, conducted by the **internal safety coordinator** shall be elaborated in accordance with rules defined by contracting entity.

## 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;*

## 5. Cybersecurity of the railway passenger rolling stock in operation

Operation and maintenance, also with regard to the digital solutions utilised in the railway passenger rolling stock, shall be carried out in accordance with the Operation and Maintenance Plan. Such plan shall be drawn up by the rolling stock manufacturer (and closed in phase 10. of the life cycle according to the EN 50126-1:2017) and handed over to the user together with the first unit of the respective rolling stock type. In accordance with the provisions of EN 50126-1:2017:

*The Operation and Maintenance Plans should include the following:*

1) *An explanation of operational status: The conditions that exist in each system/subsystem/hardware should be defined to provide operating and maintenance personnel with sufficient understanding during the following situations:*
    a) *start-up: this should describe the start-up conditions of the system, subsystem or hardware when power is initially applied, or following shut-down due to power interruption or other cause;*
    b) *normal operation: once the system/subsystem/hardware has successfully completed initialisation, the conditions during normal operation shall be defined;*
    c) *changeover: if the system/subsystem or hardware in which it is configured, has a facility to change over to either a cold or hot standby system/subsystem, then the conditions defined in a) and b) should be re-stated for this changeover routine. The reaction of the system/subsystem or hardware to the changing of failed modules shall also be clearly defined;*
    d) *shut-down: when a system/subsystem or hardware is shut down intentionally for a configuration change or de-commissioning, or unintentionally via a power failure, then all relevant conditions shall be defined.*
2) *maintenance should be defined in respect of:*
    a) *that undertaken on the system in-situ or at designated routine maintenance facilities;*
    b) *the repair or refurbishment of systems, subsystems or hardware that are no longer in-situ or that is taking place in facilities not classed as routine maintenance facilities, e.g. mid-life overhauls which are undertaken by the customer and the manufacturer;*
    c) *preventative maintenance;*
    d) *corrective maintenance;*
    e) *maintenance aids: for each level of maintenance, the maintenance aids available to personnel should be defined;*
3) *an analysis of human factors and competence requirements in maintenance that can influence the continued achievement of the required RAMS performance;*
4) *an analysis of human factors and competence requirements in operation that can influence the continued achievement of the required RAMS performance.*

*The operation and maintenance procedures shall be implemented, particularly with regard to system performance and life cycle cost issues. This requires considering the product, system or process in its operational environment, e.g. including the application of external risk reduction measures.*

*Compliance with RAMS requirements shall be assured throughout this life cycle phase, by:*

a) *regular review and update of operation and maintenance plans and procedures;*
b) *conformity with operational plans and procedures;*
c) *conformity with maintenance plans and procedures;*
d) *regular review of system training documentation;*
e) *regular review and update (if appropriate) of an operational Hazard Log;*
f) *ensuring compliance to the Safety-Related Application Conditions (SRACs);*
g) *investigating and handling hazardous incidents and accidents and ensuring rapid response fault finding;*

*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.

*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.*

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

*h) for systems undergoing modification, definition and implementation of mitigation actions, if applicable, to ensure the overall integrity of the system until the modification is completed or reported problems are investigated and corrected;*

*i) conformity with support agreements including logistics, spare parts, repairs, tools, calibration and quality measures to prevent or detect errors occurring during storage and transfer;*

*j) maintenance of the failure reporting and corrective action system (FRACAS).*

*NOTE 1 The operational Hazard Log is based on the Hazard Record extracted from the Hazard Log resulting from life cycle phase 10.*

With regard to the above-mentioned provisions of the standard, attention shall be paid to the correct interpretation of the above-mentioned provisions concerning the operation and maintenance of rolling stock in relation to its digital equipment, taking into account both hardware and software components.

The Operation and Maintenance Plan provided to the user shall be supplemented and updated by the railway rolling stock user. In accordance with the provisions of EN 50126-1:2017:

*The review and updates of the Operation and Maintenance Plan shall include issues raised and addressed during the initial operation and maintenance phase and at applicable stages thereafter.*

*It shall be implemented a process for:*

*a) the acquisition of RAMS performance data;*

*b) recording of RAMS performance data, associated analysis and evaluation as applicable, e.g. by means of a FRACAS.*

*Throughout the operational lifetime the system baseline shall be recorded and kept traceable under configuration management control.*

*NOTE 2 This is of special importance when critical faults are discovered and need to be corrected in more than one installation. Manufacturers and maintainers might need to implement complementary arrangements for configuration management, so that the manufacturer can trace the baseline of systems provided to particular customers and individual maintainers can trace the location of individual items.*

This requires the rolling stock user to implement and utilise not only the Operation and Maintenance Plan, but also a configuration management control for the rolling stock, including in particular the configuration in relation to digital rolling stock equipment including both hardware and software components.

