SEGMENTACE ŘÍDÍCÍCH SYSTÉMŮ VLAKU

SEGMENTATION OF TRAIN CONTROL SYSTEMS

Jan Procházka[1,2], Petr Novobilský[2], Dana Procházková[1]

[1]ČVUT v Praze, Fakulta strojní, Technická 4, 16607, Praha 6.
[2]Q-media s.r.o., Počernická 272/96, 10800 Praha 10, Czech Republic, jpr@qma.cz

Abstrakt: S rozvojem technologií roste počet funkcí a procesů, jež jsou řízeny digitálně, popřípadě ovládané na dálku. Jednotlivé procesy a funkce kladou různé požadavky na bezpečnost, mohou být řízeny různými osobami (fyzickými i právnickými) a mají různé cíle. V komplexním řídícím systému je nutné zajistit, aby selhání v jedné oblasti nenarušilo celý řídící systém. Segmenty sítě sloužící pro různé účely, rozdílným osobám či s odlišnou mírou kritičnosti tak potřebují fungovat nezávisle na sobě. Respektive míra jejich interakce musí být konfigurovatelná a vynutitelná.

V oblastech řízení bezpečnosti, kde byly takovéto požadavky povinné již v minulosti, se velmi osvědčil přístup vícero nezávislých úrovní bezpečnosti MILS (multiple independent level of security). V rámci platformy MILS je možné, za využití adekvátního hypervisoru, vytvořit nezávislé oddíly v rámci jedné výpočetní jednotky. Využitím právě MILS platformy pro zajištění kybernetické bezpečnosti vlaku se zabývá tento článek.

Klíčová slova: MILS; kyber-fyzický systém; železnice; vlak; bezpečnost; bezpečí.

Abstract: The number of functions and processes that are digitally controlled or remotely controlled is increasing, as technologies developed. Individual processes and functions have different security requirements, can be managed by different persons (natural or juridical) and have different goals. It is necessary to ensure that failure in one area does not disrupt the entire system, in a complex control system. Network segments serving different purposes, different people or with different criticality rate need to work independently of each other. Respectively, their level of interaction must be configurable and enforceable.

The approach of multiple independent levels of security (MILS) has proven to be very useful, in the areas of safety management where such requirements of network segmentation have been mandatory. It is possible to use an adequate hypervisor to create independent partitions within a single computing unit within the MILS platform. This article deals with the use of the MILS platform to ensure the train's cybersecurity.

Key words: MILS; cyber-physical system; railway; train; safety; security.

1. Úvod

Vlak je složitý systém. Zejména v čase, kdy je v pohybu. Vedle pevných prvků, jako jsou kola, dveře, okna nebo sedačky se skládá i z dalších částí. Při provozu vlaku musíme počítat s cestujícími, kteří mají v dnešní době větší nároky na komunikační služby během cesty. Pro posádku a cestující pak musíme zajistit jistou úroveň komfortu, světlo, teplo nebo toalety. Vlak obsahuje podsystémy, které ovládají a kontrolují správnou a bezpečnou funkci jeho částí, jako

jsou například dveře. Máme zde řídící systémy pro strojvedoucího. Další systémy vlaku pak slouží jako podpora pro centrální řídící systémy železnice, se kterými vlak komunikuje. V neposlední řadě pak musí řídící systém vlaku obsahovat funkce a opatření pro zvládání nouzových a kritických situací.

Řada těchto systémů byla v minulosti, nebo ještě je ovládána z vlaku samotného, manuálně, nebo semi-automaticky. Při původním nastavení celý systém závisel na dohledu posádky nad veškerými jeho částmi a vzhledem k prostorové distribuci na ni kladl vysoké požadavky. Postupně se ale řada funkcí převádí na automatizované systémy s dohledem v kabině strojvedoucího, nebo na pozemní centrále. Lidský faktor sice nadále hraje roli, ale při správném nastavení systémů a školení na něj nejsou kladené takové požadavky.

