miesięcznik naukowo-techniczny Wydawnictwa SITK RP sp. z o.o.

przegląd komunikacyjny

1
2024
rocznik LXXIX
cena 27,00 zł
w tym 8% VAT

UKAZUJE SIĘ OD 1945 ROKU

Stowarzyszenie Inżynierów i Techników Komunikacji RP
Zarząd Krajowy

INSTYTUT KOLEJNICTWA

VI Konferencja Naukowo-Techniczna

IT/OT w Transporcie Szynowym 2023*

Warszawa 29 - 31 stycznia 2024 r.

*Edycja 2023 przesunięta na rok 2024

Ministerstwo Edukacji i Nauki

Projekt dofinansowany ze środków budżetu państwa, przyznanych przez Ministra Edukacji i Nauki w ramach Programu Doskonała Nauka II.

Cyberbezpieczeństwo w transporcie szynowym – wyzwania i rozwiązania, w tym podsumowanie konferencji IT/OT w Transporcie Szynowym. Nowoczesne podejście do systemów telematycznych na przykładzie Pomorskiej Kolei Metropolitalnej. Diagnostyka i utrzymanie systemów sterowania ruchem kolejowym na odległość - bezpieczny zdalny dostęp do systemów kluczowych. Powszechnie przyjęte rozwiązania - sposób zapewnienia cyberbezpieczeństwa w produkcie.

eISSN
2544-6037

ISSN
0033-22-32

Podstawowe informacje dla Autorów artykułów

„Przegląd Komunikacyjny" publikuje artykuły związane z szeroko rozumianym transportem oraz infrastrukturą transportu. Obejmuje to zagadnienia techniczne, ekonomiczne i prawne. Akceptowane są także materiały związane z geografią, historią i socjologią transportu.

Artykuły publikowane w „Przeglądzie Komunikacyjnym" dzieli się na: „wnoszące wkład naukowy w dyscypliny: inżynieria lądowa i transport; ekonomia i finanse; nauki prawne; nauki socjologiczne. Prosimy Autorów o deklarację (w zgłoszeniu), do której dyscypliny zaliczyć ich prace.

Materiały do publikacji: zgłoszenie, artykuł oraz oświadczenie Autora, należy przesyłać w formie elektronicznej na adres piotr.mackiewicz@pwr.edu.pl:

artykuly@przeglad.komunikacyjny.pwr.wroc.pl

W zgłoszeniu należy podać: imię i nazwisko autora, adres mailowy oraz adres do tradycyjnej korespondencji, miejsce zatrudnienia, zdjęcie, tytuł artykułu oraz streszczenie (po polsku i po angielsku) i słowa kluczowe (po polsku i po angielsku). Szczegóły przygotowania materiałów oraz wzory załączników dostępne są ma stronie:

www.transportation.overview.pwr.edu.pl

W celu usprawnienia i przyspieszenia procesu publikacji prosimy o zastosowanie się do poniższych wymagań dotyczących nadsyłanego materiału:

1. Tekst artykułu powinien być napisany w jednym z ogólnodostępnych programów (np. Microsoft Word). Wzory i opisy wzorów powinny być wkomponowane w tekst. Tabele należy zestawić po zakończeniu tekstu. Ilustracje (rysunki, fotografie, wykresy) najlepiej dołączyć jako oddzielne pliki. Można je także wstawić do pliku z tekstem po zakończeniu tekstu. Możliwe jest oznaczenie miejsc w tekście, w których autor sugeruje wstawienie stosownej ilustracji lub tabeli. Obowiązuje odrębna numeracja ilustracji (bez rozróżniania na rysunki, fotografie itp.) oraz tabel.
2. Całość materiału nie powinna przekraczać 12 stron w formacie Word (zalecane jest 8 stron). Do limitu stron wlicza się ilustracje załączane w odrębnych plikach (przy założeniu że 1 ilustracja = ½ strony).
3. Format tekstu powinien być jak najprostszy (nie stosować zróżnicowanych styli, wcięć, podwójnych i wielokrotnych spacji itp.). Dopuszczalne jest pogrubienie, podkreślenie i oznaczenie kursywą istotnych części tekstu, a także indeksy górne i dolne. **Nie stosować przypisów.**
4. Nawiązania do pozycji zewnętrznych - cytaty (dotyczy również podpisów ilustracji i tabel) oznacza się numeracją w nawiasach kwadratowych [...]. Numerację należy zestawić na końcu artykułu (jako „Materiały źródłowe"). Zestawienie powinno być ułożone alfabetycznie.
5. Jeżeli Autor wykorzystuje materiały objęte nie swoim prawem autorskim, powinien uzyskać pisemną zgodę właściciela tych praw do publikacji (niezależnie od podania źródła). Kopie takiej zgody należy przesłać Redakcji.

Artykuły wnoszące wkład naukowy w dyscypliny: inżynieria lądowa i transport, inżynieria lądowa i transport; ekonomia i finanse; nauki prawne; nauki socjologiczne podlegają procedurom recenzji merytorycznych zgodnie z wytycznymi MNiSW, co pozwala zaliczyć je, po opublikowaniu, do dorobku naukowego oraz uwzględnić w ewaluacji jakości działalności naukowej (Dz.U. 2019 poz. 392).

Liczba uwzględnianych punktów wg listy czasopism punktowanych przez MNiSW wynosi 20.

Do oceny każdej publikacji powołuje się co najmniej dwóch niezależnych recenzentów spoza jednostki. Zasady kwalifikowania lub odrzucenia publikacji i ewentualny formularz recenzencki są podane do publicznej wiadomości na stronie internetowej czasopisma lub w każdym numerze czasopisma. Nazwiska recenzentów poszczególnych publikacji/numerów nie są ujawniane.

Przygotowany materiał powinien obrazować własny wkład badawczy autora. Redakcja wdrożyła procedurę zapobiegania zjawisku Ghostwriting (z „ghostwriting" mamy do czynienia wówczas, gdy ktoś wniósł istotny wkład w powstanie publikacji, bez ujawnienia swojego udziału jako jeden z autorów lub bez wymienienia jego roli w podziękowaniach zamieszczonych w publikacji). Tekst i ilustracje muszą być oryginalne i niepublikowane w innych miejscach (w tym w internecie). Możliwe jest zamieszczanie artykułów, które ukazały się w materiałach konferencyjnych i podobnych (na prawach rękopisu) z zaznaczeniem tego faktu i po przystosowaniu do wymogów publikacyjnych „Przeglądu Komunikacyjnego".

Na stronie internetowej czasopisma dostępne są pełne wersje artykułów wraz ze streszczeniami w języku polskim (od 2010) i angielskim (od 2016) jako OPEN ACCESS. Pod koniec 2018 roku „Przegląd Komunikacyjny" rozpoczął indeksowanie artykułów angielskich z użyciem numerów cyfrowych DOI. Czasopismo ubiega się o partycypowanie w bazie SCOPUS. Rejestrowane jest w międzynarodowej baza DOAJ https://doaj.org/.

Redakcja pisma oferuje objęcie patronatem medialnym konferencji, debat, seminariów itp.
Ceny są negocjowane indywidualnie w zależności od zakresu zlecenia. Możliwe są atrakcyjne upusty. Patronat obejmuje:

- ogłaszanie przedmiotowych inicjatyw na łamach pisma,
- zamieszczanie wybranych referatów / wystąpień po dostosowaniu ich do wymogów redakcyjnych,
- publikację informacji końcowych (podsumowania, apele, wnioski),
- kolportaż powyższych informacji do wskazanych adresatów.

www.transportation.overview.pwr.edu.pl

Ramowa oferta dla „Sponsora strategicznego" czasopisma Przegląd Komunikacyjny

Sponsor strategiczny zawiera umowę z wydawcą czasopisma na okres roku kalendarzowego z możliwością przedłużenia na kolejne lata. Uprawnienia wydawcy do zawierania umów posiada Spółka Wydawnictwa SITK RP sp. z o.o..

Przegląd Komunikacyjny oferuje dla sponsora strategicznego następujące świadczenia:

- **zamieszczenie logo sponsora w każdym numerze,**
- **zamieszczenie reklamy sponsora w jednym, kilku lub we wszystkich numerach,**
- **publikacja jednego lub kilku artykułów sponsorowanych,**
- **publikacja innych materiałów dotyczących sponsora,**
- **zniżki przy zamówieniu prenumeraty czasopisma.**

Możliwe jest także zamieszczenie materiałów od sponsora na stronie internetowej czasopisma.
Przegląd Komunikacyjny ukazuje się jako miesięcznik.
Szczegółowy zakres świadczeń oraz detale techniczne (formaty, sposób i terminy przekazania) są uzgadniane indywidualnie.

Osoba kontaktowa w tej sprawie:
Hanna Szary
hanna.szary@sitkrp.org.pl
ul. Świętokrzyska 14 A , lok. 150 , 00-050 Warszawa, tel.: (22) 336 12 06, 506 116 966

Cena za świadczenia na rzecz sponsora uzależniana jest od uzgodnionych szczegółów współpracy. Zapłata może być dokonana jednorazowo lub w kilku ratach (na przykład kwartalnych). Część zapłaty może być w formie zamówienia określonej liczby prenumerat czasopisma.

przegląd komunikacyjny
1/2024 rocznik LXXIX

Szanowni Państwo, pleno titulo czytelnicy Przeglądu Komunikacyjnego

Oddajemy w Państwa ręce numer specjalny Przeglądu Komunikacyjnego dedykowany systemom informacyjnym IT i eksploatacyjnym OT w transporcie szynowym podsumowujący Konferencję IT&OT w Transporcie Szynowym, która miała miejsce w dniach 29-30-31 stycznia 2024 r. oraz przedstawiający kluczowe wyzwania i proponowane rozwiązania w tym zakresie.

Większość osób mimo korzystania z technologii cyfrowych nie zdaje sobie sprawy z tego jak bardzo świat stał się cyfrowy w ostatnich latach i jak bardzo jest on obecnie usieciowiony. Dotyczy to także transportu kolejowego i innych rodzajów transportu szynowego, a także innych rodzajów transportu. Z jednej strony dzięki przetwarzaniu cyfrowych danych zyskaliśmy i nadal zyskujemy coraz lepsze usługi z drugiej nieodwracalnie do systemów transportowych wkradają się różnego rodzaju ryzyka związane z gromadzeniem, przechowywaniem, przetwarzaniem, transmisją i wykorzystywaniem danych, którym towarzyszyć musi stosowanie odpowiednich zabezpieczeń. Dotychczas eksperci poświęcali czas na zagwarantowanie, że pociągi nie będą się zderzały, wykolejały, płonęły, a teraz muszą zadbać jeszcze o poufność, integralność i dostępność danych – o coraz szerzej znane CIA (ang. confidentiality, integrity, accessibility).

Wyzwaniem jest nie tylko nowa grupa ryzyk, które w niesprzyjających warunkach mogą być równie groźne jak te od zawsze związane z transportem, ale także dysproporcja w dynamice rozwoju stosowanych rozwiązań technicznych. Podmioty kolejowe budują infrastrukturę na sto-kilkadziesiąt lat, i stosując odpowiednie procedury utrzymania ograniczają się do prowadzenia większych prac tzw. modernizacji co lat kilkadziesiąt. Pojazdy kolejowe są budowane na lat kilkadziesiąt. Czterdzieści lat eksploatacji pojazdu to niemal standard, a niektóre pojazdy eksploatowane są wyraźnie dłużej. Takie podejście do trwałości stosowanych rozwiązań, skądinąd słuszne, w zderzeniu z dynamicznym rozwojem technik informatycznych stanowi nie lada wyzwanie. Sześć lat w systemach IT to epoka. W systemach eksploatacyjnych OT czas nie płynie tak szybko, ale systemy te w wielu istotnych elementach bazują na rozwiązaniach sprzętowych i programowych projektowanych, produkowanych, utrzymywanych dla systemów informacyjnych IT.

Zwrócić należy także uwagę, na postrzeganie cyberzagrożeń wyłącznie jako zagrożeń płynących z cyberprzestrzeni rozumianej jako internet. To półprawda. Cyberzagrożenia dotyczą także urządzeń i systemów nie podłączonych do sieci internet. Szacuje się, że najszerzej znany robak stuxnet, zidentyfikowany w 2009 roku, zainfekował nawet kilka tysięcy instalacji przemysłowych nie podłączonych do internetu, bo rozprzestrzeniał się przede wszystkim na pamięciach USB.

Kolejowe systemy sterowania ruchem i bezpiecznej kontroli jazdy, podobnie jak cyfrowe systemy łączności przewodowej i bezprzewodowej, czy systemy zdalnego sterowania np. urządzeniami zasilania, ogrzewaniem rozjazdów, oświetleniem, a także systemy diagnostyczne, korzystają z gromadzenia, przetwarzania, przekazywania danych w formie cyfrowej. Nawet jeśli systemy kolejowe nie są połączone z siecią internet, to wzdłuż linii kolejowych, w studzienkach kablowych, w szafach aparatowych, w kontenerach, mogą mieć miejsce nieuprawnione ingerencje. Tymczasem do najgroźniejszych cyberataków zalicza się ataki przygotowywane przez zorganizowane grupy, które najpierw, często miesiącami, monitorują pracę systemów, by przygotować dedykowany cyberatak, który we właściwym z ich punktu widzenia momencie, wstrzyma transport lub uszkodzi systemy lub doprowadzi do katastrofy.

Podobnie współczesny tabor kolejowy, postrzegany przez pasażerów często jako przestrzeń na kołach z ogrzewaniem i oświetleniem, holowana przez lokomotywę po torach, w rzeczywistości jest jednocześnie siecią cyfrowych rozwiązań przemysłowych. Maszynista z odległości po kablach steruje silnikami na wózkach napędnych, drzwiami i stopniami wysuwnymi, oświetleniem, ogrzewaniem, wentylacją w przestrzeni pasażerskiej, pantografami, itd. W zakresie diagnostyki, informacji pasażerskiej, rozliczania energii trakcyjnej, łączności z dyżurnymi ruchu, itd. wykorzystywane są także cyfrowe połączenia bezprzewodowe. W celu włączenia się w transmisję bezprzewodową nie trzeba nawet wchodzić na teren kolei.

Tym samym zarówno specjaliści zajmujący się infrastrukturalnymi systemami i urządzeniami sterowania, łączności, zasilania jak i specjaliści zajmujący się taborem kolejowym nie tylko mogą, ale wręcz powinni uważnie śledzić Konferencję IT&OT w Transporcie Szynowym jako pierwsze źródło informacji o dynamicznie zmieniających się uwarunkowaniach bezpieczeństwa transportu kolejowego w zakresie rozwiązań cyfrowych, programowalnych i komputerowych szeroko wykorzystywanych w taborze i infrastrukturze transportu szynowego.

Rada Programowa Konferencji IT/OT w Transporcie Szynowym

dr inż. Jacek Paś, Prezes SITK RP,
dr inż. Wawrzyniec Wychowański, Sekretarz Generalny SITK RP,
dr hab. inż. Marek Pawlik, prof. IK, Zastępca dyrektora Instytutu Kolejnictwa, Przewodniczący ISAC-Kolej

W numerze

Wydawca:
Wydawnictwa SITK RP sp. z o.o.
ul. Świętokrzyska 14 A , lok. 150 , 00-050 Warszawa
www.sitkrp.org.pl
Wawrzyniec Wychowański – Prezes

Redaktor Naczelny:
Antoni Szydło

Redakcja:
Maciej Kruszyna (Z-ca Redaktora Naczelnego), Agnieszka Kuniczuk - Trzcinowicz (Redaktor językowy), Piotr Mackiewicz (Sekretarz), Wojciech Puła (Redaktor statystyczny), Eryk Mączka (obsługa techniczna, strona internetowa), Krzysztof Gasz, Jarosław Kuźniewski, Łukasz Skotnicki, Bartłomiej Krawczyk, Igor Gisterek, Karina Korycka (obsługa anglojęzyczna)

Adres redakcji do korespondencji:
Poczta elektroniczna:
redakcja@przeglad.komunikacyjny.pwr.wroc.pl
Poczta „tradycyjna":
Piotr Mackiewicz, Maciej Kruszyna
Politechnika Wrocławska,
Wybrzeże Wyspiańskiego 27, 50-370 Wrocław
Faks: 71 320 45 39

Rada naukowa:
Marek Ciesielski (Poznań), Antanas Klibavičius (Wilno), Jozef Komačka (Žilina), Elżbieta Marciszewska (Warszawa), Andrzej S. Nowak (Auburn University), Tomasz Nowakowski (Wrocław), Victor V. Rybkin (Dniepropietrovsk), Marek Sitarz (Katowice), Wiesław Starowicz (Kraków), Hans-Christoph Thiel (Cottbus), Tomasz Siwowski (Rzeszów), Jiri Strasky (Brno), Andrea Zuzulova (Bratysława)

Deklaracja o wersji pierwotnej czasopisma
Główną wersją czasopisma jest wersja elektroniczna. Na stronie internetowej czasopisma dostępne są pełne wersje artykułów wraz ze streszczeniami w języku polskim (od 2010) i angielskim (od 2016).

Redakcja zastrzega sobie prawo dokonywania zmian w materiałach nie podlegających recenzji.

