PROBLEMY KOLEJNICTWA
RAILWAY REPORT Zeszyt 189 (grudzień 2020)
INSTYTUT KOLEJNICTWA
DOI: 10.36137/1896P
ISSN 0552-2145 (druk) ISSN 2544-9451 (on-line)

Cyberbezpieczeństwo zarządzania sieciami i partycjami w transporcie kolejowym

Jan PROCHÁZKA[1], Petr NOVOBILSKY[2], Dana PROCHÁZKOVA[3]

Streszczenie
Infrastruktura transportu kolejowego zapewnia codzienny przewóz dużej liczby osób i ładunków. Znaczenie kolei pod względem zapewnienia sprawności obsługi na danym obszarze czyni z niej infrastrukturę krytyczną. Obserwuje się istotny rozwój wykorzystania technologii informatycznych na kolei, podobnie jak we wszystkich innych branżach. Z tego względu zarządzanie koleją, jako systemem fizycznym, należy zastąpić zarządzaniem koleją, jako systemem cyberfizycznym. Infrastruktura kolejowa jest narażona na znaczące ataki zarówno w przestrzeni fizycznej, jak i w cyberprzestrzeni.
Artykuł jest poświęcony zarządzaniu sieciami komunikacyjnymi, służącymi do transmisji danych i partycjami, rozumianymi jako logicznie wydzielone zasoby informatyczne (służące do przetwarzania danych), wykorzystywanymi na potrzeby transportu kolejowego. Systemowo, wielopoziomowe, bezpieczne i niezależne (ang. *System Multiple Independent Levels of Security* – MILS) przetwarzanie danych spełnia wysokie wymagania dotyczące bezpieczeństwa systemu. MILS jest niezawodną architekturą bezpieczeństwa opartą na koncepcji separacji i kontrolowanego przepływu danych. W artykule opisano możliwości wykorzystania platformy MILS w systemie teleinformatycznym i systemie sterowania ruchem kolejowym.

Słowa kluczowe: Systemy cyberfizyczne, infrastruktura krytyczna, systemowo wielopoziomowe, bezpieczne i niezależne przetwarzanie danych (MILS)

1. Wstęp

Ochrona infrastruktury krytycznej stała się istotną częścią zaawansowanych strategii bezpieczeństwa systemów tworzonych przez ludzi. Infrastruktura krytyczna często obejmuje kilka następujących przestrzeni:

- przestrzeń fizyczną – rozległa sieć elementów fizycznych (punktowych lub liniowych),
- przestrzeń procesową – system zarządzania, czynnik ludzki, normy techniczne, odpowiednie prawodawstwo i strategia zarządzania [3, 9, 12],
- cyberprzestrzeń – sieć łączności, technologia sterowania.

Ponieważ ochrona fizyczna nie jest wystarczająca, należy zwrócić uwagę na bariery zabezpieczające dla wszystkich wymienionych rodzajów składowych (składowe twarde, miękkie, czynnik ludzki i normy techniczne). Komponenty fizyczne i centra operatorskie (systemy zarządzania i systemy sterowania) są połączone z systemami łączności. Łączność odbywa się w cyberprzestrzeni, która wraz z fizycznymi komponentami tworzy system cyberfizyczny (CPS). System łączności musi zapewnić niezawodną i łatwo dostępną wymianę danych, zdolną do zapewnienia utrzymywania przepustowości i jednocześnie powinien być bezpieczny [2]. Celem artykułu jest przedstawienie platformy MILS, jako użytecznego i sprawdzonego sposobu ochrony cyberprzestrzeni w sieciach o różnym poziomie bezpieczeństwa, z uwzględnieniem wymagań już istniejących i przygotowywanych norm bezpieczeństwa cyberprzestrzeni i kolei.

Ze względu na fizyczną rozległość, infrastruktura jest dużym obszarem potencjalnego ataku w przestrzeni fizycznej. Ma także wysokie wymagania dotyczące zasięgu systemu łączności i dlatego infrastruktura łączności publicznej jest również wykorzystywana do łączności między elementami infrastruktury. Według Peerenbooma [10], ogrom, otwartość i dynamizm publicznej sieci łączności, to także duży obszar potencjalnego ataku w cyberprzestrzeni, jednak z możliwymi skutkami zarówno w cyberprzestrzeni, jak i w przestrzeni fizycznej. Przykładem takiej infra-

[1] Dr; Politechnika Czeska w Pradze, Wydział Transportu; e-mail: japro2am@seznam.cz.
[2] Inż.; Q-media, s.r.o. Pocernicka 272/96, Praga.
[3] Prof. nadzw., dr; Politechnika Czeska w Pradze, Bezpieczeństwo kluczowych elementów infrastruktury.

struktury jest kolej. Projektowanie rozwiązań dla kolei w cyberprzestrzeni przedstawiono w rozdziale 2.