Výsledkem je vznik takzvaného kyber-fyzického systému (*dále jen* CPS). CPS je spojeno s rozhraním mezi fyzickým a kybernetickým prostorem a vznikem nových rizik v oblasti kyberprostoru a na rozhraní obou prostorů. Je proto nutné zavádět nové principy a opatření pro jejich pokrytí. V rámci bezpečnostních systémů CPS jsou pak běžně převáděné ověřené principy a přístupy z fyzického prostoru do prostoru kybernetického. Jedním takovým přístupem je uzavření a segmentace jednotlivých částí prostoru podle potřeby jeho zabezpečení a rozdílného přístupu. Poté co se v kapitole 2 věnujeme problematice kybernetické sítě železnice, se v kapitole 3 zabýváme právě těmito opatřeními (segmentace kybernetického prostoru). Kapitola 4 je pak věnována popisu a aplikaci konkrétního nástroje pro segmentaci řídících systémů vlaku.

2. Kybernetická síť vlaku

Kapitola je věnována vnitřní kybernetické síti vlaku. Pro její lepší chápání je ale nutné nejprve začít u celkové kybernetické sítě železniční infrastruktury. Nejprve si představíme zásady celkové sítě. Potom se budeme věnovat rozdělení vnitřní sítě vlaku na zóny.

2.1. Kybernetická síť železnice

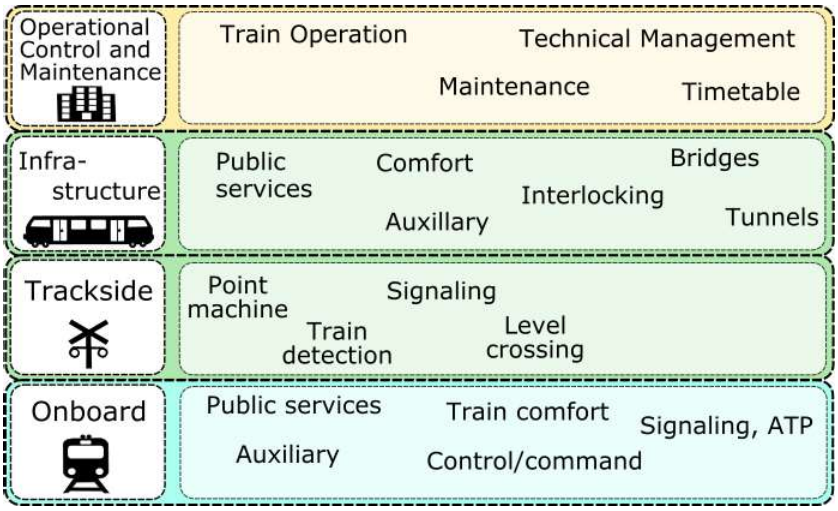
V rámci popisu kybernetické sítě železnice budeme vycházet z předběžné technické specifikace prTS50701 [1]. Uvedený dokument je zatím ve stádiu připomínek a schvalování, nese však již informace, ze kterých se dá vycházet. Hlavním cílem specifikace prTS50701 [1] je implementovat požadavky na komunikační systémy normy IEC 62443 [2] do prostředí železnice.

Norma o bezpečnosti kybernetických a řídících systémů IEC 62443 [2] člení síť na tři části: podnikovou; podnikovo-průmyslovou; a průmyslovou. Specifikace prTS50701 [1] se pak zabývá již jen technickou částí kybernetické sítě. Technickou část sítě dělí na 4 oblasti, obrázek 1. Část sítě spojená s provozem, řízením a údržbou odpovídá podnikově-průmyslové síti, obrázek 1 – žlutá část. Nad ní je podniková síť, jejíž parametry norma neřeší.