Artykuły opublikowane w „Przeglądzie Komunikacyjnym" są dostępne w bazach danych 20 bibliotek technicznych oraz są indeksowane w bazach:

BAZTECH: **http://baztech.icm.edu.pl**
Index Copernicus: **http://indexcopernicus.com**
Międzynarodowa baza DOAJ **https://doaj.org/**

Prenumerata:
Szczegóły i formularz zamówienia na stronie:
http://www.transportation.overview.pwr.edu.pl

Obecna Redakcja dysponuje numerami archiwalnymi począwszy od 4/2010.

Numery archiwalne z lat 2004-2009 można zamawiać w Oddziale krakowskim SITK, ul. Siostrzana 11, 30-804 Kraków, tel./faks 12 658 93 74, **mrowinska@sitk.org.pl**

Druk:
Grupa Intromax Sp. z o.o, ul. Biskupińska 21, 30-732 Kraków, http://www.intromax.com.pl/

Reklama:
Dział Marketingu:
hanna.szary@sitkrp.org.pl,
elzbieta.nowicka@sitkrp.com,

Nakład: 800 egz.

Cyberbezpieczeństwo w transporcie szynowym – wyzwania i rozwiązania, w tym podsumowanie konferencji IT/OT w Transporcie Szynowym

Cybersecurity in rail transport – challenges and solutions, including a summary of the IT/OT conference in rail transport

Marek Pawlik

Dr hab. inż., prof. IK

zast. dyr. Instytutu Kolejnictwa, przewod. ISAC-Kolej, członek Komitetu Naukowego Konferencji IT/OT w Transporcie Szynowym

mpawlik@ikolej.pl

Streszczenie: Artykuł przedstawia wyzwania i rozwiązania w zakresie cyberbezpieczeństwa transportu szynowego bazując na prezentacjach i dyskusjach jakie miały miejsce podczas Konferencji Naukowo-Technicznej IT/OT w Transporcie Szynowym 2023, która miała miejsce w dniach 29-31 stycznia 2024 r. Tak jak podczas konferencji artykuł rozpoczyna się od przedstawienia wyzwania z lotu ptaka, przechodzi do krótkiego przeglądu omawianych kwestii szczegółowych by dojść do sposobów budowania kompetencji pracowników oraz wytycznych dla cyberbezpieczeństwa kolei.

Słowa kluczowe: *Infrastruktura Transportowa; Sterowanie Ruchem; Łączność; Pojazdy Kolejowe; Cyberbezpieczeństwo*

Abstract: Paper presents challenges and solutions regarding rail transport cybersecurity on the basis of the presentations and discussions that took place during the IT/OT in Rail Transport 2023 Scientific and Technical Conference, which took place on the 29th -31st January 2024. As at the conference, paper starts with helicopter view of the state of the art of cybersecurity in rail transport, proceeds to an overview of the specific issues discussed during conference, to reach the ways appropriate for staff competence building and guidelines for railway cybersecurity.

Keywords: *Transport Infrastructure; Control Command & Signalling; Communication; Rolling Stock; Cybersecurity*

Wstęp

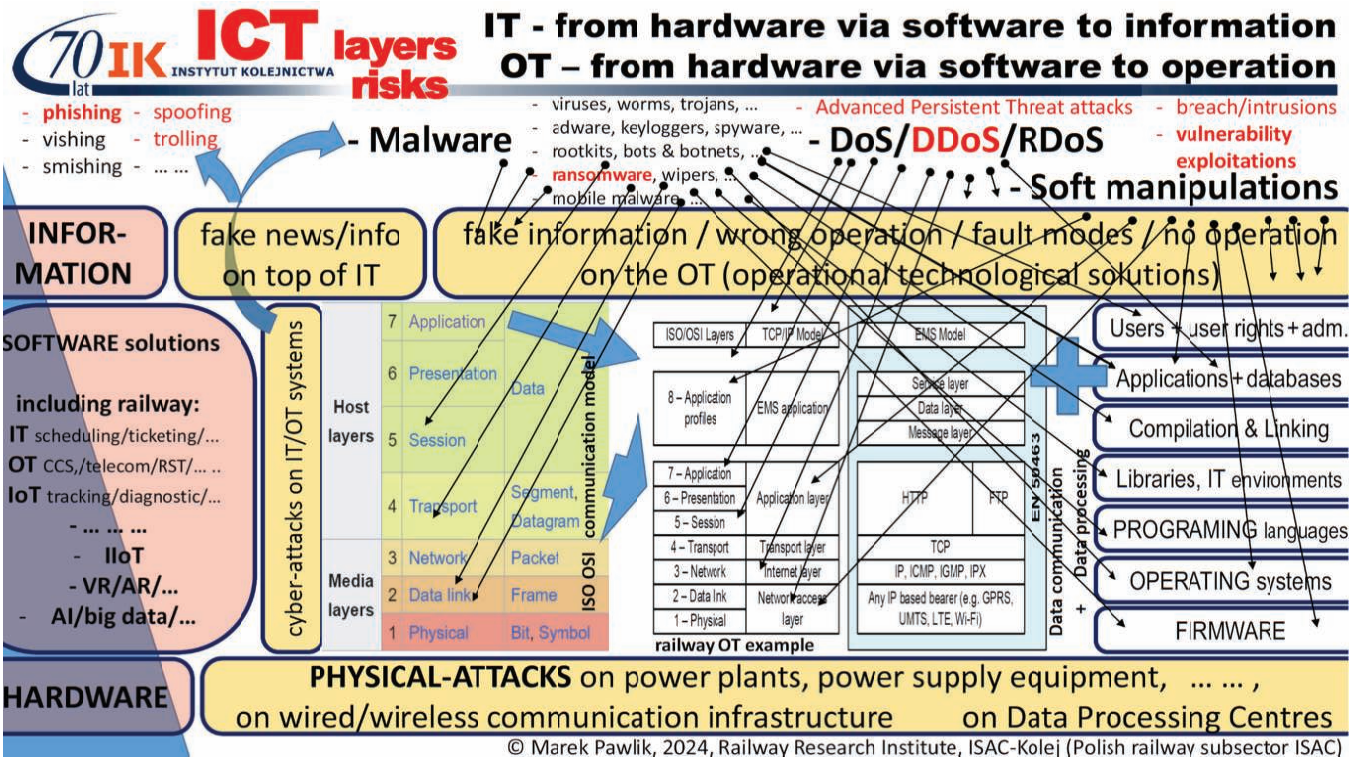
W dniach 29-31 stycznia 2023 miała miejsce Konferencja Naukowo-Techniczna IT/OT w Transporcie Szynowym 2023. Formalnie szósta, ale pierwsza w nowej odsłonie. Wcześniejsze konferencje organizowane przez SITK RP koncentrowały się na wspieraniu transportu przez systemy informatyczne. Ta po raz pierwszy była współorganizowana przez Zarząd Główny SITK RP oraz Instytut Kolejnictwa i miała o wiele szerszy zakres merytoryczny. Podjęty został szerszy temat – systemy informacyjne IT oraz systemy eksploatacyjne OT. Tym samym konferencja objęła wyzwania i rozwiązania cyfrowe także w sterowaniu ruchem kolejowym, zasilaniu, łączności, czy budowie i eksploatacji taboru kolejowego. Zmieniła się także formuła konferencji. Stała się ona międzynarodowa w odniesieniu do treści i uczestników, nowoczesna w zakresie środków oraz powiązana z budowaniem kompetencji i wiedzy, także poprzez możliwość udziału w wizycie technicznej.

Podnoszone i omawiane były tematy bardzo zyskujące obecnie na znaczeniu. Świat, także kolejowy, stał się bardzo cyfrowy, a jednocześnie trwa konflikt w cyberprzestrzeni, o czym informują nawet przedstawiciele wojska. Jesteśmy też w przededniu wejścia w życie *Dyrektywy w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii (2022/2555)*, zgodnie z zapisami której zarządcy kolejowej infrastruktury i przewoźnicy kolejowi, którzy zatrudniają więcej niż 49 osób lub posiadają obroty, względnie roczną sumę bilansową, powyżej 10 milionów euro, będą jeszcze w roku 2024 zobowiązani do zidentyfikowania własnych usług i systemów wykorzystujących rozwiązania cyfrowe oraz wdrożenia procedur: identyfikowania cyberzagrożeń, doskonalenia zabezpieczeń przed cyberzagrożeniami, i raportowania cyberataków i cyberincydentów.

Tym samym, bez żadnej wątpliwości, zasadne jest wykorzystanie informacji przekazanych podczas Konferencji IT/OT w Transporcie Szynowym do uporządkowania wiedzy o wyzwaniach i proponowanych rozwiązaniach, czemu służyć ma niniejsza publikacja.

Widok z lotu ptaka na cyberwyzwania

Nie tylko pasażerowie nie dostrzegają złożoności cyfrowych rozwiązań wykorzystywanych w transporcie szynowym. Jest ona pochodną obecnie stosowanych rozwiązań cyfrowych wspierających funkcjonowanie nie



1. *Widok z lotu ptaka na cyberwyzwania*

tylko podmiotów gospodarczych, ale także państw i społeczeństw.

Wszyscy wiemy, że pod spodem jest hardware, a całkiem na górze informacja. Zwykle hardware kojarzy nam się z naszym komputerem, tymczasem z perspektywy społeczeństw, państw, czy transportu szynowego hardware to elektrownie, sieci energetyczne, obiekty i sieci telekomunikacyjne, czy centra przetwarzania danych. Ataki fizyczne na tak rozumiany hardware mogą sparaliżować transport. Obrona przed takimi atakami to domena wojska.

Wszyscy wiemy, że możliwe i wykorzystywane są manipulacje informacjami. Nikogo już nie zaskakuje fakt pojawiania się fake newsów w dobie oprogramowania typu DeepFake oraz dynamicznego rozwoju sztucznej inteligencji. Przed dezinformacją w środkach masowego przekazu, ale także w sieciach społecznościowych chronić mają nas dedykowane zespoły funkcjonujące w ramach Krajowych Zespołów Reagowania na Incydenty Bezpieczeństwa Komputerowego CSIRT.

Pomiędzy hardwarem a informacjami mamy software – oprogramowanie. Jako software postrzegamy przede wszystkim nasze oprogramowanie biurowe oraz systemy operacyjne, bez których to oprogramowanie nie działa. Tymczasem do funkcjonowania systemów informacyjnych IT i systemów eksploatacyjnych OT konieczny jest firmware czyli oprogramowanie układowe, bez którego nie działają prawidłowo komponenty sprzętowe, konieczne są systemy operacyjne, języki programowania, związane z nimi biblioteki i środowiska cyfrowe, kompilatory i linkery, dzięki którym powstają programy wykonywalne oraz wykorzystywane przez nie struktury na przykład bazy danych. Poszczególne komputery, serwery i centra przetwarzania danych oraz sterowniki, kontrolery, czy terminale wymieniają dane dla których zachowane musi być cyberbezpieczeństwo rozumiane jako CIA, angielskie Confidentiality, Integrity, Accessibility czyli poufność, integralność i dostępność. Fizyczna reprezentacja transmitowanych danych, zer i jedynek, zależy od środka transmisji. Warstwa fizyczna to jednak dopiero początek. Ogólny model ISO OSI wyróżnia siedem warstw transmisji w systemach informatycznych: warstwę fizyczną, warstwę łącza danych, sieciową, transportową, sesji, prezentacji i warstwę aplikacji. W praktyce warstwy zależą od stosowanych rozwiązań, trzy dolne od rozwiązań w zakresie mediów transmisyjnych a cztery górne od rozwiązań w zakresie narzucanym przez hosta. Inny jest podział funkcji i relacji dla stron internetowych (http), a inny dla serwerów udostępniania plików (ftp). Przesyłanie danych w systemach wspomagających transport szynowy ma miejsce zarówno lokalnie, jak i na duże odległości. Wykorzystuje w większości standardowe ramki, protokoły, telegramy, z ich nadmiarowościami danych, zabezpieczeniami, adresowaniem, których opisy są publicznie dostępne i wykorzystywane przez różniej proweniencji zainteresowane strony. W nielicznych przypadkach tworzone są indywidualne dedykowane rozwiązania kolejowe.

Powszechnemu dostępowi do wielu stosowanych rozwiązań oraz szybkiemu rozwojowi technologii cyfrowych towarzyszą różnego rodzaju ataki na rozwiązania cyfrowe, programowalne, elektroniczne, komputerowe. Mamy więc malware (złośliwe oprogramowanie), w tym wirusy, robaki, trojany, adware, itd. Mamy cyfrowe włamania i kradzieże oraz wykorzystywany w tym celu ransomware. Mamy ataki poprzez infekowanie systemów w eks-

ploatacji, ale także poprzez ingerencje w hardware i software integratorów, ich dostawców, czy poddostawców dostawców. Mamy do czynienia z atakami socjotechnicznymi. O phishingu wszyscy słyszeli dzięki kampaniom informacyjnym banków. Vishing, smishing, whaling, pharming, spoofing, to ciągle techniki, które nie tylko pozostają nienazwane w wielu językach krajowych, ale także są szerzej nieznane lub słabo rozpoznawane, a tymczasem ilość ataków bardzo wyraźnie rośnie. Dziś nie atakują nas hakerzy, a przede wszystkim booty. Dopiero jak booty znajdą lukę i zainfekują system dalsze działania przejmują hakerzy, coraz częściej działający w zorganizowanych grupach sponsorowanych czy wręcz finansowanych przez państwa, czy organizacje terrorystyczne. Działają także crackerzy i haktywiści i chociaż pierwsi dopiero raczkują w hakowaniu, a drudzy mają dobre intencje, to także oni stanowią realne zagrożenie.

Dziś funkcjonują publicznie dostępne bazy podatności. Wspierać mają przede wszystkim tych, którzy chcą się zabezpieczać przed cyberatakami. Są jednak wykorzystywane także przez drugą stronę – coraz częściej mają miejsce tzw. vulnerability exploitations. Przed podatnościami często zabezpiecza patching, updating, upgrading, ale zmiany softwaru w warstwach poniżej mogą zakłócać a nawet uniemożliwiać działanie aplikacji. W dodatku wersje oprogramowania często traktowane są jako parametry w formalnych dokumentach dopuszczających rozwiązania techniczne do stosowania w transporcie szynowym, skutkiem czego często rezygnuje się z jakichkolwiek ingerencji w software. Stoi to w sprzeczności z praktyką w odniesieniu do powszechnie wykorzystywanych rozwiązań cyfrowych – nikogo już nie dziwi, że komputer, tablet, czy telefon informuje że dostępne są aktualizacje, które należy zainstalować ze względów bezpieczeństwa. W wielu przypadkach możemy odmówić, ale w nocy i tak aktualizacja zostanie zainstalowana.

W darknecie za bitcoiny można kupić cyberatak wskazując obiekt ataku i skalę oraz moment ataku. Coraz częstsze i coraz poważniejsze są ataki wolumetryczne, od zwykłych DoS, przez rozproszone DDoS, które znaczne trudniej jest wykryć i zablokować, po RDoS, które mają umożliwić żądanie okupu. Ataki wolumetryczne wykorzystywane są do blokowania funkcjonowania systemów czy usług niezależnie od tego czy mówimy o systemach informacyjnych IT czy eksploatacyjnych OT. Skutki w przypadku tych drugich mogą być poważne nie tyle dla bezpieczeństwa transportu co dla gospodarki kraju, a nawet zdolności obronnych, bo kolej odgrywa poważną rolę w odniesieniu do działań wojennych co widać wyraźnie na przykładzie działań jakie mają miejsce za naszą wschodnią granicą.

Cyfrowe aspekty podnoszone podczas konferencji IT/OT w transporcie szynowym

Konferencja obejmowała cztery panele dyskusyjne oraz czterdzieści prezentacji. Nie sposób omówić wszystkich w jednym artykule. Część zagadnień omówiona jest w innych artykułach tego numeru Przeglądu Komunikacyjnego, ale o części wypada przynajmniej wspomnieć.

Wśród materiałów udostępnionych po konferencji znajdziecie państwo wspólną rozbudowaną wypowiedź dyrektora wykonawczego Agencji Unii Europejskiej do spraw Kolei Josefa Doppelbauera oraz dyrektora Departamentu Bezpieczeństwa i Interoperacyjności Kolei w Dyrektoriacie Generalnym Komisji Europejskiej do spraw Transportu i Mobilności Keira Fitcha. Z ich wypowiedzi jasno wynika jak bardzo bezpieczeństwo cyfrowe w najbliższych latach będzie wpływało na transport kolejowy.