Bezpieczeństwo bram sieciowych, wykorzystywanych do przekazywania danych pokonujących interfejsy między systemami, można zapewnić w standardowy sposób, np. za pomocą kluczy dostępu, haseł i zapór ogniowych. Jednak w przypadku kluczowych elementów infrastruktury, zwykłe techniki zabezpieczania bram sieciowych mogą okazać się niewystarczające. Systemowo, wielopoziomowe, bezpieczne i niezależne przetwarzanie danych (MILS) jest w tym przypadku właściwym rozwiązaniem. System z zasadą MILS gwarantuje, że pokonanie jednej bariery nie wpływa na zachowanie poufności danych dla pozostałych. Zasady MILS są opisane w rozdziale 3.

W rozdziale 4 omówiono aspekty stosowania zasad MILS w środowisku kolejowym.

2. Sieć cybernetyczna w pociągu

Rozdział ten jest poświęcony wewnętrznej sieci cybernetycznej w pociągu. W celu lepszego zrozumienia zagadnienia, konieczne jest ogólne wyjaśnienie schematu działania sieci cybernetycznej infrastruktury kolejowej, począwszy od zasady funkcjonowania sieci dla infrastruktury, a następnie na wewnętrznych strefach sieci w pociągu.

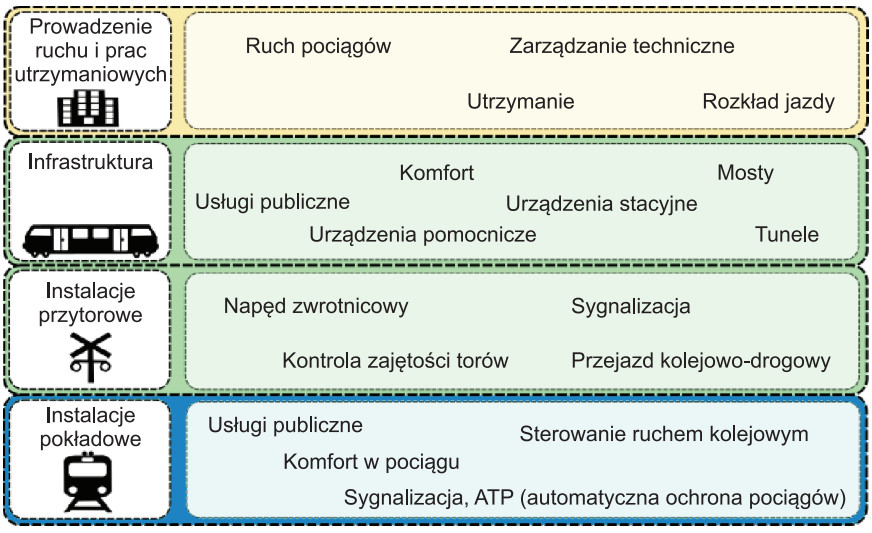
2.1. Kolejowa sieć cybernetyczna

Opis kolejowej sieci cybernetycznej jest oparty na normie prTS 50701 [13]. Do tej pory norma ta była przedmiotem komentarzy i opinii, zawiera jednak informacje, na których można polegać. Głównym celem zastosowania normy prTS 50701 jest wdrożenie wymagań normy IEC 62443 [7] do systemów łączności w środowisku kolejowym.

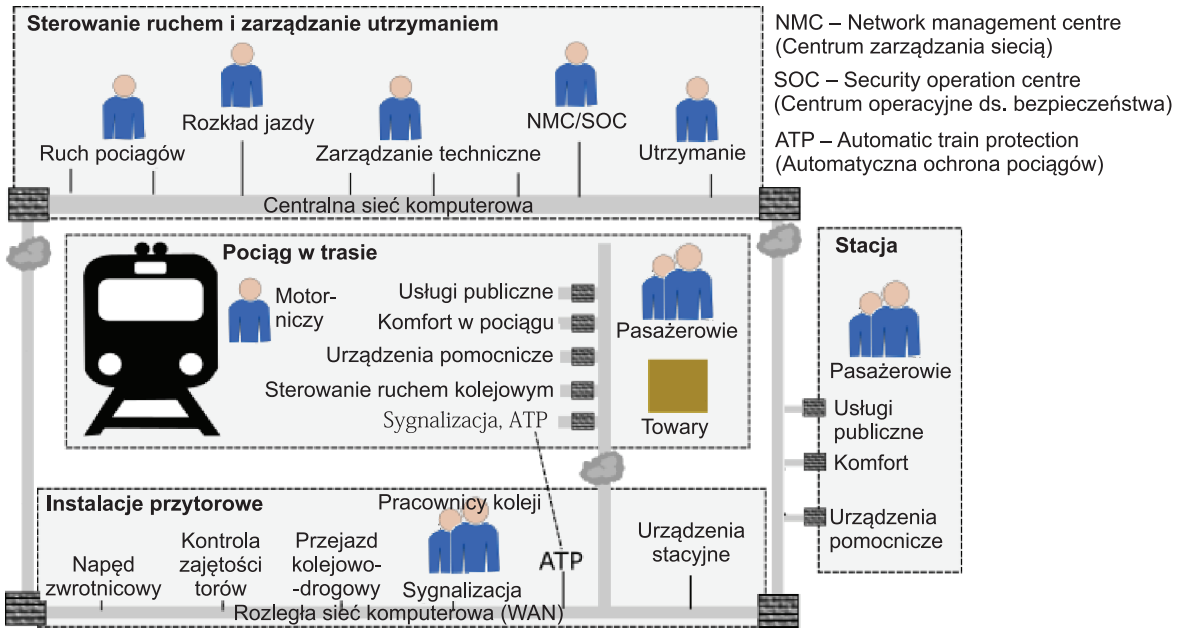
Norma dotycząca bezpieczeństwa cybernetycznego i systemów sterowania IEC 62443 dzieli sieć na trzy poziomy: korporacyjny, przemysłowy / korporacyjny i przemysłowy. Norma prTS 50701 zajmuje się tylko techniczną częścią sieci cybernetycznej. Część techniczna sieci jest podzielona na 4 obszary (rys. 1). Część sieci dotycząca eksploatacji, zarządzania i utrzymania odpowiada sieci przemysłowej / korporacyjnej (rys. 1, kolor żółty), natomiast parametrów sieci korporacyjnej (nadrzędnej), w normie nie uwzględniono.