*The FRACAS process is required to continuously provide feedback to the operations safety manager, the designer, manufacturer, operations manager and maintenance manager regarding any failures and defects (and possible causes) found during operational service, Failures will potentially have a variety of causes including component failures, operational errors, maintenance and other errors. It is therefore imperative that the reporting process is clear and logical and that there is a collective forum for all stakeholders to agree the most likely source of failure and hence investigation and corrective actions.*

Appropriate supervision of the operation, and maintenance works, requires implementing and maintaining of FRACAS (Failure Reporting Analysis and Corrective Action System). In accordance with the provisions of EN 50126-1:2017:

*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.

*NOTE 3*

1) *Complementary FRACAS records can need to be kept by different entities. Maintenance organisations might have a generic FRACAS which covers many different types of system for which they are responsible, while manufacturers can have a FRACAS which encompasses systems supplied to a variety of different customers. The manufacturer can be able to diagnose component failures which are not accessible to the maintainer.*

2) *Referencing of accidents, hazards and causes will preferably be consistent within the safety case and other performance monitoring tools and processes. This will help respective organisations to align issues and identify trends.*

*The FRACAS shall be maintained throughout the operation and maintenance life cycle. To ensure that priority issues are addressed, the failures and defects should be categorised for both safety and reliability for varying levels of severity/criticality. As a minimum, the FRACAS shall be populated with information about failures and defects identified during operation and maintenance. This information shall include:*

*a) time of the failure;*

*b) cause of the failure;*

*c) detailed description of the failure;*

*d) corrective action taken;*

*e) safety ranking for the failure;*

*f) when and how the failures and defects have been detected (e.g. in operation or during a scheduled maintenance);*

*g) the effects of the failures and defects up to the railway system level.*

*The FRACAS records shall be periodically reviewed to determine whether any improvement is needed in the following:*

*h) Operation and maintenance procedures and manuals;*

*i) System training documentation;*

*j) Operational Hazard Log;*

*k) System design;*

*l) Human factors aspects of operation and maintenance.*

*When changes are proposed an impact analysis shall be performed on each change request. The analysis shall include reviewing the impact on:*

*m) the system/subsystem or hardware operational/functional safety performance;*

*n) the system/subsystem/hardware interfaces;*

*o) adjacent system/subsystem or hardware operational/functional safety performance;*

*p) the modification installation work, with consideration given to adjacent system/subsystem and hardware that can be affected due to systematic failures.*

*The impact analysis shall result in a decision on which parts of the safety life cycle will be repeated for the modification, all relevant documentation for the effected life cycle steps shall be updated, with equal depth and quality as the original documentation that was produced during the development of the system. The details and results of the modification, risk analysis and testing shall be included in the safety case.*

*All changes and system/subsystem or hardware identified as being at risk shall be tested for correct operation on completion of the change.*

*For each identified recommendation a decision shall be taken whether the recommendation shall be realised or not. These decisions shall be justified and recorded.*

With regard to the above-mentioned provisions of the standard, attention shall be paid to the correct interpretation of the above-mentioned provisions concerning the operation and maintenance of rolling stock in relation to its digital equipment, taking into account both hardware and software components.

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.

Provisions of Chapter 5 of the ‘Recommendations regarding railway passenger rolling stock cybersecurity’ should apply also to railway passenger rolling stock put in service before adoption of the recommendations or without applying them, whereby:

- Both the manufacturer and the user may take the initiative to include a certain type of the railway passenger rolling stock in the relevant systems/documents – Maintenance and Operations Plan, rolling stock configuration management system, and FRACAS (Failure Reporting Analysis and Corrective Action System).
- Whichever party takes the initiative to include a certain type of the railway passenger rolling stock in the relevant systems, both parties shall cooperate in the development and implementation of the respective systems/documents.
- The manufacturer of a certain type of the railway passenger rolling stock shall be entitled to use the developed systems/documents also for the rolling stock of the same type utilised by other users and for the railway passenger rolling stock which is being produced by manufacturer or another licensed business entity which is using the same or similar hardware and/or software solutions.
- The user of a certain type of rolling stock, which is involved in the development of the systems/documents shall start using them in the maintenance and operation processes as soon as the development of the systems/documents has been finalised.
- The user of a certain type of rolling stock, which is not involved in the development of the systems/documents shall start using them in the maintenance and operation processes as soon as they have been made available by the manufacturer of a certain type of rolling stock.
- Each user of a certain type of the railway passenger rolling stock has the right to modify these systems/documents within the process of improving the way the work is organised and for the purpose of adaptation to the operational and maintenance conditions applicable to that user's rolling stock.