Wspomniane cztery panele dyskusyjne dotyczyły:

- Podejścia do cyberbezpieczeństwa i związanych z tym wyzwań w transporcie szynowym, w tym w szczególności barier formalnoprawnych w zakresie aktualizacji oprogramowania układowego rozwiązań technicznych przenaczonych dla kolei, a podlegających pod dopuszczenia świadectwowe;
- Wyzwań związanych z Rozporządzeniem Komisji (UE) 2023/1695 wprowadzającym nowe wydanie Technicznej Specyfikacji Interoperacyjności w zakresie podsystemów „sterowanie" systemu kolei w Unii Europejskiej TSI CCS (Control Command and Signalling); Specyfikacja TSI CCS 2023 wprowadza między innymi wzorzec 4. Europejskiego Systemu Sterowania Pociągiem ETCS (European Train Control System), pierwsze wydania specyfikacji przyszłego standardu bezprzewodowej łączności kolejowej oparte na standardzie 5G tzw. FRMCS (Future Railway Mobile Communication System) przedstawiając GSM-R i FRMCS jako mobilne radio kolejowe RMR (Railway Mobile Radio), oraz pierwsze specyfikacje automatycznego prowadzenia pojazdów ATO (Automatic Train Operation) zapewniające drugi poziom autonomiczności GoA 2 (Grade of Automation). Przyjęta TSI CCS obejmuje po raz pierwszy załącznik B z trzema tabelami podającymi zasady uaktualniania funkcjonalności i usuwania odchyleń od specyfikacji szczegółowych w instalacjach na liniach kolejowych i w taborze kolejowym na różnych etapach realizacji, włącznie z instalacjami już przekazanymi do eksploatacji. Takie zmiany, już budzą obawy w zakresie zgodności z prawem zamówień publicznych oraz w zakresie ich finansowania, a będą niemal na pewno kłopotliwe formalnie ze względu na wielokrotne zmiany oprogramowania poprzez patching, updating, czy upgrading;
- Rozwiązań technicznych w zakresie łączności bezprzewodowej i transmisji tor-pojazd, ze szczególnym uwzględnieniem wyzwań w zakresie planowania, budowania i zabezpieczania przed cyberatakami sieci GSM-R (Global System for Mobile Communication – Railways); oraz
- Potrzeb w zakresie odporności taboru na cyberzagrożenia, ze szczególnym uwzględnieniem wyzwań związanych z cyberbezpieczeństwem pasażerskiego ta-

boru kolejowego, uwzgledniając fakt, że obecnie zamawiany tabor dostarczany będzie po wejściu w życie dyrektywy NIS2 (dyrektywy (UE) 2022/2555), w świetle której przewoźnicy pasażerscy swój tabor postrzegają jako zestawy urządzeń cyfrowych sterowanych przez maszynistów z wykorzystaniem sieci pokładowych oraz wymieniających bezprzewodowo dane dla potrzeb rozlicznia energii, utrzymywania aktualności informacji pasażerskiej podawanej na pokładzie, diagnostyki, itd.

Wspomniane czterdzieści referatów przedstawionych zostało podczas sześciu sesji merytorycznych, z których dwie dedykowane były wprost cyberbezpieczeństwu, dwie łączności i transmisji tor-pojazd, jedna dedykowana była wymaganiom dla nowego taboru pasażerskiego oraz cyberbezpieczeństwu taboru w eksploatacji, a jedna była sesją otwarcia, podczas której cyberbezpieczeństwo w transporcie szynowym przedstawione zostało z lotu ptaka w zakresie złożoności stosowanych rozwiązań i skali wyzwań. W sesji otwarcia miały miejsce także wspomniane już wypowiedzi dyrektora wykonawczego Agencji Unii Europejskiej do spraw Kolei oraz dyrektora Departamentu Bezpieczeństwa i Interoperacyjności Kolei w Dyrektoriacie Generalnym Komisji Europejskiej do spraw Transportu i Mobilności.

Uzupełnieniem paneli dyskusyjnych i sesji merytorycznych była także sesja warsztatowa zorganizowana przez pracowników Agencji Unii Europejskiej do spraw Kolei w całości poświęcona wyzwaniom związanym ze zmianami specyfikacji TSI w roku 2023.

Przeciwdziałanie cyberzagrożeniom – działania i rozwiązania

Nie ma odwrotu od stosowania w transporcie szynowym rozwiązań cyfrowych, programowalnych, softwarowych, elektronicznych, mechatronicznych, hybrydowych, komputerowych. Musimy jednak podejmować działania dla zapewnienia i ciągłego doskonalenia ich zabezpieczeń przed cyberzagrożeniami. Atakujący wykorzystują także najnowsze rozwiązania techniczne, oraz świeżo ujawnione podatności, i nie respektują ani zasad moralnych ani przepisów prawa zamówień. Nie jesteśmy jednak na straconej pozycji.

W październiku 2020 roku powołane zostało Centrum Wymiany i Analiz Informacji podsektora transportu kolejowego ISAC-Kolej. Równolegle do wojny za naszą wschodnią granicą, przez ostatnie dwa lata, członkowie ISAC-Kolej otrzymali ponad 1200 ostrzeżeń związanych z cyberzagrożeniami. Obejmowały one: informacje o nowych kampaniach phishingowych; informacje o zarejestrowaniu domen podszywających się pod transport i podmioty związane z transportem; rekomendacje blokowania domen na urządzeniach brzegowych, stosowania odpowiednich filtrów antyspamowych; informacje o wykryciu podatności, szczególnie podatności typu zero-day; informacje o dystrybucji złośliwego oprogramowania, rekomendacje w zakresie reguł do stosowania na urządzeniach filtrujących pocztę elektroniczną; informacje o atakach DDoS, o możliwych atakach na strony internetowe i serwisy; rekomendacje antyDDoS, dotyczące monitorowania i ograniczania ruchu przy eskalacji; oraz inne przydatne informacje, np. dotyczące działalności grup APT, Killnet, itp.

Niezależnie od ostrzeżeń członkowie ISAC-Kolej otrzymują codzienne raporty krajowe dotyczące złośliwego ruchu sieciowego z rekomendacjami dotyczącymi blokowania konkretnych adresów IP; tygodniowe raporty krajowe zawierające informacje na temat wykrytych podatności w produktach IT z rekomendacjami w zakresie uaktualniania systemów i oprogramowania; oraz dwutygodniowy biuletyn informacyjny Centrum Bezpieczeństwa Operacyjnego PKP Informatyka dedykowany cyberbezpieczeństwu transportu kolejowego.

Niemal wszyscy pracownicy podmiotów kolejowych korzystają w swojej pracy z systemów informacyjnych IT i/lub systemów eksploatacyjnych OT. Jednocześnie nie bez powodu mówi się, że najsłabszym ogniwem w bezpieczeństwie systemów cyfrowych jest człowiek. Konieczne jest więc budowanie wiedzy pracowników w zakresie cyberhigieny. Od właściwego podejścia do definiowania i wykorzystywania haseł do reagowania na symptomy wskazujące na malware, ataki wolumetryczne DoS/DDoS/RDoS, ransomware, czy ingerencje w oprogramowanie. Już w kwietniu 2021 ISAC-Kolej przyjął *Wytyczne dotyczące cyberbezpieczeństwa dla pracowników podmiotów kolejowych*. Są one publicznie dostępne na www.isac-kolej.pl i są wykorzystywane przez podmioty kolejowe zarówno do budowania wiedzy pracowników w zakresie cyberhigieny jak i do weryfikowania kompletności procedur wewnętrznych w zakresie bezpieczeństwa informacji i ich doskonalenia.

Na konferencji szczegółowo przedstawione zostały najnowsze *Wytyczne dotyczące cyberbezpieczeństwa pasażerskiego taboru kolejowego* przyjęte przez ISAC-Kolej w lipcu 2023 r. Od stycznia 2024 r., ze względu na potrzeby przemysłu taborowego, w tym jego międzynarodowy charakter w zakresie łańcuchów dostaw i w zakresie klientów końcowych, wytyczne te są dostępne w pełnej wersji dwujęzycznej obejmującej język polski i język angielski (także dostępna na www.isac-kolej.pl). Wytyczne zawierają zarówno podstawy, w tym definicje, jak i czternaście kart kontrolnych i związaną z nimi metodologię. Przyjęta metodologia pozwala na identyfikowanie niedostatków zabezpieczeń przed cyberatakami dla konkretnych typów taboru. Pozwala na proste definiowanie wymagań w zakresie odporności na cyberzagrożenia przez podmioty zamawiające tabor kolejowy, czy szerzej tabor szynowy. Pozwala także na różnicowanie poziomów zabezpieczeń przed cyberzagrożeniami. To rozbudowany dojrzały dokument.

W roku 2023 dla członków ISAC-Kolej zorganizowane zostały także pierwsze dwudniowe warsztaty na cyberpoligonie. Środowisko sieciowe obejmujące wiele powiązanych maszyn wirtualnych opartych na różnych systemach operacyjnych (linux, unix, windows) i aplikacjach webowych odtwarza infrastrukturę IT/OT pozwalając

na szkolenie pracowników z wykorzystaniem systemów i procedur używanych na co dzień w podmiotach kolejowych. Pozwala na weryfikowanie odporności organizacji, weryfikowanie i doskonalenie umiejętności pracowników odpowiedzialnych za ochronę przed cyberzagrożeniami, np. pracowników zespołów SOC (Security Operation Centre), czy administratorów sieci. Instalacje takie wykorzystuje się np. w trybie threat hunting informując zespoły niebieskie, których zadaniem jest wykrycie źródła ataku i uszczelnienie systemów, o ataku/atakach, które są realizowane przez równolegle pracujące atakujące zespoły czerwone.

Na zakończenie

Autor w imieniu Komitetu Naukowego Konferencji IT/OT w Transporcie Szynowym chce podziękować wszystkim uczestnikom paneli dyskusyjnych oraz autorom prezentacji za wkład w budowanie świadomości wyzwań oraz wiedzy i umiejętności w zakresie ich pokonywania w odniesieniu do digitalizacji otaczających nas rozwiązań technicznych.

Jednocześnie zwrócić należy uwagę, że szybki rozwój technologii cyfrowych informacyjnych IT i eksploatacyjnych OT w powiązaniu z długimi okresami trwałości kolejowych instalacji i rozwiązań infrastrukturalnych i taborowych z całą pewnością będzie wymagał ciągłego uzupełniania wiedzy i doskonalenia umiejętności ekspertów od transportu szynowego. W imieniu Komitetu Naukowego oraz Komitetu Organizacyjnego autor deklaruje, że kolejne Konferencje IT/OT w Transporcie Szynowym z całą pewnością będą wychodzić naprzeciw tym wyzwaniom.

Na zakończenie słowa podziękowania należą się Komitetowi Organizacyjnemu za sprawną organizację i wielkie zaangażowanie oraz firmie Alstom, która udostępniła uczestnikom konferencji możliwość udziału w wycieczce technicznej w centrum utrzymania pociągów pendolino. ◄

Materiały źródłowe

[1] Dyrektywa w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii (NIS2, czyli dyrektywa (UE) 2023/2555)
[2] Wytyczne dotyczące cyberbezpieczeństwa dla pracowników podmiotów kolejowych. www.isac-kolej.pl
[3] Wytyczne dotyczące cyberbezpieczeństwa pasażerskiego taboru kolejowego. www.isac-kolej.pl

Nowoczesne podejście do systemów telematycznych na przykładzie Pomorskiej Kolei Metropolitalnej

A modern approach to telematics systems on the example of the Pomeranian Metropolitan Railway

Piotr Wulgaris

Dr

Dyrektor ds. inżynierii ruchu i telematyki,
Pomorska Kolej Metropolitalna,
Prezes Oddziału SITK RP w Gdańsku,
Dyrektor Biura Transportu, Polskie
Towarzystwo Ekspertów i Biegłych Sądowych

Streszczenie: W artykule zwrócono uwagę, że telematyka w kolejnictwie może skupiać się na monitorowaniu wszystkich dostępnych cyfrowych systemów i aplikacji stosowanych przez zarządcę infrastruktury do kierowania i sterowania ruchem kolejowym. Centrum Utrzymania i Diagnostyki jest miejscem, w którym skupia się monitoring systemów umożliwiający nie tylko sprawne zarządzanie utrzymaniem według wymagań norm RAMS, ale także elementem umożliwiającym optymalizacje zasobów i kosztów eksploatacji i utrzymania.

Słowa kluczowe: *Telematyka; Cyfryzacja Kolei, Monitoring Procesów; Sterowanie Ruchem Kolejowym*

Abstract: Telematics in railways can focus on monitoring all available digital systems and applications used by the infrastructure manager to direct and control railway traffic. The Maintenance and Diagnostics Center is a place where system monitoring is focused, enabling not only efficient maintenance management in accordance with RAMS standards, but also an element enabling the optimization of resources and operation and maintenance costs.

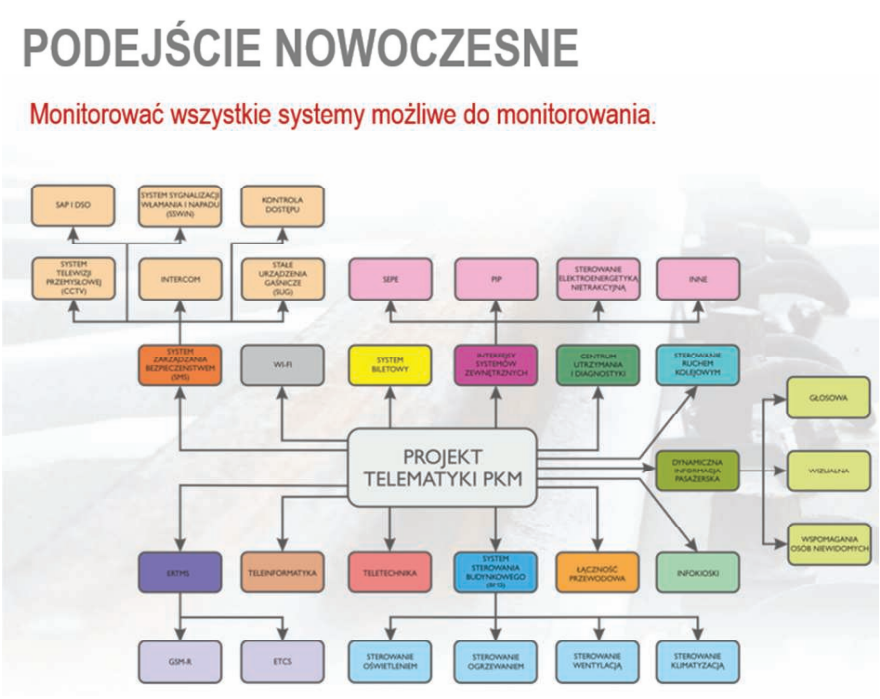
Keywords: *Telematics; Railway Digitization; Process Monitoring; Railway Traffic Control*

Pomorska Kolej Metropolitalna (PKM) została powołana 11 czerwca 2010 roku jako jednoosobowa spółka samorządu Województwa pomorskiego. Celem spółki jest prowadzenie inwestycji infrastrukturalnych na terenie Województwa pomorskiego oraz zarządzanie wybudowaną przez siebie infrastrukturą kolejową. Spółka zarządza liniami kolejowymi nr 248 i 253 łączącymi Gdańsk z Kaszubami oraz Gdynią. Są to pierwsze linie kolejowe wybudowane przez Samorząd Województwa w Polsce.

W wyniku ukończonych w roku 2023 inwestycji linie kolejowe będące w zarządzie PKM zostały zelektryfikowane, a dzięki budowie tzw. bajpasu kartuskiego linia nr 248 uzyskała połączenie z linią nr 234 i stacją Gdańsk Kokoszki umożliwiając w ten sposób alternatywne połączenie z Kartuzami. Pomorska Kolej Metropolitalną jest aktualnie najbardziej scyfryzowanym zarządcą infrastruktury kolejowej w Polsce. W związku z niekonwencjonalnym dotychczas rozwiązaniem, skupiającym w jednym miejscu nadzór nad funkcjonowaniem linii kolejowej, należało wypracować nowoczesne podejście do zarządzania wszystkimi aplikacjami składającymi się na zarządzanie ruchem kolejowym, informacje pasażerską oraz sterowanie ruchem kolejowym.

Jedną z pierwszych definicji słowa telematyka była definicja francuska z lat 80. XX wieku mówiąca, że telematyka to zastosowanie technologii informatycznych w transporcie (kolejnictwie).[1] Słowo to powstało z połączenia słów telekomunikacja oraz informatyka. Telematyka jest dziedziną, która zajmuje się zintegrowanymi systemami telekomunikacyjnymi, informatycznymi i informacyjnymi wykorzystywanymi w transporcie. Na gruncie prawa europejskiego o telematyce mówią nam dwa rozporządzenia dotyczące technicznych specyfikacji interoperacyjności systemu kolei w zakresie aplikacji telematycznych dla przewozów pasażerskich i przewozów towarowych.[2] W PKM pojęcie „telematyka" rozumiane jest jako zbiór wszystkich systemów (aplikacji) komputerowych wspierających proces prowadzenia ruchu kolejowego.