Rysunek 1 przedstawia przemysłowe elementy sieci w części przemysłowej / korporacyjnej. Przemysłowe elementy kolei można podzielić na część podłączoną do kolei (rys. 1, kolor zielony) z systemami scentralizowanymi na poziomie infrastruktury oraz systemami instalowanymi wzdłuż torów. Następnie przemysłową sieć kolejową łączy się z eksploatowanymi pociągami (rys. 1, kolor niebieski).

Poszczególne segmenty sieci można następnie włączyć w kontekst cyberprzestrzennej zależności według rysunku 2 przedstawiającego obszar eksploatacji, zarządzania i utrzymania, bezpiecznie połączony z siecią WAN. Poszczególne elementy infrastruktury, takie jak stacje i systemy instalowane wzdłuż torów, są następnie podłączane do sieci WAN. Ponieważ zapewnienie bezpieczeństwa dużego obszaru łączności stanowi poważne wyzwanie, wszystkie połączenia muszą być odpowiednio zabezpieczone. Połączenie pociągu z siecią obsługującą system kolejowy jest utrzymane dzięki stacjonarnym elementom łączności instalowanym wzdłuż torów. Należy także zabezpieczyć dostęp na poziomie pociągów.



Rys. 1. Obszary cyberprzestrzeni kolejowej według prTS50701 [13]

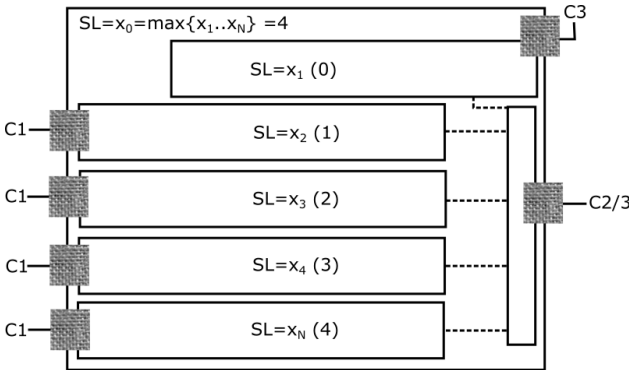


Rys. 2. Cyberprzestrzeń kolejowa według prTS50701 [13]

2.2. Segmentacja sieci kolejowej

Zasadniczo, z eksploatowanego pociągu można komunikować się wyłącznie bezprzewodowo i chociaż istnieją sposoby zapewnienia łączności bezprzewodowej, obszar ataku pozostaje zbyt duży. W związku z tym, bezpieczeństwo musi być zapewnione również na poziomie bramy sieciowej pociągu.

Rysunek 2 przedstawia 5 różnych segmentów sieci, które należy uwzględnić w sieci pociągu. Jedna z nich jest przeznaczona do usług publicznych, które znajdują się w otwartej przestrzeni internetowej, co determinuje konieczność zapewnienia bezpiecznego rozdzielania dostępu na poszczególne segmenty, aby niezabezpieczone lub mniej zabezpieczone segmenty sieci nie zagrażały krytycznym funkcjom w pociągu (rys. 3).