## 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**.

## 6. Cybersecurity of the altered/modified rolling stock

Introducing changes in rolling stock requires the use of risk analysis and evaluation in accordance with binding requirements of the Risk Evaluation and Assessment Regulation [6, 7] to identify and confirm the elimination of any unacceptable risks and the identification and mitigation of any tolerable risks requiring oversight by the railway undertaking and/or by respective Entity in Charge of Maintenance ECM during operation and maintenance of passenger rolling stock.

Introducing changes in rolling stock can affect, among others, its cybersecurity, so the risk analysis and evaluation referred to the above mentioned regulation shall cover possible changes within software based systems/subsystems/components.

The introduction of changes shall be accompanied by the revision of the Maintenance and Operations Plan, the revision of the rolling stock configuration management system, and the revision of the FRACAS (Failure Reporting Analysis and Corrective Action System), or by their development and implementation.

The introduction of changes within software based systems/subsystems/components and/or within on-board and wireless data exchange networks, as well as within configurations, including the relationship between systems/subsystems/components and the data exchange networks should:

- be based on the use of the complete documentation of the digital component,
- keep the structure of the on-board data exchange networks, including the principles of the separation of the sub-networks utilised for different functions,
- ensure, that software changes are based on source code rather than modifying the executable soft using e.g. AI based tools and/or reverse engineering,
- take into account aspects, which are pointed in the cybersecurity control sheets for individual systems/subsystems/components (G10÷G13) and in the overall cybersecurity control sheet (G14) which are given in this recommendation,
- ensure, that SSC case proving safety, security and cybersecurity integrity is developed (or updated) and evaluated.

## 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


--- ---

## 7. Reference documents

The following reference documents were utilised for the development of the “Recommendations regarding railway rolling stock cybersecurity”:

EU legal documents:
- EU European Parliament and Council formal documents:
1. Directive (EU) 2016/797 of the European Parliament and of the Council of 11 May 2016 on the interoperability of the rail system within the European Union (EU.OJ L 138/44 of 26.05.2016)
2. Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union (EU.OJ L 194/1 of 19.7.2016)
3. Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive)
4. Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities and repealing Council Directive 2008/114/EC
5. Regulation (EU) 2021/782 of the European Parliament and of the Council of 29 April 2021 on rail passengers’ rights and obligations

- European Commission formal documents:
6. Commission Implementing Regulation (EU) No 402/2013 of 30 April 2013 on the common safety method for risk evaluation and assessment and repealing Regulation (EC) No 352/2009 (EU.OJ L 121/8 of 03.05.2013)
7. Commission Implementing Regulation (EU) 2015/1136 of 13 July 2015 amending Implementing Regulation (EU) No 402/2013 on the common safety method for risk evaluation and assessment (EU.OJ L 185/6 of 14.07.2015)

referenced standards and normative documents:
- European standards adopted by CEN, CENELEC, ETSI
8. EN ISO/IEC 27001:2017 Information technology - Security techniques - Information security management systems - Requirements (ISO/IEC 27001:2013 incl. Cor 1:2014 & Cor2:2015)
9. EN 50126-1:2017 Railway Applications - The Specification and Demonstration of Reliability, Availability, Maintainability and Safety (RAMS) - Part 1: Generic RAMS Process
10. EN 50126-2:2017 Railway Applications - The Specification and Demonstration of Reliability, Availability, Maintainability and Safety (RAMS) - Part 2: Systems Approach to Safety
11. EN 50128:2011+A2:2020 Railway applications - Communication, signalling and processing systems - Software for railway control and protection systems, and
    EN 50657:2017 Railway applications - Rolling stock applications - Software onboard of rolling stock, which are both replaced in 2023 by following standard
    EN 50716:2023 Cross-functional Software Standard for Railways
12. EN 50129:2018 Railway applications - Communication, signalling and processing systems - Safety related electronic systems for signalling
13. EN 50159:2010 Railway applications - Communication, signalling and processing systems - Safety-related communication in transmission systems
14. Set of standards EN ISO/IEC 62443 Security for industrial automation and control systems

--- ---