Sercem monitorowania i diagnostyki systemów telematycznych w PKM jest Centrum Utrzymania i Diagnostyki. Tradycyjnie Centrum Utrzymania i Diagnostyki (CUiD) zajmuje się monitorowaniem dostępności zasilania oraz działania systemów sterowania ruchem kolejowym. Według nowoczesnego podejścia do telematyki CUiD zajmuje się monitorowaniem wszelkich możliwych do monitorowania systemów. W PKM jest ich 28. Tak rozumiane CUiD pełni funkcję diagnostyczną, nadzorczą i informacyjną. W początkowej fazie eksploatacji w centrum utrzymania i diagnostyki skupiało się przede wszystkim na regulacji systemu oraz przyśpieszeniu procesu



***1**. Projekt telematyki PKM. Źródło: materiały PKM*

gwarancyjnego. Dziś służy ono także jako centrum informacji dla dyżurnych ruchu, branżystów i służb technicznych oraz zarządu i kierownictwa firmy. Efektem globalnym wdrożenia takiej idei centrum utrzymania i diagnostyki jest skupienie się na prewencji utrzymania owej oraz skróceniu czasu reakcji na usterki. To z kolei prowadzi do obniżenia kosztów utrzymania i eksploatacji. Na monitorach w centrum Utrzymania i Diagnostyki, prezentowana jest zbiorcza informacja o stanie systemów i aplikacji w czasie rzeczywistym oraz rejestracja zdarzeń, alarmów oraz usterek. Dedykowany system diagnostyki wspomaga zautomatyzowane prowadzenie dokumentacji elektronicznej w postaci dziennika uszkodzeń urządzeń łączności oraz książki kontroli urządzeń. Cała informacja diagnostyczna prezentowana jest na ekranach monitorów w sposób zbiorczy. W stanie zasadniczym informacja ta ma charakter prosty, świadczący o dostępności systemu i innych podsystemów. Wszystkie aplikacje i systemy pracują w oparciu o zsynchronizowany czas (jednakowy dla wszystkich urządzeń) w całym obszarze LCS, a wszystkie urządzenia komputerowe w obszarze CUiD pracują w sieci zamkniętej.

W celu pomocy przy rozwiązywaniu problemów związanych z utrudnieniami w ruchu pociągów stanowisko operatorskie umożliwia prezentacje aktualnej sytuacji ruchowej. Sprawne prowadzenie ruchu pociągów, wymaga wsparcia dla utrzymania zainstalowanych systemów i podsystemów na obszarach zdalnego sterowania LCS, z wykorzystaniem diagnostyki technicznej, w tym ciągłego monitoringu zdarzeń, ich bieżącej rejestracji on-line, raportowania oraz analiz dla szybkiego usuwania usterek, prowadzenia konserwacji i regulacji urządzeń i podzespołów. Prezentowane na stanowisku diagnostycznym dane są uporządkowane, oddzielnie dla każdego podsystemu, w klasy ważności oraz obszary według poniższej klasyfikacji:[3]

1. Klasa I (alarmy) – stan wymagający natychmiastowej interwencji personelu utrzymania (kolor czerwony), w obszarze:
   a. zasilanie podsystemu,
   b. transmisja podsystemu,
   c. warstwa wewnętrzna podsystemu (zależnościowa),
   d. warstwa zewnętrzna podsystemu (obiektowa).

2. Klasa II (zdarzenia) – stan wymaga śledzenia lub poddania dokładnej analizie technicznej (kolor pomarańczowy), w obszarze:
   a. zasilanie podsystemu,
   b. transmisja podsystemu,
   c. warstwa wewnętrzna podsystemu (zależnościowa),
   d. warstwa zewnętrzna podsystemu (obiektowa).

3. Klasa III (komunikaty, meldunki) – stan niewymagający ingerencji (kolor zielony), w obszarze:
   a. zasilanie podsystemu,
   b. transmisja podsystemu,
   c. warstwa wewnętrzna podsystemu (zależnościowa),
   d. warstwa zewnętrzna podsystemu (obiektowa).

Ilustrując powyższą klasyfikację można przywołać parametry monitorowane w systemie radiołączności GSM-R obejmujące:

1. Gotowość
2. Prace sieci transmisyjnej
3. Prace z energetycznej sieci zasilającej
4. Prace z baterii / zasilania rezerwowego
5. Poprawność pracy rejestratora

Minimalny zakres prezentowanych informacji to:

1. Śledzenie pracy systemu – Klasa III
2. Awaria stacji bazowej – Klasa I
3. Awaria (w) sieci transmisyjnej – Klasa I i Klasa II (osiągnięcie wartości granicznych przynajmniej jednego z parametrów)
4. Awaria zasilania podstawowego stacji bazowej – Klasa II
5. Awaria zasilania rezerwowego stacji bazowej – Klasa I
6. Tryb pracy stacji bazowej (zdalny / miejscowy) – Klasa III

W razie zaistnienia usterki i konieczności natychmiastowej interwencji (Klasa I decyzji), wykrycia ograniczenia dyspozycyjności systemu i konieczności przeprowadzenia głębszej analizy (Klasa II decyzji), operator po wybraniu z menu odpowiedniego okna jest w stanie stwierdzić, co uległo lub może ulec uszkodzeniu i przedsięwziąć odpowiednie środki zaradcze.

W Pomorskiej Kolei Metropolitalnej monitoring systemów telematycznych obejmuje: sterowanie i kierowanie ruchem kolejowym, informacje pasażerską, stan sieci i urządzeń transmisyjnych, stan sieci i urządzeń SN i NN, bezpieczeństwo oraz wszelkie zasoby

informatyczne spółki.

Monitorowanie systemu sterowania ruchem kolejowym obejmuje:[4]

1. status połączeń systemu zależnościowego ze sterownikami obiektowymi;
2. prezentacja zdarzeń, alarmów i komunikatów (meldunków) systemu – odpowiednio do podjęcia niezbędnych działań utrzymaniowych tj. klasy I (korekcji), klasy II (prewencji) oraz klasy III;
3. podgląd statusu sterowanych obiektów;
4. status linii sterujących urządzeniami wykonawczymi (obiektami);
5. tryb pracy poszczególnych komputerów systemu;
6. tryb sterowania (miejscowe, zdalne);
7. podgląd wersji oprogramowania komputerów systemu;

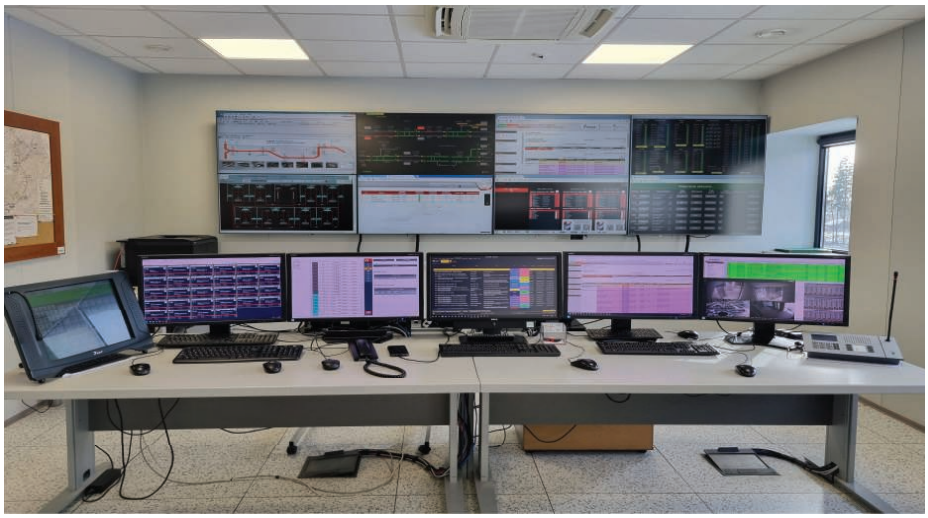
Urządzenia wykonawcze infrastruktury (sygnalizatory, napędy zwrotnicowe i rogatkowe, itd.) są monitorowane jedynie w ograniczonym zakresie (przepalenie żarówki, utrata kontroli, rozprucie, itd.)

Ponadto dla zwiększenia bezpieczeństwa ruchu kolejowego w Pomorskiej Kolei Metropolitalnej eksploatowany jest również symulator dyżurnego ruchu LCS PKM. Symulator ten umożliwia:

1. Sterowanie (blokadą liniową, rozjazdami, semaforami, wskaźnikami na semaforach, powtarzaczem semafora, tarczą ostrzegawczą, obwodem torowym, resetem licznika osi sekcji kontroli nie zajętości, wejściami)
2. Prowadzenie nadzoru nad RBC LCS PKM
3. Prowadzenie ruchu pociągów za pomocą ETCS L2

Ponadto, umożliwia on realizację przykładowych scenariuszy szkoleniowych, takich jak:

1. Blokada (włączenie, zmiana kierunku, awaryjne włącznie lub zmiana kierunku, zamknięcie szlaku, zwolnienie kierunku , poza kontrolą),
2. Zwrotnica (zmiana położenia, zmiana położenia przy zajętym obwodzie torowym utrata kontroli położenia, likwidacja rozprucia)
3. ETCS i RBC (rejestracja pociągu, wyrejestrowanie pociągu, ustawienie TSR, wysyłanie SMS do maszynisty, awaryjne zatrzymanie pociągu)
4. Możliwość definiowania dowolnego scenariusza i sytuacji ruchowej na szlaku.



***2**. Centrum Utrzymania i Diagnostyki. Źródło: Materiały autora*

Na symulatorze prowadzone są zajęcia praktyczne mające na celu ciągły rozwój i podnoszenie kompetencji i kwalifikacji personelu ruchowego odpowiedzialnego za bezpieczne prowadzenie jest pociągów na sieci PKM. Symulator ten jest rzeczywistym i wiernym odwzorowaniem infrastruktury i linii kolejowych 248 oraz 253 i jest wierną kopią systemu sterowania i kierowania ruchem zainstalowanego na LCS PKM.[8]

System Informacji Pasażerskiej (SIP) składa się z informacji wizualnej, informacji głosowej, infokiosku, informacji dla niewidomych. Informacje wizyjne zapewniają wyświetlacze SIP umieszczone na peronach. Podgląd aktualnego stanu i obrazu każdego z wyświetlaczy na całej linii znajduje się na jednym z monitorów CUiD. Zarówno operator CUiD jak i Dyspozytor Ruchu Kolejowego w razie konieczności może w każdej chwili wprowadzić dodatkowe tzw. paski informacyjne na wyświetlaczach informujące np. o utrudnieniach w ruchu pociągów lub wystąpieniu innych sytuacji nietypowych. Informacja głosowa dzieli się na automatycznie generowaną z informacji dostarczanych z liczników osi poszczególnych odcinków zbliżania i bezpośrednia wygłaszaną przez Dyspozytora Ruchu Kolejowego. Infokioski wyświetlają rozkład jazdy zarówno pociągów jak i komunikacji miejskiej (na przystankach będących węzłami przesiadkowymi). Informacje dla niewidomych zapewniają napisy w języku Braille'a (zgodnie z TSI PRM). [5] Dodatkowo, w momencie zbliżania się pojazdu szynowego do przystanku system dźwiękowego wspomagania poruszania się osób z dysfunkcją narządu wzroku rozpoczyna emitowanie kierunkowego sygnału dźwiękowego. Sygnał kieruje w bezpieczny sposób wysiadające osoby o ograniczonej sprawności do wyjść z peronu oraz do wind.[6]

Ponadto centrum utrzymania i diagnostyki umożliwia prowadzenie zintegrowanego systemu bezpieczeństwa polegającego na monitoringu wizyjnym wraz z analityką, systemach przeciwpożarowych i gaszenia pożaru, kontroli dostępu, systemów SOS-Info, oraz interkomów. Na przystankach zamontowane są słupki umożliwiające bezpośrednią komunikację z personelem PKM. W przypadku wystąpienia konieczności uzyskania informacji przycisk Info łączy bezpośrednio dyspozytorem ruchu kolejowego LCS PKM. Przycisk SOS umożliwia bezpośrednią komunikację z Centrum Monitoringu (CM) w razie wystąpienia jakiegokolwiek niebezpieczeństwa lub zagrożenia. Ponadto, w 2021 roku w celu podniesienia bezpieczeństwa podróżnych, Spółka we własnym zakresie doposażyła wszystkie przystanki w urządzenia umożliwiające prowadzenie reanimacji ludzi na wypadek zatrzymania krążenia. Urządzenia te zostały włączone do

systemu bezpieczeństwa w PKM oraz systemu monitoringu CCTV.

W przypadku zaistnienia zdarzenia i użycia defibrylatora, system bezpieczeństwa generuje powiadomienie do Centrum Monitoringu, a system CCTV automatycznie rejestruje zaistniałe zdarzenie.

Pomorska Kolej Metropolitalna posiada bardzo rozbudowany system monitoringu wizyjnego. Składa się na niego około 400 kamer zainstalowanych na przystankach i wzdłuż całej linii kolejowej. Za nadzór nad zapisami monitoringu odpowiada Centrum Monitoringu natomiast za prawidłowe działanie systemu odpowiada Centrum Utrzymania i Diagnostyki. System telewizji przemysłowej CCTV jest wyposażony w funkcję inteligentnej analizy obrazu z możliwością wyszukiwania zdarzeń na bieżąco oraz zdarzeń archiwalnych. Zaimplementowane funkcje analizy obrazu pozwalają na:

a. wykrywanie przekroczenia linii (np. zbliżenie się do krawędzi peronu);
b. wykrywanie wejścia na wyznaczony obszar (np. poruszanie się po torach)
c. wykrywanie pozostawionych przedmiotów;
d. wykrywanie zmiany kadru kamery;

Tak rozbudowany monitoring przyczynia się do wzrostu bezpieczeństwa zarówno na obszarze kolejowym jaki bezpieczeństwa prowadzenia ruchu kolejowego.

Pomorska Kolej Metropolitalna jest również autorem rozwiązania o nazwie PKM Display Manager. System ten umożliwia prezentację informacji z wielu źródeł między innymi informacji lotniskowej, komunikacji miejskiej, informacji kolejowej, informacje o dostępnych miejscach parkingowych pogodzie i jakości powietrza, dostępności roweru miejskiego. System ten łączy możliwość prezentacji treści informacyjnych z reklamowymi na jednym ekranie przyjazny dla oglądającego sposób można połączyć informacje oraz promocje. Z tego rozwiązania korzystają szpitale pomorskie, galeria metropolia, Urząd Marszałkowski Województwa Pomorskiego, Torus, Colliers International.[7]

W dobie powszechnej digitalizacji

***3**. Centrum Monitoringu PKM. Źródło: Materiały autora*

i cyfryzacji również sektor kolejowy musi stawić czoła wyzwaniu współczesności. Kluczem do sukcesu jest sprawne zarządzanie systemami i aplikacjami stosowanymi przez przedsiębiorstwo kolejowe w taki sposób, aby uzyskać optymalizacje kosztów utrzymania i eksploatacji, a także uzyskać jak najwyższy poziom niezawodności urządzeń i systemów przekładający się na bezawaryjną pracę co w konsekwencji przełoży się na zwiększenie atrakcyjności kolei jako środa transportu. Będzie to możliwe przy globalnym podejściu do monitoringu systemów poprzez zarządzanie nimi na poziomie Centrum Utrzymania i Diagnostyki będącego centralnym miejscem zarządzania systemami i aplikacjami. ◄

Materiały źródłowe

[1] Termin „telematyka" został użyty po raz pierwszy w 1978 roku przez Simona Norę i Alaina Minca w raporcie zatytułowanym „L'Informatisation de la société" – przygotowanym dla francuskiego premiera w odpowiedzi na rozwój technologii komputerowych i początek ery informacyjnej, za: https://www.verizonconnect.com/pl/zasoby/artykul/telematyka-co-to-jest/

[2] TSI TAP - rozporządzenie Komisji (UE) nr 454/2011 z dnia 5 maja 2011 r. w sprawie technicznej specyfikacji interoperacyjności odnoszącej się do podsystemu „Aplikacje telematyczne dla przewozów pasażerskich" transeuropejskiego systemu kolei,

TSI TAF - rozporządzenie Komisji (UE) nr 1305/2014 z dnia 11 grudnia 2014 r. dotyczące technicznej specyfikacji interoperacyjności odnoszącej się do podsystemu aplikacji telematycznych dla przewozów towarowych wchodzącego w skład systemu kolei w Unii Europejskiej.

[3] Program Funkcjonalno – Użytkowy Tom III – część telematyczna w postępowaniu o udzielenie zamówienia publicznego na: „Zaprojektowanie i budowa Pomorskiej Kolei Metropolitalnej Etap I - rewitalizacja „Kolei Kokoszkowskiej""

[4] Szczegółowa koncepcja wyposażenia telematycznego linii kolejowej, Gdańsk 2013

[5] TSI PRM – Rozporządzenie Komisji (UE) nr 1300/2014 z dnia 18 listopada 2014 r. w sprawie technicznych specyfikacji interoperacyjności odnoszących się do dostępności systemu kolei Unii dla osób niepełnosprawnych i osób o ograniczonej możliwości poruszania się.

[6] Znaczenie dynamicznej informacji pasażerskiej w aglomeracji miejskiej na przykładzie PKM – wystąpienie z konferencji „Telekomunikacja i informatyka na kolei" 15.03.2018,

[7] PKM Display Manager +. Elastyczny system informacyjno – promocyjny – materiały PKM S.A.

[8] Stanowisko szkoleniowe dla dyżurnych ruchu PKM S.A., Gdańsk 2019, materiały PKM S.A.

Diagnostyka i utrzymanie systemów sterowania ruchem kolejowym na odległość - bezpieczny zdalny dostęp do systemów kluczowych

Remote maintenance and diagnostics of railway control systems- secure remote access to essential systems

Radosław Zawierucha

Mgr
Członek Zarządu ds. Rozwoju Infrastruktury IT i Bezpieczeństwa, PKP Informatyka Sp. z o.o.

radoz72@gmail.com

Grzegorz Kuta

Biuro Bezpieczeństwa Informacji i Spraw Obronnych,

PKP Polskie Linie Kolejowe S.A.