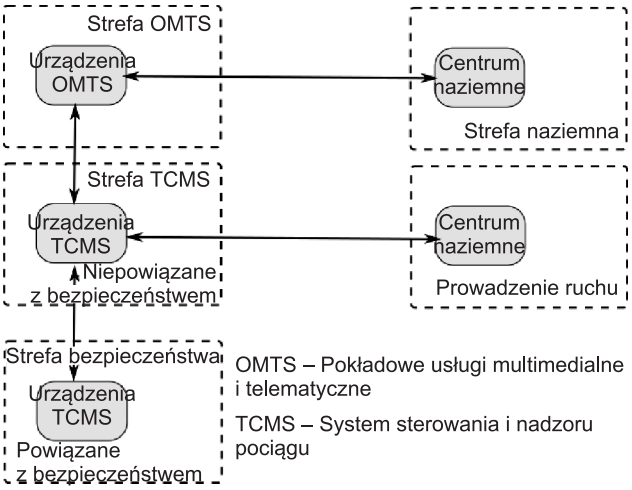


Rys. 3. Brama sieciowa w pociągu zgodnie z potrzebami sieci z rysunku 2 [13]

Segment sieciowy musi być tak zabezpieczony, aby zakłócenie w jednej części nie naruszało funkcji wykonywanych przez pozostałe segmenty. Aplikacja platformy MILS [8] jest jednym ze sposobów zarządzania tym wymogiem. System MILS jest opisany w rozdziale 4. Segmenty odpowiadają poszczególnym kanałom sieci przedstawionym na rysunku 3:

- usługi publiczne (nie są częścią wewnętrznej sieci w pociągu),
- komfort pociągu (obecnie jest on kontrolowany wewnętrznie w pociągu),
- systemy pomocnicze (pokładowe usługi multimedialne i telematyczne, określane jako OMTS),
- sterowanie i nadzór (system sterowania i nadzorowania pociągu w normalnych warunkach pracy określane jako TCMS),
- systemy ochrony pociągu (system sterowania i nadzorowania pociągu w warunkach awaryjnych).

Istnieje również segment sieci z urządzeniami oraz funkcjami o krytycznym znaczeniu dla bezpieczeństwa. Strefa ta nie może być jednak podłączona do sieci otwartej, a jedynie do zabezpieczonej strefy systemów ochrony pociągu. W celu uproszczenia wewnętrznej sieci w pociągu można również wykorzystać schemat z normy IEC 61375-2-6 [6] (rys. 4). Strefa OMTS odpowiada układom pomocniczym z rysunku 2, natomiast strefa TCMS obejmuje systemy sterowania pociągiem w warunkach normalnych i awaryjnych, z podziałem na strefę bezpieczeństwa, a także strefę nie związaną z bezpieczeństwem.



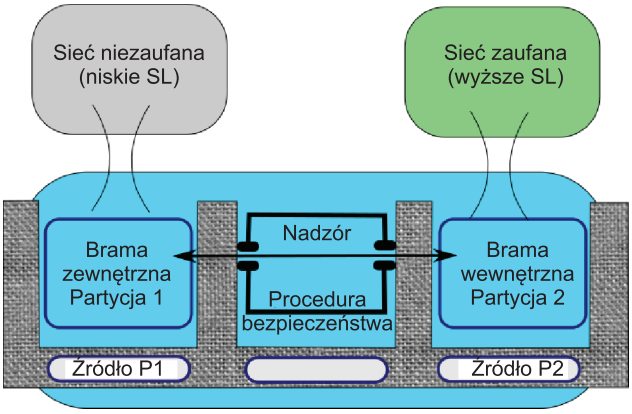
Rys. 4. Uproszczone strefy bezpieczeństwa pociągów według IEC 61375-2-6 [6]

3. Systemowo wielopoziomowe, bezpieczne i niezależne przetwarzanie danych (MILS)

Rozdział trzeci opisuje zasady działania, płaszczyzny działania i fizyczną realizację MILS (MILS *Community*) [8].

3.1. Zasady działania MILS

W rozdziale 2 opisano zastosowanie interfejsów pomiędzy podsystemami o różnych poziomach bezpieczeństwa w cyberprzestrzeni, a także przestrzeń zaufaną i niezaufaną. Wymiana danych pomiędzy tymi obszarami musi być zabezpieczona i konieczne jest stosowanie bram bezpieczeństwa, aby zapobiegać naruszaniu zaufanych podsystemów (rys. 5). Rodzaje barier ochronnych są opisane np. w normie IEC 62443 [7].



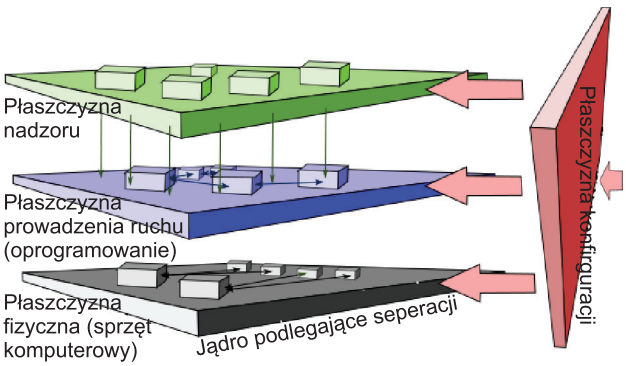
Rys. 5. Schematyczne przedstawienie interfejsu między sieciami zaufanymi i niezaufanymi przy stosowaniu zasad MILS [7]