Streszczenie: W artykule przedstawiono opis prac nad projektem p*roof of concept* rozwiązania diagnostyki i utrzymania systemów sterowania ruchem kolejowym na odległość, przeprowadzonym przez PKP Polskie Linie Kolejowe S.A. oraz PKP Informatyka Sp. z o.o. wraz z firmą ALSTOM Polska S.A. Artykuł opisuje otoczenie prawne i wynikające z niego zapotrzebowanie na utworzenie podobnego projektu, proces określania wymagań dla docelowego rozwiązania na podstawie norm, standardów i zaleceń branżowych, oraz jego efekty, w formie opisu funkcjonalności i podstawowej architektury logicznej rozwiązania. W drodze *proof of concept* stwierdzono, że proponowane rozwiązanie realizuje określone wymagania funkcjonalne.

Słowa kluczowe: *Cyberbezpieczeństwo; Sterowanie Ruchem Kolejowym; Zdalny Dostęp; Cyberbezpieczeństwo OT*

Abstract: The article presents a description of the work on the proof of concept for the remote diagnostics and maintenance of railway traffic control systems solution, carried out by PKP Polskie Linie Kolejowe S.A., PKP Informatyka Sp. z o.o. and ALSTOM Polska S.A. The article describes the legal environment and the resulting needs for the creation of a similar project, the process of determining the requirements for the target solution and the underlying norms, industry standards and best practices, and a description of the functionality and basic logical architecture of the solution. Proof of concept has confirmed that the proposed solution meets the specified functional requirements.

Keywords: *Cybersecurity; Railway Signaling; Remote Access; OT Cybersecurity*

Otoczenie prawne dla prac nad diagnostyką nad bezpiecznym zdalnym dostępem do systemów kluczowych

W 2023 roku w Unii Europejskiej przyjęta została Dyrektywa Parlamentu Europejskiego i Rady 2022/2555 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 (tzw. Dyrektywa NIS2) [1]. Dyrektywa NIS2 (ang. *Network and Information Systems Directive*) stanowi nowelizację obowiązującego od 2016 roku prawa europejskiego dotyczącego obszaru cyberbezpieczeństwa, które do polskiego systemu prawnego zaimplementowano przepisami ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (t.j. Dz. U. z 2023 r. poz. 913 z późn. zm.) [2]. Załączniki I Dyrektywy NIS2 podobnie jak obecnie obowiązujący załącznik do ustawy o krajowym systemie cyberbezpieczeństwa wskazuje sektory i podsektory kluczowe oraz rodzaje podmiotów objęte tymi regulacjami. Jeśli chodzi o transport kolejowy to Dyrektywa NIS2 pozycjonuje go jako podsektor kluczowy sektora transportu wymieniając w zakresie podmiotowym zarządców infrastruktury zgodnie z definicją zawartą w art. 3 pkt 2 dyrektywy Parlamentu Europejskiego i Rady 2012/34/UE oraz przedsiębiorstwa kolejowe zgodnie z definicją zawartą w art. 3 pkt 1 dyrektywy 2012/34/UE [3], w tym operatorów infrastruktury kolejowej zdefiniowanej w art. 3 pkt 12 tej samej dyrektywy. W myśl Dyrektywy NIS2 „zarządca infrastruktury" to każdy podmiot lub przedsiębiorstwo, które jest odpowiedzialne w szczególności za założenie infrastruktury kolejowej, zarządzanie nią i jej utrzymanie, w tym za prowadzenie ruchu pociągów, urządzenia bezpiecznej kontroli jazdy i urządzenia sterowania ruchem kolejowym, a funkcje zarządcy infrastruktury na sieci lub części sieci mogą być przydzielane różnym podmiotom lub przedsiębiorstwom. Z kolei „przedsiębiorstwo kolejowe" w rozumieniu Dyrektywy NIS2 to każde

przedsiębiorstwo publiczne lub prywatne, posiadające licencję zgodnie z dyrektywą w sprawie utworzenia jednolitego europejskiego obszaru kolejowego, którego działalność podstawowa polega na świadczeniu usług w transporcie towarowym lub pasażerskim koleją, z zastrzeżeniem, że przedsiębiorstwo to zapewnia pojazdy trakcyjne, czyli obejmuje także przedsiębiorstwa, które tylko dostarczają pojazdy trakcyjne. „Operator obiektu infrastruktury usługowej" oznacza natomiast każdy podmiot publiczny lub prywatny odpowiedzialny za zarządzanie co najmniej jednym obiektem infrastruktury usługowej lub świadczący przedsiębiorstwom kolejowym jedną lub więcej usług (np. terminale towarowe, punkty zaplecza technicznego czy dostawę prądu trakcyjnego). W obecnie obowiązującym stanie prawnym, czyli bazując na przepisach aktualnie obowiązującej ustawy o krajowym systemie cyberbezpieczeństwa operatorem usługi kluczowej jest podmiot, o którym mowa w załączniku nr 1 do ustawy, posiadający jednostkę organizacyjną na terytorium Rzeczypospolitej Polskiej, wobec którego organ właściwy do spraw cyberbezpieczeństwa wydał decyzję o uznaniu go za operatora usługi kluczowej.

Dla sektora transportu i podsektora transportu kolejowego jest nim minister właściwy do spraw transportu. Stąd w obecnym stanie prawnym, aby zarządca infrastruktury kolejowej, przedsiębiorstwo kolejowe czy operator kolejowej infrastruktury usługowej zobowiązany był stosować przepisy ustawy o krajowym systemie cyberbezpieczeństwa musi otrzymać od organu właściwego do spraw cyberbezpieczeństwa decyzję administracyjną uznającą go za operatora usługi kluczowej. Dopiero na tej podstawie dana Spółka kolejowa w terminach wskazanych w ustawie (art. 16) wdrożyć musi obowiązki i wymagania z niej wynikające określone w art. 8 oraz art. 15. W decyzji administracyjnej wskazane są również wprost systemy informacyjne, które wspierają usługę kluczową. Zgodnie z Dyrektywą NIS2 znacznemu rozszerzeniu ulega katalog sektorów objętych działaniem tego przepisu. Mimo, że taki podział nie przesądza jeszcze o uznaniu danego podmiotu za kluczowy, odnosząc się do podsektora kolejowego zakres podmiotowy polskich Spółek kolejowych odjęty tą regulacją ulegnie znacznemu rozszerzeniu w stosunku do dziś obowiązujących przepisów. Obecnie, na bazie posiadanych informacji, pod przepisy ustawy o krajowym systemie cyberbezpieczeństwa w podsektorze kolejowym podlegają tylko cztery spółki kolejowe mające status operatora usługi kluczowej, świadczące usługi wskazane w rozporządzeniu Rady Ministrów z dnia 11 września 2018 r. w sprawie wykazu usług kluczowych oraz progów istotności skutku zakłócającego incydentu dla świadczenia usług kluczowych [4]. Ten akt prawny wskazuje, że w podsektorze transportu kolejowego podmiotem świadczącym usługi kluczowe jest zarządca infrastruktury kolejowej w rozumieniu art. 4 pkt 7 ustawy z dnia 28 marca 2003 r. o transporcie kolejowym [5] z wyłączeniem zarządców wyłącznie infrastruktury nieczynnej, infrastruktury prywatnej oraz infrastruktury kolei wąskotorowej, a usługą kluczową jest „Konstrukcja rozkładu jazdy pociągów". Ponadto podmiotem świadczącym usługi kluczowe jest przewoźnik kolejowy, o którym mowa w art. 4 pkt 9 ustawy o transporcie kolejowym, którego działalność podlega licencjonowaniu, oraz operator obiektu infrastruktury usługowej jeżeli przedsiębiorca wykonujący funkcję operatora jest jednocześnie przewoźnikiem kolejowym. W przypadku przewoźników kolejowych usługą kluczową jest odpowiednio „transport kolejowy pasażerski" oraz „transport kolejowy towarów". W przypadku Dyrektywy NIS2 dla podsektora transportu kolejowego za podmioty kluczowe lub podmioty ważne uznane zostaną zarządcy infrastruktury, przedsiębiorstwa kolejowe oraz operatorzy infrastruktury kolejowej przekraczające pułapy określone dla średnich przedsiębiorstw (zatrudniające co najmniej 50 osób oraz których obroty roczne lub roczna suma bilansowa wynoszą od 10 mln euro do 50 mln euro). Za podmiot kluczowy lub ważny w podsektorze transportu kolejowego uznane mogą zostać również spółki kolejowe wskazane jako podmioty krytyczne na podstawie dyrektywy o odporności podmiotów krytycznych [6] (tzw. Dyrektywy CER), podmioty które państwo członkowie Unii Europejskiej wskazało przed wejściem w życie NIS2 jako operatorów usług kluczowych czy pomioty z sektorów wymienionych w załączniku I i II Dyrektywy NIS2, które nie kwalifikują się jako pomioty kluczowe (staną się one podmiotami ważnymi na gruncie Dyrektywy NIS2). W tym miejscu, odnosząc się do powyższego, należy również zwrócić uwagę na zapisy rozporządzenia Komisji Europejskiej 2023/2450 z dnia 25 lipca 2023 r. uzupełniającego dyrektywę Parlamentu Europejskiego i Rady (UE) 2022/2557 [7] (Dyrektywę CER o odporności podmiotów krytycznych) przez ustanowienie wykazu usług kluczowych. Dokument ten ustanawia niewyczerpujący wykaz usług kluczowych, w rozumieniu definicji zawartej w art. 2 pkt 5 Dyrektywy CER, świadczonych w poszczególnych sektorach i podsektorach.

Dla podsektora transportu kolejowego jako usługi kluczowe w/w rozporządzenie wskazuje:

- usługi w zakresie transportu kolejowego (pasażerskiego i towarowego) (przedsiębiorstwa kolejowe);
- eksploatację i utrzymanie infrastruktury kolejowej, w tym stacji pasażerskich, terminali to-

warowych, stacji rozrządowych i centrów sterowania ruchem, i zarządzanie nimi (zarządcy infrastruktury);
- eksploatację i utrzymanie obiektów kolejowej infrastruktury usługowej i zarządzanie nimi (operatorzy obiektów infrastruktury usługowej);
- eksploatację i utrzymanie instalacji i systemów związanych z zarządzaniem i sterowaniem ruchem kolejowym oraz telekomunikacją, które są wykorzystywane do sterowania ruchem, oraz zarządzanie tymi systemami i instalacjami (zarządcy infrastruktury).

Zapotrzebowanie dla prac nad diagnostyką nad bezpiecznym zdalnym dostępem do systemów kluczowych

Przygotowując się do wdrożenia zapisów Dyrektywy NIS2 oraz Dyrektywy CER, mając na względzie potrzebę zapewnienie odporności przed zagrożeniami nie tylko systemów informacyjnych (systemów IT), ale również technologii operacyjnych (systemów OT) do których zaliczyć należy urządzenia sterowania ruchem kolejowym, PKP Polskie Linie Kolejowe S.A. oraz PKP Informatyka Sp. z o.o. wraz z firmą ALSTOM Polska S.A. wykonały tzw. „proof of concept" w zakresie zdalnego dostępu i monitorowania komputerowych systemów sterowania ruchem kolejowym w PKP Polskie Linie Kolejowe S.A. w oparciu o infrastrukturę SIEM (Security Information and Event Management) oraz SOC (Security Operations Center). Utworzenie projektu motywowane było m.in. rosnącym zainteresowaniem podmiotów odpowiedzialnych za cyberbezpieczeństwo, w tym CSIRT-ów poziomu krajowego wskazanych w przepisach ustawy o krajowym systemie cyberbezpieczeństwa, kwestią zapewnienia bezpieczeństwa serwisu utrzymania i diagnostyki w systemach sterowania ruchem kolejowym oraz, jak wskazano powyżej, realizacji wymagań prawnych (Dyrektywy NIS2 oraz ustawy o krajowym systemie cyberbezpieczeństwa). Projekt został zrealizowany oraz nadal jest kontynuowany w ramach prac badawczo - rozwojowych zespołu CERT PKP Informatyka Sp. z o.o., we współpracy z dostawcami komputerowych systemów sterowania ruchem kolejowym, producentami rozwiązań z domeny cyberbezpieczeństwa oraz z PKP Polskie Linie Kolejowe S.A. Celem projektu jest wykazanie możliwości i słuszności zastosowania wybranych rozwiązań i technologii bezpieczeństwa w celu zwiększenia odporności cybernetycznej w komputerowych systemach sterowania ruchem kolejowym. Po raz pierwszy wyniki projektu zaprezentowano podczas VI Konferencji naukowo – technicznej „IT&OT w transporcie szynowym" zorganizowanej przez Stowarzyszenie Inżynierów i Techników Komunikacji RP.

Wymagania dla rozwiązania bezpiecznego zdalnego dostępu do systemów kluczowych

Kluczowym elementem związanym z diagnostyką i utrzymaniem systemów sterowania ruchem kolejowym z wykorzystaniem zdalnego dostępu było w pierwszej kolejności określenie zarówno środków proceduralnych jak i technicznych związanych projektowanym rozwiązaniem. W tym celu w pierwszej kolejności określono standardy obowiązujące zarówno w obszarze IT jak i OT biorąc pod uwagę zarówno elementy związane z bezpieczeństwem funkcjonalnym systemów sterowania ruchem kolejowym (m.in. normy RAMS serii EN 50120 [8]) jak również standardy związane z bezpieczeństwem systemów informacyjnych (normy serii ISO/IEC 27000 [9]), dotyczące zarządzania usługami (norma ISO 20000 [10]), związane z bezpieczeństwem systemów sterowania i automatyki przemysłowej (normy serii IEC 62443 [11]), powiązane z cyberbezpieczeństwem aplikacji kolejowych (norma CLC/TS 50701 [12]) oraz dotyczące zapewnienia ciągłości działania organizacji (norma ISO 22301 [13]). Zaznaczyć należy, że przesłanki związane z wdrożeniem określonych elementów systemu zarządzania cyberbezpieczeństwem dla komputerowych systemów sterowania ruchem kolejowym powinny wynikać z procesu zarządzania ryzykiem oraz uwzględniać obowiązujące u zarządcy infrastruktury kolejowej elementy zarządzania ruchem kolejowym, uwzględniać istniejącej polityki bezpieczeństwa w obszarze bezpieczeństwa ruchu kolejowego (SMS) [14], obszar bezpieczeństwa informacji (SZBI) a także być zgodne z wymaganiami prawnymi (np. ustawą o transporcie kolejowym, dyrektywami kolejowymi, Dyrektywą NIS2, ustawą o krajowym systemie cyberbezpieczeństwa). Wymagania dotyczące zapewnienia kontroli dostępu zarówno do systemów informacyjnych (IT) jak i operacyjnych (OT) określa odpowiednio standard ISO/IEC 27001:2022 (obszar IT) jak również standard IEC 62443 (obszar OT). W tym miejscu zwrócić uwagę należy na fakt, że kojarzony dotychczas tylko i wyłącznie z obszarem bezpieczeństwa informacji standard ISO/IEC 27001 został całkowicie zmieniony i w wersji normy z 2022 roku oprócz bezpieczeństwa informacji obejmuje on elementy związane z cyberbezpieczeństwem oraz ochroną prywatności. Koncepcje cyberbezpieczeństwa wskazane w normie ISO/IEC 27001:2022 umożliwiają postrzeganie zabezpieczeń w odniesieniu do tych określonych chociażby w standardzie ISO/IEC TS 27110 (informatyka, cyberbezpieczeństwo i ochrona prywatności – wytyczne dotyczące rozwoju ram cyberbezpieczeństwa), czyli m.in. odnosić się do celów biznesowych

***1**. Funkcjonalności rozwiązania*

organizacji, aktywów, procesów biznesowych oraz praw i regulacji, którym dany podmiot podlega. Mając na względzie powyższe w realizowanym projekcie uwzględniono wymagania normy ISO/IEC 27001:2022 w następującym zakresie:

- kontrola dostępu (pkt 5.15 normy),
- zarządzanie tożsamością (pkt 5.16 normy),
- informacje uwierzytelniające (pkt 5.17 normy),
- prawa dostępu (pkt 5.18 normy),
- monitorowanie, przegląd i zarządzanie zmianą usług dostawców (pkt 5.22 normy),
- praca zdalna (pkt 6.7 normy),
- uprzywilejowane prawa dostępu (pkt 8.2 normy),
- bezpieczne uwierzytelnianie (pkt 8.5 normy),

Natomiast stosując zapisy standardu IEC 62443 uwzględniono takie wymagania jak:

- uwierzytelnianie wszystkich zdalnych użytkowników na odpowiednim poziomie (pkt 4.3.3.6.5 normy),
- kontrola dostępu: administracja kontami (pkt 4.3.3.5 normy),
- kontrola dostępu: uwierzytelnienie (pkt 4.3.3.6 normy),
- kontrola dostępu: autoryzacja (pkt 4.3.3.7 normy),

Wymagania kontroli dostępu jakie uwzględniono w realizowanym projekcie zdalnego dostępu i monitorowania komputerowych systemów sterowania ruchem kolejowym to:

- zapewnienie gwarancji, że cecha tożsamości użytkownika logującego się do systemów sterowania ruchem kolejowym czy to lokalnie np. w Lokalnym Centrum Sterowania, czy w sposób zdalny (np. z siedziby usługodawcy) jest prawidłowa, gdyż uwierzytelnianie użytkownika jest warunkiem niezbędnym do przyznania dostępu do wszystkich zasobów w systemie sterowania ruchem kolejowym,
- zapewnienie, że środki użyte do potwierdzenia tożsamości użytkownika (np. hasło) są bezpieczne oraz umożliwiają zapewnienie autentyczności, czyli atrybutu bezpieczeństwa polegającego na tym, że użytkownik jest tym, za kogo się podaje,
- umożliwienie szybkiego i niezawodnego dostępu do korzystania z informacji oraz z funkcjonalności systemu sterowania ruchem kolejowym,
- wdrożenie zasady najmniejszego uprzywilejowania, czyli mechanizmów które zapewnią, że użytkownicy będą posiadali jak najmniejsze przywileje w systemie zgodne z przydzielonymi obowiązkami, funkcjami i rolami.