Norma IEC 62443 opisuje elementarne bariery bezpieczeństwa i procedury dla systemów sterowania i systemów autonomicznych w cyberprzestrzeni, ale przede wszystkim zawiera zasady i wymogi, których stosowanie powinno być spełnione. Jedną z podstawowych filozofii normy IEC 62443 jest stosowanie zasady „obrony w głąb", co oznacza, że dla każdej pojedynczej bariery bezpieczeństwa należy liczyć się z możliwością awarii pozostałych barier. Według Harrisona [4], zasady zawarte w MILS spełniają wymogi strategii obrony w głąb w obszarze bezpieczeństwa wymiany danych pomiędzy zaufanymi i niezaufanymi obszarami cyberprzestrzeni.

Zasady MILS oznaczają tworzenie wielu bram sieciowych i procedur bezpieczeństwa, przez które musi przechodzić wymiana danych (rys. 3). Każda brama sieciowa i każda procedura zabezpieczeń ma swoje zasoby (m.in. procesor, dysk twardy, pamięć RAM, Ethernet). Z tego względu zakłócenie jednej bariery bezpieczeństwa nie zagrozi innym barierom.

3.2. Płaszczyzny działania MILS

Aplikacja MILS Approach zakłada, że ustawienie zabezpieczeń rozpoczyna się już na poziomie sprzętowym. Niezależne działanie poszczególnych bram sieciowych i procedur wymaga również przestrzegania ustawień bezpieczeństwa systemu na wszystkich płaszczyznach działania MILS (rys. 6). Należy jednak przestrzegać następujących zasad:



Rys. 6. Płaszczyzny implementacji MILS, płaszczyzna fizyczna (sprzęt), płaszczyzna działania (oprogramowanie), płaszczyzna monitorowania (procedury zabezpieczeń) i płaszczyzna konfiguracji (plik konfiguracyjny) [1]

1. System operacyjny nie może losowo przydzielać zasobów, jak w przypadku konwencjonalnych systemów operacyjnych. Musi on ściśle podążać za płaszczyzną konfiguracji – „systemami działającymi w czasie rzeczywistym z technologią hipernadzoru separacji jądra systemu" (na przykład PikeOS).
2. Płaszczyzna konfiguracyjna lub plik konfiguracyjny jest najsłabszym punktem systemu i dlatego musi być chroniony (ponieważ dotyczy wszystkich partycji).
3. Stabilność procedur bezpieczeństwa w płaszczyźnie monitorowania znacząco wpływa na zalety systemu MILS.

W płaszczyznach implementacji MILS czasami obecna jest także płaszczyzna adaptacji (rys. 6), która jest umieszczana po prawej stronie płaszczyzny konfiguracji, na którą wpływa. Płaszczyzna ta jest narzędziem do zarządzania aktualizacjami i usterkami, albo może być zautomatyzowana. Automatyczna reakcja platformy na bardziej złożone problemy, bez naruszania procedur bezpieczeństwa, jest nadal przedmiotem badań.

3.3. Fizyczna realizacja MILS

Znanych jest kilka sposobów wdrażania zasad MILS. Sposób stałej alokacji zasobów, jak połączenie Ethernet lub miejsce na dysku twardym jest oczywisty, jednak stała alokacja procesora jest bardziej skomplikowana.

Oczywiście możliwe jest posiadanie własnego procesora dla każdej bariery, jest to jednak bardzo niepraktyczne rozwiązanie i w praktyce MILS jest wdrażany na jednym procesorze. Procesor może być wielordzeniowy lub jednordzeniowy. Rozdział zasobów dla wielordzeniowego procesora logicznie sugeruje przypisanie każdego rdzenia do innej partycji. Według Rushby'ego [14], w procesorze jednordzeniowym lub gdy jest mniej rdzeni niż barier zabezpieczających, można wykonać „separacje jądra" i przypisać poszczególne partycje rdzeniowe do poszczególnych partycji interfejsu.

Do prawidłowego funkcjonowania całego systemu ważne są również poziomy bezpieczeństwa poszczególnych barier, ponieważ korzyści wynikające z MILS są znikome gdy bariery są słabe lub nieistotne. W połączeniu z barierami o wysokim poziomie bezpieczeństwa MILS zapewnia jednak wysoki, ogólny poziom bezpieczeństwa, który w przeciwnym razie byłby trudny lub niemożliwy do osiągnięcia.

Bariery powinny mieć także różne ustawienia. Zasada MILS umożliwia również łączenie technologii wielu różnych partycji pochodzących od różnych producentów, dzięki czemu żadna z nich nie ma „kluczy" do całego systemu. Następnie można zmierzyć i porównać bariery poszczególnych producentów, aby uzyskać informacje na temat ich zachowań. Należy przy tym zastrzec, że integrator systemów musi pamiętać, że złożoność systemu (liczba i różnorodność barier) zwiększa wymagania dotyczące działania systemu i mogą pojawić się nowe zagrożenia.

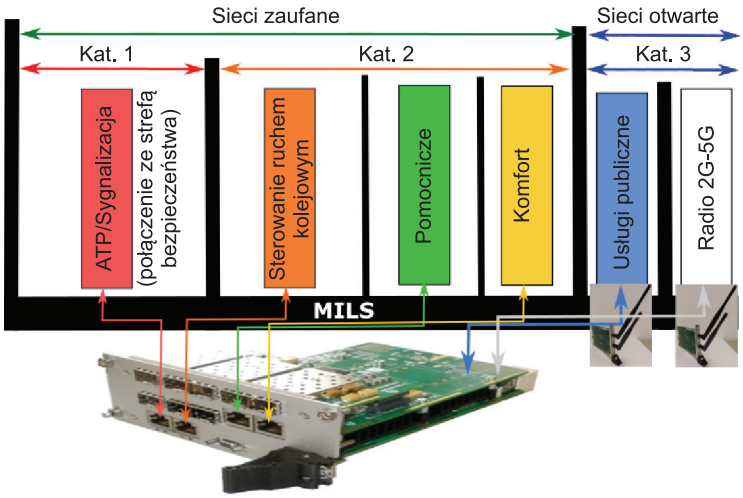
4. Projekt pilotażowy

W niniejszym rozdziale przedstawiono przykład wdrożenia projektu pilotażowego MILS na kolejach czeskich.

4.1. Cybernetyczna brama sieciowa pociągu

Cybernetyczną bramę sieciową pociągu można wykorzystać jako przykład platformy MILS w kontekście kolejowej sieci cybernetycznej, opisanej w rozdziale 2. Platforma MILS nadaje się również do segmentacji wewnętrznej sieci w pociągu, nie tylko na wejściu sieci łączności. Na rysunku 2, na wejściu do sieci łączności pociągu, pokazano 5 różnych stref o różnych funkcjach i wymaganiach bezpieczeństwa. Brama sieciowa może być zabezpieczona technicznie za pomocą zespołów łączności przedstawionej na rysunku 7.

Brama sieciowa pociągu (rys. 7) zawiera 2 nadajniki Wi-Fi: pierwszy do łączności ze stacjonarnymi zespołami łączności z urządzeniami zainstalowanymi wzdłuż linii (połączenie z centrum kontroli ruchu), drugi zaś do świadczenia usług pasażerskich. Pozostałe kanały telekomunikacyjne są realizowane za pomocą połączeń Ethernet. System operacyjny bramy sieciowej, PikeOS [11], jest hipernadzorcą zapewniającym stałą alokację zasobów do poszczególnych obszarów. Alokacja zasobów



Rys. 7. Brama sieciowa pociągu [11]

łączności (Ethernet, Wi-Fi) do partycji na rysunku 7 jest przykładem stałej alokacji. Innym przykładem jest alokacja miejsca na dysku twardym pamięci operacyjnej lub czasu procesora.

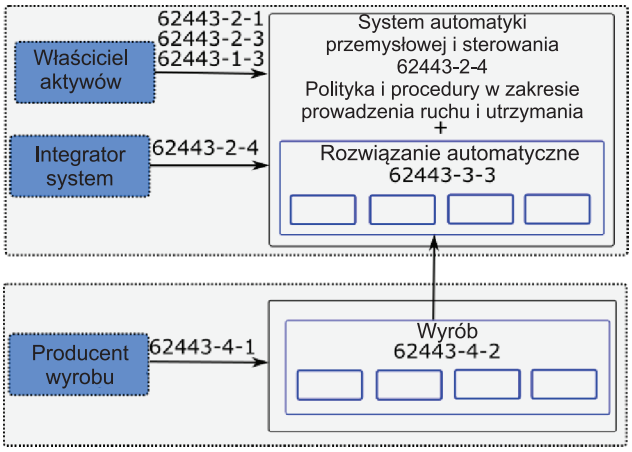
Brama sieciowa z rysunku 7 umożliwia transfer niektórych zasobów przydzielonych w trybie normalnym do mniej krytycznych partycji (usługi publiczne), do partycji o wyższym stopniu krytyczności (sterowanie lub ochrona pociągu) dla trybu awaryjnego w kontekście zdolności adaptacyjnych.

4.2. Integracja i adaptacja

W praktyce, przedstawiona koncepcja rozwiązania nie wystarcza do zlikwidowania problemów technologicznych, takich jak cyberataki. Niezbędny jest również dobór odpowiednich komponentów (sprzętu i oprogramowania), sposób ich integracji, certyfikacji, a w dynamicznym środowisku, takim jak cyberprzestrzeń, także procedura dostosowywania do nowych zagrożeń.

Dywersyfikacja dostawców i producentów poszczególnych elementów systemu może zwiększyć bezpieczeństwo, jak również złożoność systemu barier ochronnych. Na rysunku 8 pokazano trzy poziomy dostępu oraz odpowiedzialności, które dotyczą sterowania bramami sieciowymi:

- producenci poszczególnych elementów,
- integrator,
- operator / użytkownik.