Dodatkowo w realizowanym projekcie dokonano analizy możliwości wdrożenia w komputerowych systemach sterowania poszczególnych elementów kontroli bezpieczeństwa CIS (Critical Security Controls) wydanych przez instytut SANS [15]. Standard CIS Controls w wersji 8 zawiera konkretne rekomendacje podzielone na 18 grup środków bezpieczeństwa (rozwiniętych na 153 szczegółowe wymagania) dotyczące działań oraz najlepszych praktyk poprawiających cyberbezpieczeństwo. Dla realizowanego projektu ze standardu CIS Controls v8 wybrano następujące środki kontroli bezpieczeństwa:

- kontrola 04: bezpieczna konfiguracja zasobów i oprogramowania, kontrola 12: zarządzanie infrastrukturą sieciową oraz kontrola 13: monitorowanie i ochrona sieci – system sterowania ruchem kolejowym, oprócz segmentacji i separacji sieci będzie chroniony systemem klasy firewall w sposób zapewniający ochronę przed niepożądanymi połączeniami do Lokalnego Centrum Sterowania, a bezpośrednia komunikacja możliwa będzie poprzez tunele VPN (ang. Virtual Private Network),
- kontrola 05: zarządzanie kontami oraz kontrola 06: zarządzanie kontrolą dostępu – dostęp administratorów i serwisantów zewnętrznych do systemu sterowania ruchem kolejowym zapewniony będzie za pomocą narzędzia klasy PAM (Privileged Access Management), czyli rozwiązania dotyczącego zarządzana dostępem uprzywilejowanym, który zapewni bezpieczeństwo w zakresie tożsamości użytkowników oraz ochronę przed cyberzagrożeniami poprzez monitorowanie, wykrywanie i zapobieganie nieautoryzowanemu, uprzywilejowanemu dostępowi do zasobów systemu sterowania ruchem kolejowym.

W ramach zarządzania kontami zakładane jest wdrożenie serwera dostępowego i przesiadkowego, dwuskładniowe uwierzytelnianie użytkownika, rejestracja i audyt sesji zdalnych zarówno aktualnych jak i archiwalnych, nagrywanie wszystkich trwających sesji oraz możliwość ich odtworzenia, śledzenie aktywności użytkowników, budowanie indywidualnych profili behawioralnych użytkowników co pozwoli wykryć anomalie w sesji użytkownika i na ich podstawie raportować do SOC sesję jako podejrzaną oraz automatycznie wstrzymać lub zablokować podejrzaną sesję oraz użytkownika,

- kontrola 08: zarządzanie dziennikiem audytu – dostęp do dzienników systemowych zapewni kontrolę aktywności użytkowników i serwisantów w systemach srk poprzez dostęp i zarządzanie logami systemowymi, co w przypadku incydentu cyberbezpieczeństwa zapewni wiedzę na temat danego zdarzenia. Kontrola ta zapewniona zostanie poprzez system klasy SIEM służący do zbierania i przetwarzania logów oraz agregowania i korelowania zdarzeń dla zespołu SOC (Security Operations Center). W ten sposób będzie można monitorować i wykrywać naruszenia bezpieczeństwa np. nieautoryzowane próby połączeń do systemów,
- kontrola 15: zarządzanie dostawcami usług – dostęp serwisantów zewnętrznych będących dostawcami usług w systemie sterowania ruchem kolejowym zapewniony będzie za pomocą narzędzia klasy PAM oraz monitorowany za pomocą systemu klasy SIEM,
- kontrola 17: zarządzanie i reagowanie na incydenty – kontrola zapewniona zostanie przez zespół SOC i wdrożone narzędzia klasy PAM oraz SIEM, a także opracowane w tym celu procedury reagowania, co umożliwi m.in. wyznaczenie osób po stronie SOC, zarządcy infrastruktury kolejowej jak i dostawcy systemów sterowania ruchem kolejowy do procesu zarządzania obsługą wykrytych incydentów oraz ustanowienie procesu reagowania na nie.

Na podstawie powyższych kontroli i otoczenia prawnego określono wymagania funkcjonalne dla projektowanego i opisywanego rozwiązania. Rozwiązanie bezpiecznego zdalnego dostępu do systemów kluczowych ma zapewnić:

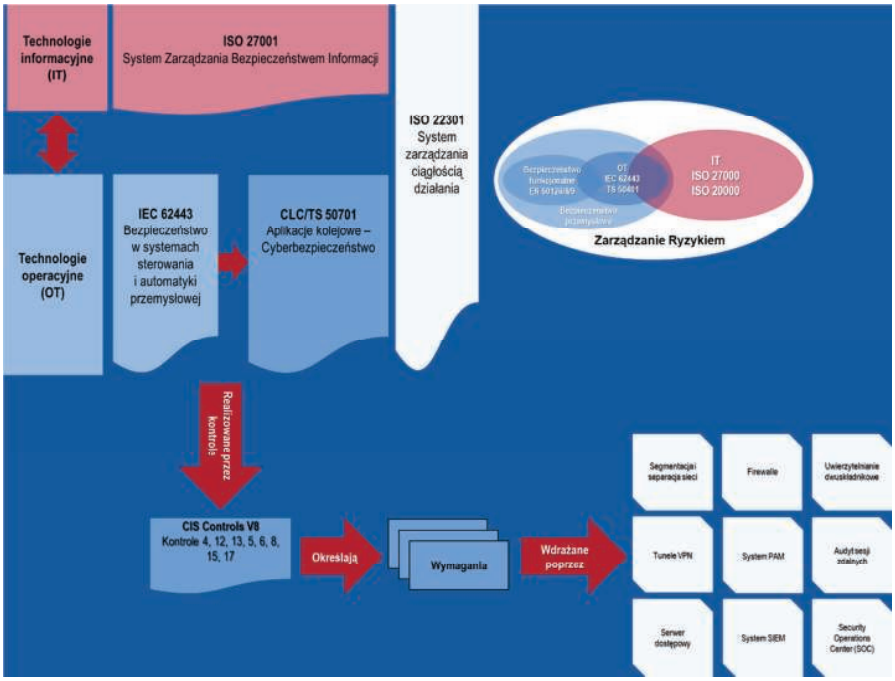
- szybki zdalny dostęp do logów oraz narzędzi diagnostycznych w systemach sterowania ruchem kolejowym w celu identyfikacji przyczyny zaistniałego problemu lub awarii,
- zdalne zarządzania sesjami serwisantów zewnętrznych oraz użytkowników z poziomu zarządcy infrastruktury (gestora systemu) oraz zespołu SOC,
- rozliczalność serwisantów zewnętrznych systemów sterowania ruchem kolejowym przez zarządcę infrastruktury kolejowej,
- integrację z systemem klasy SIEM, a przez to umożliwienie zarządzania i reagowania na incydenty cybernetyczne.

Proces określania komponentów rozwiązania bezpiecznego zdalnego dostępu do systemów przedstawiony został na ilustracji **2**.

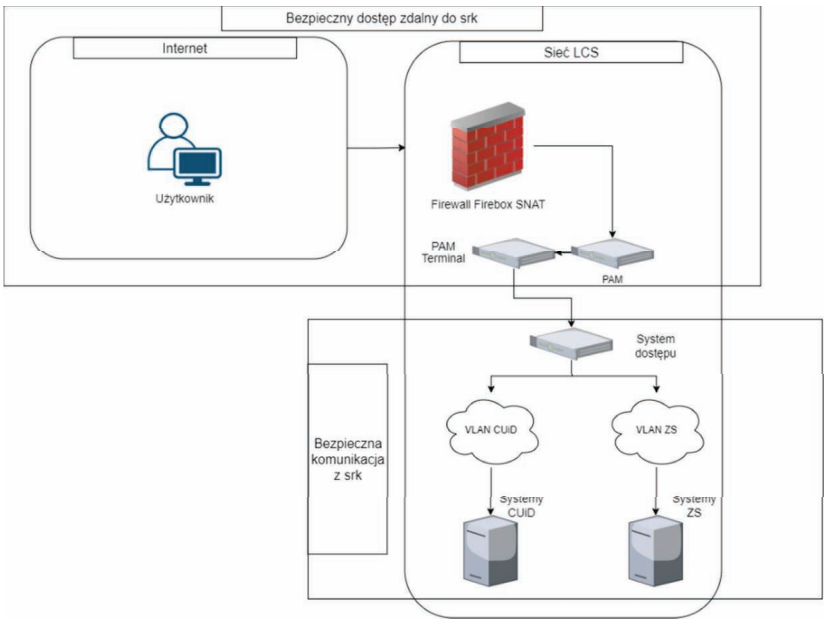
Rozwiązanie bezpiecznego zdalnego dostępu do systemów kluczowych i etapy przedsięwzięcia

Realizacja przedsięwzięcia podzielona została na następujące fazy:

1. opracowanie architektury rozwiązania (koncepcje, studium wykonalności),
2. wdrożenie laboratoryjne rozwiązania u dostawcy systemu,
3. testy opracowanego rozwiązania (raport techniczny z przeprowadzonych testów wraz z wnioskami, przeprowadzenie oceny znaczenia zmiany zgodnie z procedurami SMS),
4. akceptacja interesariuszy (zarządca infrastruktury, dostawca systemu sterowania ruchem kolejowym, SOC),
5. wdrożenie rozwiązania w środo-



***2**. Wpływ otoczenia prawnego i wymagań technicznych na komponenty rozwiązania. Opracowanie własne*



***3**. Architektura logiczna systemu. Opracowanie własne*

wisku produkcyjnym, w Lokalnym Centrum Sterowania.

Wymagania dla rozwiązania bezpiecznego zdalnego dostępu do systemów kluczowych stanowiły podstawę do opracowania podstawowej architektury logicznej rozwiązania, przedstawionej na ilustracji **3**.

Podsumowanie i wnioski

Aktualnie realizowany projekt zakończony został w fazie 2 (wdrożenia laboratoryjnego), a wdrożenie potwierdziło poprawność wszystkich założonych funkcji projektowanego rozwiązania oraz prawidłowe działanie systemu klasy PAM w zakresie zarządzania uprawnieniami oraz kontroli i rejestracji zdalnych sesji oraz zarządzania dziennikami zdarzeń w systemie klasy SIEM. Z tego punktu widzenia nie ma przeszkód technicznych do realizacji zdalnego dostępu zarówno do systemów diagnostycznych jak i systemów sterowania ruchem kolejowym. ◄

Materiały źródłowe

[1] 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). https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CELEX%3A32022L2555

[2] Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa. https://isap.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=WDU20180001560

[3] Dyrektywa Parlamentu Europejskiego i Rady 2012/34/UE z dnia 21 listopada 2012 r. w sprawie utworzenia jednolitego europejskiego obszaru kolejowego (przekształcenie). https://eur-lex.europa.eu/legal-content/PL/ALL/?uri=CELEX%3A32012L0034

[4] Rozporządzenie Rady Ministrów z dnia 11 września 2018 r. w sprawie wykazu usług kluczowych oraz progów istotności skutku zakłócającego incydentu dla świadczenia usług kluczowych. https://isap.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=WDU20180001806

[5] Ustawa z dnia 28 marca 2003 r. o transporcie kolejowym. https://isap.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=wdu20030860789

[6] 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. https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=celex%3A32022L2557

[7] Rozporządzenie delegowane Komisji (UE) 2023/2450 z dnia 25 lipca 2023 r. uzupełniające dyrektywę Parlamentu Europejskiego i Rady (UE) 2022/2557 przez ustanowienie wykazu usług kluczowych. https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CELEX:32023R2450

[8] EN 50126 (IEC 62278) – Reliability, Availability, Maintainability, and Safety (RAMS)

[9] ISO/IEC 27000:2018

[10] ISO/IEC 20000-1:2018 Service Management System (SMS) Standard

[11] IEC 62443-1-1, Industrial communication networks – Network and system security

[12] CLC/TS 50701:2023 Railway applications – Cybersecurity

[13] ISO 22301:2019, Security and resilience – Business continuity management systems – Requirements

[14] Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/798 z dnia 11 maja 2016 r. w sprawie bezpieczeństwa kolei. https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CELEX:02016L0798-20200528

[15] Center for Internet Security CIS, Critical Security Controls Version 8, 2021. https://www.cisecurity.org/controls/v8

Powszechnie przyjęte rozwiązania - sposób zapewnienia cyberbezpieczeństwa w produkcie

Code of practice - method for assuring cybersecurity in product

Marek Kuciński

Mgr inż.

voestalpine Signaling Poland Sp. z o. o.

marek.kucinski@voestalpine.com

Mariusz Buława

Dr inż.

voestalpine Signaling Poland Sp. z o. o.

mariusz.bulawa@voestalpine.com

Streszczenie: Wdrożenie cyberbezpieczeństwa w systemach sterowania ruchem kolejowym nie jest zadaniem łatwym. Zgodnie ze zdefiniowanymi procesami bezpiecznego wytwarzania produktów (w szczególności zdefiniowanymi w IEC62443-4-1 i TS50701) wymagane jest podjęcie zadań takich jak: analiza zagrożeń, definicja wymagań, projekt i implementacja, weryfikacja i testowanie. Proces ten można znacząco uprościć wykorzystując powszechnie przyjęte rozwiązania (ang. c*ode of practice*). W artykule przedstawiono przykładowe wykorzystanie tej możliwości w kontekście sterownika obiektowego zgodnego z wymaganiami EULYNX.

Słowa kluczowe: *Cyberbezpieczeństwo; EULYNX; Sterownik Obiektowy; TS50701; IEC62443*

Abstract: Introducing cybersecurity in railway traffic command and control systems is not an easy task. Conforming to defined processes of secure product development (especially defined in IEC62443-4-1 and TS50701) there are required tasks to be done such as: threat analysis, requirements definition; design and implemmentation, verification and testing. This process could be significantly simplified with utilization of the industry approved codes of practice. In the article an example showing this possibility was given based on the EULYNX compliant Object Controller.

Keywords: *Cybersecurity; EULYNX; Object Controller; TS50701; IEC62443*

Wstęp

Wzrastający poziom zagrożeń, zarówno lokalnych jak i globalnych, powoduje, że wdrożenie cyberbezpieczeństwa w produktach staje się nie tylko tematem ważnym, ale i obowiązkowym. Nadchodzące wejście w życie wymogów dyrektywy NIS2 [1] nałoży na wiele podmiotów z branży transportu szereg wymogów tak formalnych jak i technicznych. Odkładanie w wielu firmach inwestycji w obszarze cyberbezpieczeństwa spowodowało, że dystans do nadrobienia jest znaczny. Powoduje to potrzebę stosowania efektywnych i adekwatnych metod w celu jak najszybszego osiągnięcia pożądanego poziomu cyberbezpieczeństwa.

Cyberbezpieczeństwo na kolei a normy

W szczególności systemy sterowania ruchem kolejowym, ze względu na ich rolę w całym systemie kolejowym, wymagają szczególnej uwagi. Potencjalne błędne zadziałanie może doprowadzić do utraty zdrowia i życia wielu ludzi lub szkód materialnych w znacznym rozmiarze. Stąd wiele z tych systemów musi zapewnić poziom integralności bezpieczeństwa SIL-4.

Dotąd stosowane metodyki związane z bezpieczeństwem funkcjonalnym, zdefiniowane przez CENELEC w grupie norm EN50126, EN50128 czy EN50159, nie zapewniają wystarczającego poziomu ochrony przed intencjonalnymi próbami naruszenia integralności systemów. Stąd konieczość sięgnięcia do opracowań definijących kompleksowe podejście do cyberbezpieczeństwa w produkcie. Dobrym punktem odniesienia jest zespół norm IEC62443, w szczególności części -4-1 [2] i -4-2 [3]. Pierwsza z nich definiuje wymagania procesowe i organizacyjne dla dostawców komponentów i podsystemów. Druga grupuje i wymienia konkretne wymagania techniczne, które powinny być zaimplementowane w komponentach i podsystemach. Dobór właściwych i adekwatnych rozwiązań bazujących jedynie na powyższych normach jest zadaniem trudnym, obarczonym znacznym ryzykiem.

Trudność ta została już zauważona przez ekspertów z branży kolejowej. W celu usprawnienia zrozumienia potrzeb a następnie właściwej ich implementacji opracowana została specyfikacja techniczna TS50701 [4], której celem jest wdrożenie wymagań i rekomendacji związanych z wdrożeniem cyberbezpieczeństwa na kolei. Prezentuje ona odniesienie pomiędzy implementacją cyberbezpieczeństwa i bezpieczeństwa funkcjonalnego zgodnie z modelem V. Procesy zostały podzielone na fazy, które są jasno zdefiniowane i następują po sobie.

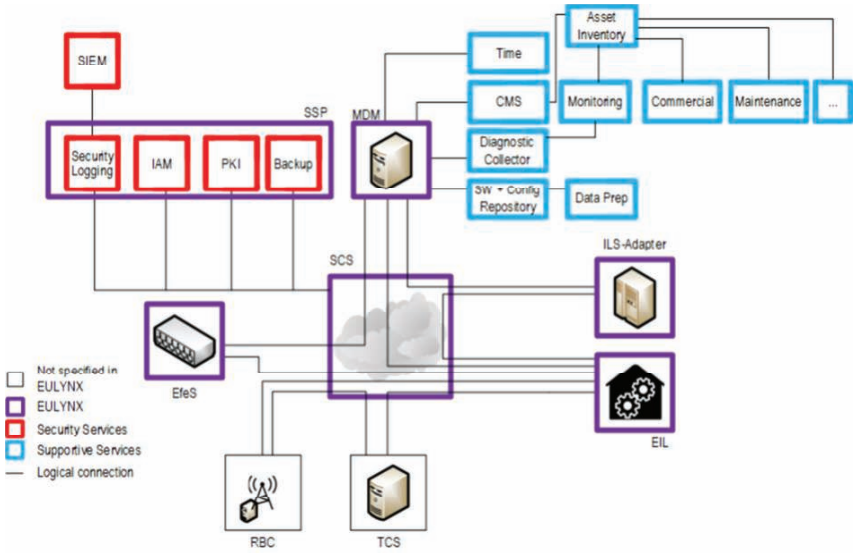
1. Dr inż. Mariusz Buława, Prezes Zarządu voestalpine Signaling Poland podczas prezentacji na Międzynarodowej Konferencji naukowo-technicznej „IT/OT w transporcie szynowym" w Warszawie

2. Mgr inż. Marcin Kuciński z voestalpine Signaling Poland prezentujący „Powszechnie przyjęte praktyki a wdrożenie cyberbezpieczeństwa w produkcie" podczas Międzynarodowej Konferencji naukowo-technicznej „IT/OT w transporcie szynowym" w Warszawie

Inicjatywa EULYNX

Przykładem praktycznego podejścia do zapewnienia cybersecurity w systemach sterowania ruchem kolejowym są wymagania opracowane w ramach inicjatywy EULYNX. Pierwszym krokiem, od którego należy zacząć jest zidentyfikowanie systemu i jego otoczenia (ang. System Definition) oraz podzieleniu go na strefy bezpieczeństwa połączone konduktami [5]. Przykładowe podejście zaprezentowano na rys. **3**. Tak zdefiniowana jest architektura systemu w kontekście cyberbezpieczeństwa w specyfikacjach EULYNX [7].

W kontekście sterowników obiektowych (EfeS) widoczne są dwa połączenia (kondukty) – pierwszy do cyfrowego interlockingu (EIL) a drugi do systemu monitoringu, diagnostyki i utrzymania (MDM). Dla każdej strefy i konduktu należy przeprowadzić analizę zagrożeń. Składa się ona z dwóch kluczowych elementów podlegających ocenie: prawdopodobieństwa (ang. likelihood) oraz znaczenia (ang. severity). Korzystając z tych dwóch określonych współczynników można przystąpić do przypisywania rozwiązań adekwanych do ryzyk, których poziom nie jest akceptowalny, względem przyjętych założeń.



3. Architektura systemu w kontekście cyberbezpieczeństwa w EULYNX [7]

Kodeks postępowania

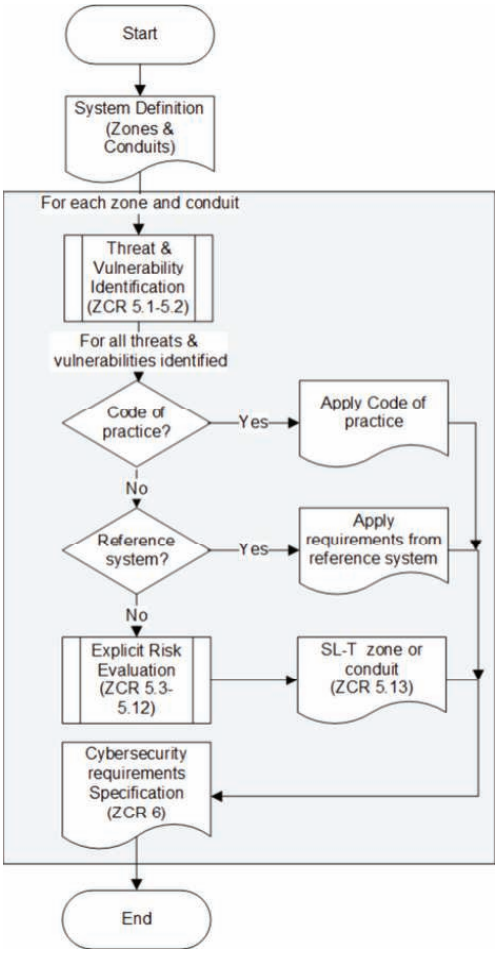
W normie TS50701 szczególnie interesująca jest zaproponowana metodyka szczegółowej oceny ryzyka (rys. **4**). Wskazano dwie możliwości uproszczenia analizy ryzyka z wykorzystaniem kodeksu postępowania lub systemu referencyjnego. Skorzystanie z tych możliwości pozwala znacząco uprościć proces doboru właściwych rozwiązań. Szczególnie korzystne jest wykorzystanie powszechnie przyjętych przez ekspertów branżowych rozwiązań tzw. kodeksów postępowania. Warto przytoczyć tu definicję [4]:

3.1.21 kodeks postępowania
<w cyberbezpieczeństwie> spisany zestaw reguł, zatwierdzony przez grupę ekspertów, który jeśli zostanie poprawnie zastosowany, może zostać wykorzystany do ograniczenia jednego lub więcej zagrożeń
3.1.21 code of practice
<in cybersecurity> written set of rules, validated by a group of experts, that, when correctly applied, can be used to control one or more specific threats

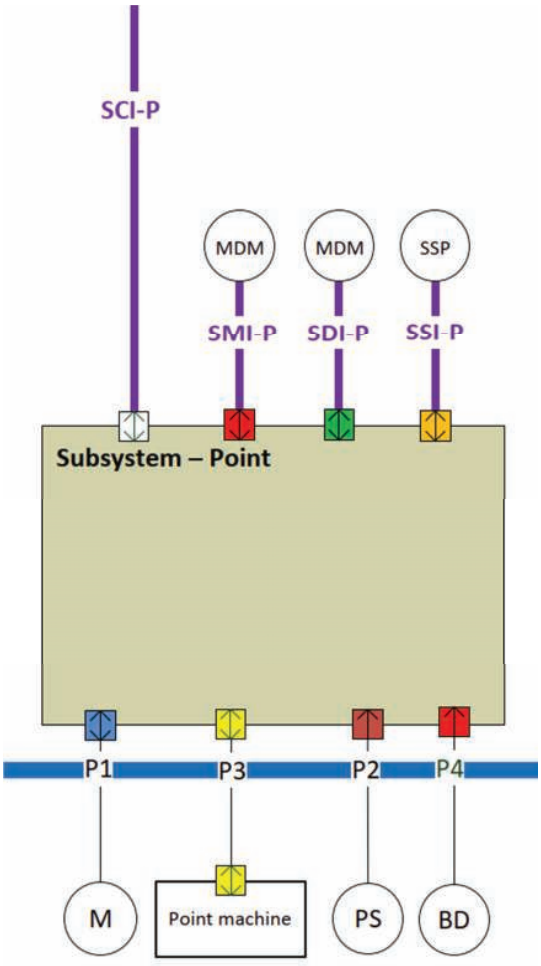
Sterownik obiektowy i jego interfejsy

Dobrym przykładem wykorzystania tej możliwości jest specyfikacja EULYNX Baseline 4 Release 2 (najnowsza aktualnie dostępna). W architekturze dla każdego komponentu (np. sterowników obiektowych) zdefiniowano komplet interfejsów. Przykładowo dla sterownika obiektu typu rozjazd (ang. point) wskazano m.in. interfejsy SCI-P, SDI-P, SMI-P i SSI (rys. **5**). Aby nie przeprowadzać szczegółowej analizy względem wszystkich zagrożeń dla interfejsów zdecydowano się na wybranie powszechnie uznanego za bezpieczny interfejsu TLS w wersji 1.3 (rys. **6**) [7]. Dobór tego protokołu pozwolił ograniczyć do pomijalnego poziomu m.in. poniższe zagrożenia:

1) Naruszenie poufności – cała komunikacja jest szyfrowana kluczem symetrycznym, który jest negocjowany unikalnie dla każdej sesji.
2) Naruszenie integralności – każda wiadomość posiada zabezpieczenie w postaci MAC (ang. Message Authentication Code) co umożliwia wykrycie usunięcia lub podmiany w treści przesyłanej informacji.
3) Podszywanie i zaprzeczalność – połączenia nawiazywane są z wy-



***4**. Diagram szczegółowej analiza ryzyka [4]*



***5**. Definicja interfejsów dla sterownika obiektu typu rozjazd [6]*

***6**. Połączenie między sterownikiem obiektowym a cyfrowym interlockingiem [7]*

korzystaniem kryptografii asymetrycznej. Dzięki temu uczestnicy komunikacji mogą być pewni, że partnerzy są tymi, za których się podają.

4) Atak powtórzenia – ramki są podpisywane przez MAC z uwzględnieniem numeru sekwencyjnego (który nie jest przesyłany w wiadomości) stąd usunięcia czy powtórzenia są wykrywalne.

Dzięki powyższym cechom połączenie przez interfejsy prowadzone konduktami chronionymi przez TLS 1.3 można uznać za odpowiednio zabezpieczone.

Podsumowanie

Przed dostawcami systemów sterowania ruchem kolejowych stoi duże wyzwanie w postaci zapewnienia zgodności z wymaganiami cyberbezpieczeństwa. Zagadnienie jest złożone zarówno organizacyjnie jak i technicznie a jednocześnie ważne i pilne. Tym samym szczególnego znaczenia nabiera dobór właściwych i adekwatnych metod pozwalających ograniczać zidentyfikowane ryzyka. Jednym z nich jest stosowanie kodeksów postępowania tzn. powszechnie przyjętych rozwiązań technicznych, zamiast szczegółowej analizy ryzyka. Wykorzystanie tej możliwości znacząco skraca czas projektowania i wprowadzenia na rynek. ◄

Materiały źródłowe

[1] European Parliament; Dyrektywa NIS2; Directive (EU) 2022/2555
[2] IEC 62443-4-1:2018; Security for industrial automation and control systems Part 4-1: Secure product development lifecycle requirements; ISBN 978-2-8322-5239-0
[3] IEC 62443-4-2:2019; Security for industrial automation and control systems Part 4-2: Technical security requirements for IACS components; ISBN 978-2-8322-6597-0
[4] PD CLC/TS 50701:2023; Railway applications - Cybersecurity; ISBN ISBN 978 0 539 20855 9
[5] IEC62443-3-2:2020; Security for industrial automation and control systems – Part 3-2: Security risk assessment for system design; ISBN 978-2-8322-8501-5
[6] EULYNX System Definition – Appendix A1; Eu.Doc.7 A1 v4.2.
[7] EULYNX Security Concept; Eu-.Doc.15 v2.1

Relacja z VI Międzynarodowej Konferencji Naukowo-Technicznej IT/OT w Transporcie Szynowym 2023 r., Warszawa, 29-31 stycznia 2024 r.

W dniach 29-31 stycznia 2024 r. w Warszawskim Domu Technika NOT odbyła się VI edycja Międzynarodowej Konferencji Naukowo-Technicznej „IT/OT w Transporcie Szynowym". Organizatorami konferencji byli Zarząd Krajowy Stowarzyszenia Inżynierów i Techników Komunikacji RP oraz Instytut Kolejnictwa. Wydarzenie zostało objęte m.in. patronatami Ministerstwa Cyfryzacji, Urzędu Transportu Kolejowego oraz innych instytucji i firm, którym bliska jest tematyka bezpieczeństwa i cyberbezpieczeństwa transportu szynowego.

Konferencja uzyskała dofinansowanie Ministerstwa Edukacji i Nauki w ramach programu: Doskonała Nauka II.

Komitet Programowy konferencji zadbał o stronę merytoryczną przygotowując bogaty program wydarzenia. W skład Komitetu Programowego weszli: dr inż. Jacek Paś, Prezes SITK RP; dr inż. Wawrzyniec Wychowański, Sekretarz Generalny SITK RP; dr hab. inż. Marek Pawlik, prof. IK; dr hab. inż. Andrzej Toruń, prof. IK; dr inż. Marek Sumiła z Instytutu Kolejnictwa; mgr inż. Radosław Zawierucha, Członek Zarządu PKP Informatyka oraz dr inż. Andrzej Bartosiewicz, Prezes CISO4U.

Kolej przeznaczona zarówno do przewozów pasażerskich jak i towarowych należy niewątpliwie do infrastruktury krytycznej państwa, narażonej potencjalnie na ataki hakerskie i inne zagrożenia pochodzące z sieci komputerowych, za którymi stać mogą np. organizacje terrorystyczne, nieprzyjazne państwa czy też domorośli desperaci.

Tematyka Konferencji objęła szerokie spektrum zagadnień takich jak: budowanie wiedzy o relacji między systemami IT oraz systemami OT zarówno dla infrastruktury jak i taboru szynowego, omówienie ryzyk dla systemów cyfrowych płynących z cyberprzestrzeni, wskazanie możliwych działań w zakresie cyberbezpieczeństwa kolei, przedyskutowanie kierunków rozwoju systemów IT oraz systemów OT w transporcie szynowym, a także interoperacyjnych systemów łączności i bezpiecznej kontroli jazdy opartych na transmisji danych w relacji tor-pojazd, w tym systemów GSM-R oraz FRMCS wraz z przedstawieniem planu migracji pomiędzy nimi.

Zaproponowane tematy spotkały się z dużym zainteresowaniem ze strony biznesu, przemysłu, instytucji rządowych i środowiska akademickiego, którzy licznie przybyli na konferencję.

Partnerami Konferencji były takie firmy jak Tekniska Polska (Partner Platynowy), EY, Splunk, VIAVI Solutions, RazorSecure, Elmark Automatyka, voestalpine Signaling Poland, ATDI, Ketel (Partner Złoty), Dell Technologies, Infodas (Partner Srebrny).

W sesji otwierającej, na zakończenie wypowiedzi przedstawicieli urzędów i kolei oraz głównych partnerów konferencji, krótko przedstawiona została skala złożoności współczesnych rozwiązań cyfrowych z uwzględnieniem systemów informacyjnych IT oraz systemów eksploatacyjnych OT wraz z przykładami cyberzagrożeń dla rozwiązań szeroko stosowanych w transporcie kolejowym.

Ważnym elementem programu była debata nad dyrektywą Parlamentu Europejskiego NIS 2, która musi zostać wprowadzona do prawa krajowego do października 2024 roku.

Pośród zaproszonych ekspertów warto szczególnie wspomnieć nazwiska Keira Fitcha – Dyrektora Departamentu Interoperacyjności i Bezpieczeństwa Kolei w ramach Dyrektoriatu Generalnego Komisji Europejskiej do spraw Transportu i Mobilności (Head of Unit Rail Safefy and Interoperability z DG MOVE European Commission) oraz Josepha Doppelbauera – Dyrektora wykonawczego Agencji Unii Europejskiej do spraw Kolei (Executive Director of the European Union Agency for Railways), którzy przygotowali wprowadzenie do tej tematyki.

Kolejno przygotowana została seria dyskusji panelowych z udziałem ekspertów z najważniejszych branżowych organizacji międzynarodowych takich jak ERA (European Union Agency for Railways) oraz ENISA (European Union Agency for Cyber Security) i krajowych – Ciso #Poland i NASK Państwowy Instytut Badawczy.

***1**. Prezes SITK RP Jacek Paś otwiera konferencję*

***2**. Sekretarz Generalny SITK RP Wawrzyniec Wychowański wita zaproszonych Gości*

***3**. Profesor Marek Pawlik podczas prezentacji wprowadzającej*

***4**. Audytorium konferencji*

Tematyka ta wzbudziła ogromne zainteresowanie przedstawicieli firm przemysłowych zaangażowanych w tworzenie produktów i rozwiązań technicznych dla linii i pojazdów kolejowych, w tym pojazdów trakcyjnych. W dyskusję zaangażowali się liczni menadżerowie firm przemysłowych, dla których nowe wymagania Unii Europejskiej wiążą się bezpośrednio z koniecznością ich implementowania w rozwiązaniach praktycznych.