Rys. 8. Trzy poziomy odpowiedzialności: producenta, integratora i operatora według różnych części normy IEC 62443 [7] dla różnych zastosowań

Wymienione trzy poziomy mają własne zasady (normy), które nimi zarządzają oraz organy, które nimi nadzorują.

Na potrzeby projektu pilotażowego zaprojektowano układ technologiczny MILS o nazwie „Composition-T" certMILS [1]. Układ T-Composition jest opisany w raporcie 8.1 projektu certMILS. Weryfikacja możliwości zastosowania MILS T-Composition w systemach kolejowych jest jednym z działań projektowych.

Następnym krokiem w projekcie CertMILS jest certyfikacja. Certyfikacja w odniesieniu do zdolności adaptacyjnych (lub zdolności adaptacji w odniesieniu do certyfikacji) jest przedmiotem osobnego artykułu. Producent, integrator i operator muszą przestrzegać różnych norm dotyczących działania w zależności od obszaru ich działania. Normy nie tylko nakładają na nich obowiązki, ale także stawiają wymagania dla poprzedniego segmentu przetwarzania i przekazywania danych (patrz rysunek 7).

Obszar cyberbezpieczeństwa jest objęty własnymi normami, jednak w artykule opisano głównie normę IEC 62443 [7]. Norma IEC 62443 nie jest prawnie wiążąca w Europie, ale zawiera wskazówki, jak postępować lub czego się spodziewać po poprzednich segmentach przetwarzania i przekazywania danych z punktu widzenia poszczególnych części technologicznych, a także z punktu widzenia integracji całego systemu. Mimo tego, Grupa robocza CENELEC pracuje np. nad normą dotyczącą cyberbezpieczeństwa systemów kolejowych, prTS 50701 [13], opartą na normie IEC 62443.

Bezpieczeństwo cybernetyczne poszczególnych komponentów może być również znormalizowane w normie IEC 15408 [5] za pomocą wspólnych kryteriów. Obie wymienione normy IEC 62443 i IEC 15408 są uwzględnione w europejskich projektach certMILS.

Możliwość ponownej konfiguracji opartej na wymaganiach eksploatacyjnych i możliwości adaptacji jest jedną z najważniejszych cech systemu, w praktyce, wdrożenie takiego rozwiązania wymaga jednak znacznych środków finansowych. Konieczne jest przygotowanie i zastosowanie procesów, które umożliwią łatwą weryfikację i wdrażanie nowych konfiguracji. Rozwiązaniem może być konfiguracja technologiczna MILS o nazwie „I-composition", dostarczana w wersji 8.1 z projektu certMILS. Konfiguracja I-composition jest certyfikowaną podstawą systemu i może być rozszerzana o kolejne dodatki, aż do osiągnięcia pożądanej konfiguracji T-composition.

Zdolność systemu do adaptacji ma kilka poziomów: system w pełni samoadaptacyjny, system częściowo samoadaptacyjny i system adaptowalny manualnie.

1. System, który potrafi ocenić sytuację, określić najbardziej optymalną konfigurację, zapewnić bezpieczne wyłączenie i uzyskać certyfikację bez ingerencji człowieka, stoi na najwyższym poziomie samokonfiguracji dynamicznej. Trudność w tworzeniu w pełni samoadaptacyjnego systemu polega na zachowaniu niezależności poszczególnych barier bezpieczeństwa i certyfikacji w czasie rzeczywistym.
2. Częściowo samoadaptacyjny system jest łatwiejszy do skonfigurowania. Ma on kilka „dopuszczalnych

stanów" rozdzielania zasobów. Wszystkie dopuszczalne stany są wcześniej weryfikowane i certyfikowane. System może przełączać się tylko pomiędzy dopuszczalnymi stanami. Należy przygotować bezpieczną procedurę przełączania.
3. System adaptacji manualnej jest najmniej progresywny z opisanych sposobów adaptacji, ale wiąże się również z mniejszym ryzykiem, związanym z procedurami bez nadzoru. System adaptacji manualnej wykorzystuje konfigurację I-composition. Zweryfikowana i certyfikowana jednostka I-compositon jest skrzynką z miejscem na karty. Kartę można łatwo wyjąć, zmodyfikować i ponownie włożyć. Skrzynka i karty tworzą razem jednostkę T-composition.

5. Wnioski

Według A. Torunia [15], krytyczność elementów infrastruktury, jak również podatność na zagrożenia wzrasta wraz z rosnącym uzależnieniem funkcjonowania infrastruktury od systemów tworzonych przez ludzi. Infrastruktura cybernetyczna jest jednym z takich obszarów, gdzie dynamicznie pojawiają się nowe, szkodliwe zjawiska. Awaria bezpieczeństwa spowodowana przez nieznanego sprawcę, producenta sprzętu lub twórcę oprogramowania cieszy się dziś sporym zainteresowaniem mediów, choć zjawiska te występują już od dłuższego czasu.