Do udziału w dyskusji Stowarzyszenie Inżynierów i Techników Komunikacji RP zaprosiło zarówno specjalistów z Polski jak i innych krajów europejskich: Niemiec, Francji, Austrii, Czech, Rumunii i Litwy. Pozwoliło to na uzyskanie spojrzenia na zagadnienia cyberbezpieczeństwa w szerszym, międzynarodowym wymiarze. Udział tak wielu podmiotów zagranicznych był możliwy dzięki osobistemu i bezpośredniemu zaangażowaniu Sekretarza Generalnego SITK RP – Wawrzyńca Wychowańskiego.

Doskonale sprawdziła się także koncepcja warsztatów realizowanych równolegle do głównego nurtu konferencji. Wzięły w nich udział firmy szczególnie zainteresowane problematyką nowych uregulowań prawnych. Warsztaty były jednocześnie doskonałą okazją do bezpośredniego spotkania przedstawicieli przemysłu ze specjalistami zaangażowanymi w proces tworzenia nowych europejskich regulacji prawnych. Najszerzej omawianym i budzącym emocje okazało się nowe wydanie Technicznej Specyfikacji Interoperacyjności dla podsystemów sterowania systemu kolei w Unii Europejskiej.

Sprawdziła się także formuła polegająca na

***5**. Policy Officer z DG Move European Union, Wawrzyniec Pershke i Project Officer z ERA ERTMS & Telematics Unit, Juan Hernandez Fernandez wspólnie prowadzą "TSI CCS 2023 Revision Panel"*

***6**. Keir Fitch, Dyrektor Departamentu Interoperacyjności i Bezpieczeństwa Kolei w ramach Dyrektoriatu Generalnego Komisji Europejskiej do spraw Transportu i Mobilności oraz Joseph Doppelbauer, Dyrektor wykonawczy Agencji Unii Europejskiej do spraw Kolei podczas zdalnej sesji wprowadzającej w tematykę cyberbezpieczeństwa*

***7**. Sekretarz Generalny SITK RP Wawrzyniec Wychowański i Kierownik Laboratorium Automatyki i Telekomunikacji w Instytucie Kolejnictwa Marek Sumiła prowadzą wspólnie panel dyskusyjny pt. „Train 2 Ground Communications Railways" z udziałem firm: Rail Baltica, ATDI, Viavi Solutions, Kontron, Hitachi Energy, Nokia Solutions &Networks*

***8**. Dyrektor infrastruktury kolejowej w Siemens Mobility Adam Szymankiewicz, VP Sales w Tekniska Polska Piotr Gawiński, CEO w RazorSucure Alex Cowan, Vice President Products & Solutions Cybersecurity w Alstom Eddy Thesee w międzynarodowym panelu poświęconym cyberbezpieczeństwu*

***9**. Policy Officer z DG Move European Union Wawrzyniec Pershke i Kierownk Zakładu Sterowania Ruchem I Telematyki w Instytucie Kolejnictwa Andrzej Toruń prowadzą wspólnie „TSI CCS 2023 Revision Panel" z udziałem firm: PKP PLK, Alstom Polska, voestalpine Signaling Poland, Siemens Mobility, Sprava Zeleznic*

***10**. Prezes Zarządu ATDI Agnieszka Slosarska i Sekretarz Generalny SITK RP Wawrzyniec Wychowański razem prowadzą Sesję „Train 2 Ground Communications Radio Planning"*

podzieleniu konferencji na różne aktywności realizowane w kolejnych jej dniach. I tak, pierwszy dzień poświęcono głównie na serię paneli dyskusyjnych zaś drugi na sesje wykładowe z prezentacjami poszczególnych podmiotów.

W porównaniu do poprzedniej edycji tego wydarzenia rozszerzono znacząco zakres merytoryczny o zagadnienia wymagań dla przewoźników kolejowych i dostawców taboru kolejowego. Tematyka ta wypełniła trzeci, ostatni dzień konferencji, w którym obrady przeniosły się do siedziby Instytutu Kolejnictwa w Warszawie na Olszynce Grochowskiej. Część tą zorganizował i prowadził dr hab. inż. Marek Pawlik, prof. IK.

Zgromadziła ona przedstawicieli czołowych firm związanych z produkcją taboru kolejowego: Newag, Pesa, Siemens Mobility, Alstom, Stadler Polska, Skoda Polska i RazorSecure.

Konferencja zakończyła się wycieczką techniczną do Centrum Serwisowego Pendolino Alstom Polska w Warszawie na Pradze. Poziom nowoczesności tego miejsca wzbudził ogromne zainteresowanie uczestników, którym umożliwiono zajrzenie nie tylko do kabiny sterowniczej składu ale również do najrozmaitszych zakamarków pociągu i służących jego serwisowaniu urządzeń.

Podsumowując – tegoroczna Konferencja okazała się dużym sukcesem. Sprawdziła się zarówno jej formuła jak to, że w jednym miejscu udało się zebrać wszystkich głównych aktorów rynku kolejowego z Polski i zagranicy. Wieczorne spotkania w znakomitej, koleżeńskiej atmosferze pozwoliły na networking i liczne nieformalne rozmowy sprzyjające zawieraniu relacji. Uczestnicy nie kryli swego zadowolenia, co miejmy nadzieję, przyczyni się do sukcesu kolejnej edycji Konferencji.

Relację przygotowała: Elżbieta Nowicka, Manager Marketingu i Komunikacji, SITK RP ZK

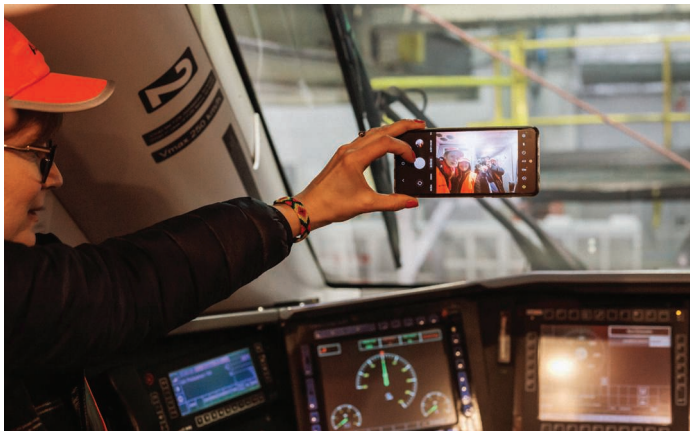
***11**. Prezes Zarządu voestalpine Signaling Poland Mariusz Buława podczas prezentacji w międzynarodowej sesji poświęconej cyberbezpieczeństwu*

***12**. Prezes Fundacji CISO #Poland Andrzej Bartosiewicz podczas prezentacji w międzynarodowej sesji poświęconej cyberbezpieczeństwu"*

***13**. Pre-sales & Bid Manager CEE Isidora Karapandza podczas prezentacji pt. „Kontron Transportation FRMC migration plan and FRMCS product portfolio"*

***14**. Profesor Marek Pawlik prowadzi międzynarodowy panel dyskusyjny pt. „Railway rolling stock cybersecurity" z przedstawicielami firm: Newag, Pesa, Siemens Mobility, Alstom, Stadler Polska, Skoda Polska i RazorSecure*

***15**. Uczestnicy konferencji zwiedzają Centrum Serwisowe Pendolino, Alstom Polska na warszawskiej Pradze*



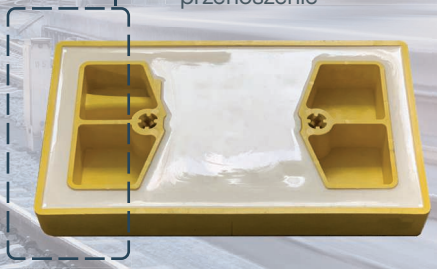
***16**. Pamiątkowe zdjęcie w kabinie maszynisty lokomotywy Pendolino*

rail-mil.eu

Technologie dostosowane
do potrzeb klienta.

Q7-BL-TR | Eurobalisa przełączalna

Q7 rmRailProtector4.0® | Rozwiązania dla ERTMS | ETCS - L1



Eurobalisa **Q7-BL-TR** produkcji firmy Rail-Mil jest jednym z produktów należących do rodziny **Q7 – rmRailProtector4.0®**, która została zaprojektowana specjalnie z myślą o wymogach oraz funkcjonalności systemów ERTMS i ETCS.

Podstawowe parametry urządzenia:

Eurobalisa o zmniejszonym rozmiarze
Obsługuje uniwersalny interfejs C, zgodny z wymaganiami SUBSET-036, umożliwiający współpracę z koderem LEU dowolnego producenta
Stopień szczelności obudowy IP67
Programowanie odbywa się bezprzewodowo, z wykorzystaniem dedykowanego programatora eurobalis Q7-UPKE
Posiada możliwość zablokowania interfejsu, dzięki czemu staje się niewidoczna dla przejeżdżającego pociągu

Rail-Mil sp. z o.o. jest polską firmą działającą w obszarze elektroniki i automatyki przemysłowej, która skupia się na oferowaniu kompletnych oraz innowacyjnych rozwiązań dla sektora kolejowego i wojskowego. Rozwiązania te oparte są na sprzęcie własnej produkcji, lub od wiodących na rynku zagranicznych partnerów. Naszym głównym celem jest dostarczanie polskich, nowoczesnych i niezawodnych rozwiązań na światowym poziomie dostosowanych do konkretnych potrzeb klienta. W celu zapewnienia najwyższej jakości proponowanych rozwiązań prowadzimy bliską współpracę z najlepszymi jednostkami naukowo-badawczymi w Polsce oraz renomowanymi partnerami zagranicznymi takimi jak m.in.: Ansys Inc., VIAVI Solutions, ERTMS Solutions, RedHat oraz Adlink.

Posiadamy certyfikaty: PN-EN ISO 9001:2015 oraz AQAP 2110:2016

ertms Więcej na temat ETCS i ERTMS: www.ertms.net

made in POLAND

MADE IN EU

rail-mil.eu

ZAKŁADY AUTOMATYKI ®
KOMBUD SA

WWW.KOMBUD.COM.PL

Zakłady Automatyki Kombud SA
ul. Wrocławska 7, 26-600 Radom
+48 48 389 43 01

PDP – POWIADAMIANIE DRÓŻNIKÓW PRZEJAZDOWYCH

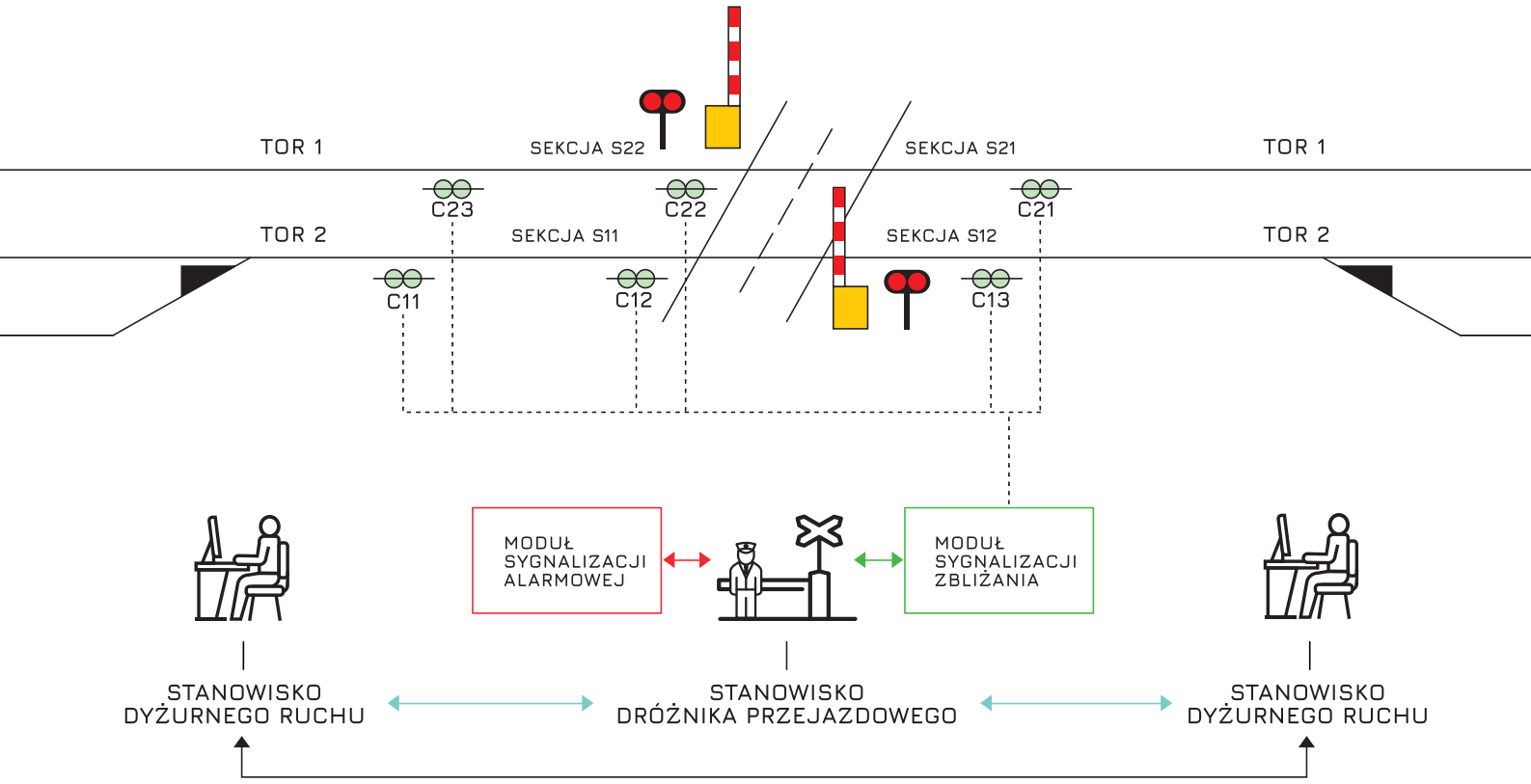
Podnosi poziom bezpieczeństwa i skraca czas zamknięcia przejazdów kolejowych kategorii A.

- dzięki integracji z systemem zdalnego sterowania i kierowania ruchem usprawnia proces prowadzenia ruchu
- pozwala na krótszy czas zamknięcia przejazdu
- zmniejszenie ryzyka wystąpienia błędów ludzkich
- monitoring pracy dróżnika umożliwia zdalną kontrolę jego obecności
- usprawnienie komunikacji z sąsiednimi posterunkami dzięki przesyłaniu informacji o sytuacjach szczególnych

FUNKCJE SYSTEMU PDP:

- dwukanałowa sygnalizacja alarmowa
- mechanizm kontroli obecności
- dwukierunkowa komunikacja
- rejestracja zdarzeń i powiadomień
- administrowanie i kontrola dostępu
- sygnalizacja alarmów i usterek
- samokontrola systemu
- automatyczne informacje dla sąsiednich posterunków

#TRANSFORMUJEMY TRANSPORT



TEKNISKA® | Everything connects

Dbamy o niezawodność i bezpieczeństwo Twojej sieci OT

PRZEMYSŁOWE SYSTEMY TRANSMISJI DANYCH

CYBERBEZPIECZEŃSTWO

SZKOLENIA

USŁUGI

PRZEMYSŁOWA TRANSMISJA DANYCH:

- Dobór technologii
- Rozwiązania
- Projektowanie sieci

KOMUNIKACJA RADIOWA

- GSM
- LTE
- 5G

- Integracja sieci OT i IT
- Usługi wdrożeniowe

CYBERBEZPIECZEŃSTWO W OT:

- Analiza bezpieczeństwa
- Projekt architektury
- Integracja ze SIEM/SOC
- Wsparcie analityka
- Zgodność z KSC
- Testy penetracyjne

SYSTEMY IDS

- Implementacja
- Obsługa

Everything connects

SZKOLENIA

SIECI PRZEMYSŁOWE

- Projektowanie sieci
- Ethernet przemysłowy

Bezpieczny zdalny dostęp

- Aplikacje przemysłowe
- Systemy produkcyjne
- Energetyka

CYBERBEZPIECZEŃSTWO

- Bezpieczeństwo SCADA
- Cyber kolej
- Sieci przemysłowe
- IDS
- Zarządzanie ryzykiem
- Infrastruktura krytyczna

Odwiedź nas

WWW.TEKNISKA.PL

ELMARK Automatyka

MOXA

Firewalle kolejowe Moxa TN-4900

Pierwszy firewall kolejowy z wbudowanym systemem cyberbezpieczeństwa klasy IPS

- Chroń sieci pokładowe wykorzystując moduł **IPS (Intrusion Prevention System)** wykrywający podatności cyberbezpieczeństwa na bazie analizy ruchu sieciowego.
- Polegaj na cyberbezpieczeństwie w oparciu o certyfikat **IEC 62443-4-2**.
- Agreguj zdarzenia i zarządzaj firewallami dzięki dedykowanej aplikacji MXSecurity.
- Buduj sieci w architekturze ETBN w oparciu o jedną z najbardziej zaawansowanych platform w zakresie wspracia i obsługi standardu IEC 61375.
- Wybierz optymalny model z prawie **20 dostępnych konfiguracji**.

Zobacz co potrafi
i sprawdź w naszym sklepie:
www.elmark.com.pl