Ochrona przetwarzania oraz wymiany danych wyłącznie na poziomie danych za pomocą oprogramowania nie jest wystarczająca. Konieczne są również środki sprzętowe na poziomie bezpieczeństwa cybernetycznego. Systemy cyberfizyczne CPS są szczególnie narażone na cyberataki, ponieważ są związane ze światem fizycznym i oddziaływaniem fizycznym.

Wzrost krytyczności infrastruktury i pojawienie się nowych, szkodliwych zjawisk cybernetycznych wymaga zastosowania zaawansowanych procedur bezpieczeństwa. Koncepcja MILS umożliwia skuteczne osiągnięcie wysokiego ogólnego poziomu bezpieczeństwa. Sposób certyfikacji i adaptacji musi być przygotowany w środowisku dynamicznym, jakim jest cyberprzestrzeń.

Literatura

1. certMILS: Compositional security certification for medium- to high-assurance COTS-based systems in environments with emerging threats [Kompozytowa certyfikacja bezpieczeństwa dla średnio- i wysokowydajnych systemów opartych na COTS w środowiskach, w których występują zagrożenia], EU, Horizon 2020, nr 731456, 2017.
2. EN 50126-1: Railway applications – The specification and demonstration of Reliability, Availability, Maintainability and Safety (RAMS) [Zastosowania kolejowe – Specyfikowanie i wykazywanie niezawodności, dostępności, podatności utrzymaniowej i bezpieczeństwa (RAMS)]. CENELEC, Brussels, 2017.
3. Green Paper on a European Programme for Critical Infrastructure Protection [Zielona księga w sprawie europejskiego programu ochrony infrastruktury krytycznej]. EU COM(2005) 576 final, Brussels, 2005.
4. Harrison W.S.: *The MILS Architecture for a Secure Global Information Grid* [Architektura MILS dla bezpiecznej globalnej sieci informacyjnej], The CrossTalk Journal of Defense Software Engineering, 2005.
5. IEC 15408: Common Criteria for Information Technology Security Evaluation [Wspólne kryteria oceny bezpieczeństwa technologii informatycznych]. ISO i IEC, 1999, WWW https://commoncriteriaportal.org/.
6. IEC 61375-2-6: Electronic railway equipment – Train communication network: On-board to ground communication [Elektroniczne urządzenia kolejowe – Sieć łączności z pociągiem: Łączność pomiędzy instalacjami pokładowymi i naziemnymi], International Electrotechnical Commission, 2018.
7. IEC 62443: *Security for industrial automation and control systems* [Bezpieczeństwo dla automatyki przemysłowej i systemów sterowania], *International Electrotechnical Commission / International Society of Automation* [Międzynarodowa Komisja Elektrotechniczna/Międzynarodowe Stowarzyszenie ds. Automatyki] IEC i ISA, 2019.
8. MILS Community [Społeczność MILS], 2019, WWW http://mils.community.
9. Moteff J., Copeland C., Fischer J.: *Critical Infrastructures: What Makes an Infrastructures Critical*? [Infrastruktura krytyczna: Co sprawia, że infrastruktura jest krytyczna?], CRS Web, Report for Congress, Order Code RL31556, 2003.
10. Peerenboom J.: *Infrastructure Interdependencies: Overview of Concepts and Terminology* [Współzależności infrastrukturalne: przegląd pojęć i terminologii], Argonne National Laboratory, National Science Foundation Workshop, Argonne, 2001.
11. PikeOS Certified Hypervisor, SYSGO, 2019, WWW https://www.sysgo.com/products/pikeos-hypervisor.
12. Procházkova D.: *Challenges connected with critical infrastructure safety* [Wyzwania związane z bezpieczeństwem infrastruktury krytycznej], Lambert Academic Publishing ISBN: 978-3-659-54930-4. s. 218, 2014.
13. prTS 50701: Railway applications – Cybersecurity [Zastosowania kolejowe – Cyberbezpieczeństwo], wersja robocza D6E4, CENELEC, 2019.

14. Rushby J.:*The Design and Verification of Secure Systems, Eighth ACM Symposium on Operating System Principles* [Projektowanie i weryfikacja systemów bezpiecznych, ósme sympozjum ACM na temat zasad systemu operacyjnego, pp. 12–21, Asilomar (ACM Operating Systems Review, Vol. 15, No. 5), 1981.
15. Toruń A. et.al.: *Challenges for Air Transport Providers in Czech Republic and Poland* [Wyzwania dla przewoźników lotniczych w Czechach i Polsce], Journal of Advanced Transportation, nr. 6374592, 2018.

Podziękowanie

Praca ta jest częścią projektu certMILS, finansowanego przez unijny program ramowy w zakresie badań naukowych oraz innowacji „Horyzont 2020" na podstawie umowy nr 731456 o dofinansowanie.