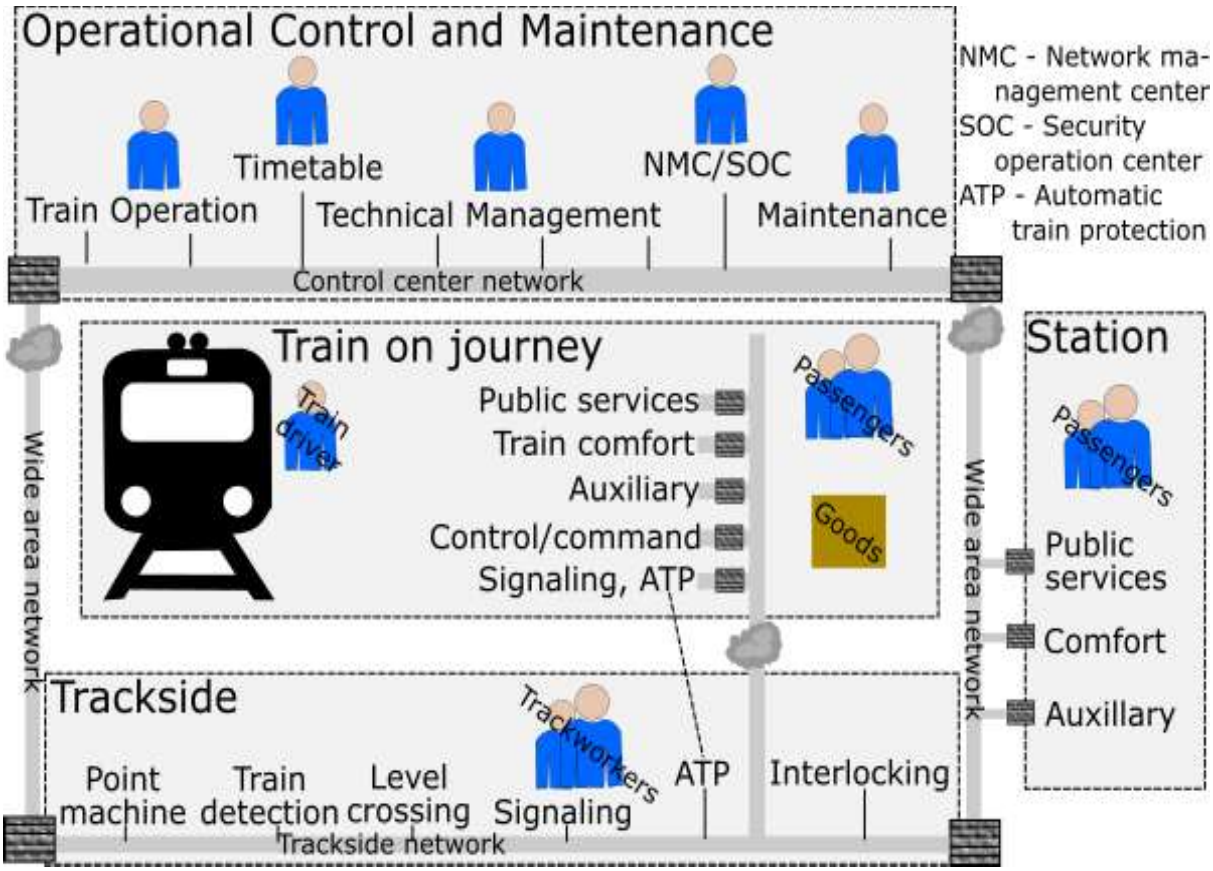
Pod podnikově-průmyslovou sítí jsou pak průmyslové části. Průmyslové části železnice můžeme rozdělit na část spojenou s železničními cestami, obrázek 1 – zelená část. U železničních cest máme systémy na úrovni celková infrastruktury a systémy rozmístěné podél trati. Další průmyslová síť železnice je pak spojená právě s vlakem, konkrétně s pohybujícím se vlakem, obrázek 1 – spodní zelenomodrá část.

Jednotlivé segmenty sítě si pak můžeme vynést i v rámci kyber-prostorové závislosti, obrázek 2. Na obrázku 2 vidíme oblast provozu, řízení a údržby, která je skrze zabezpečené

přístupy propojená s rozsáhlým komunikačním prostorem. Na rozsáhlý komunikační prostor jsou pak napojeny jednotlivé prvky infrastruktury, například stanice, a systémy podél trati. Jelikož zabezpečení rozsáhlého komunikačního prostoru je náročné, musí být zabezpečena všechna připojení.



Obr. 1. Zóny zájmů kybernetického prostoru železnice, prTS50701 [1].

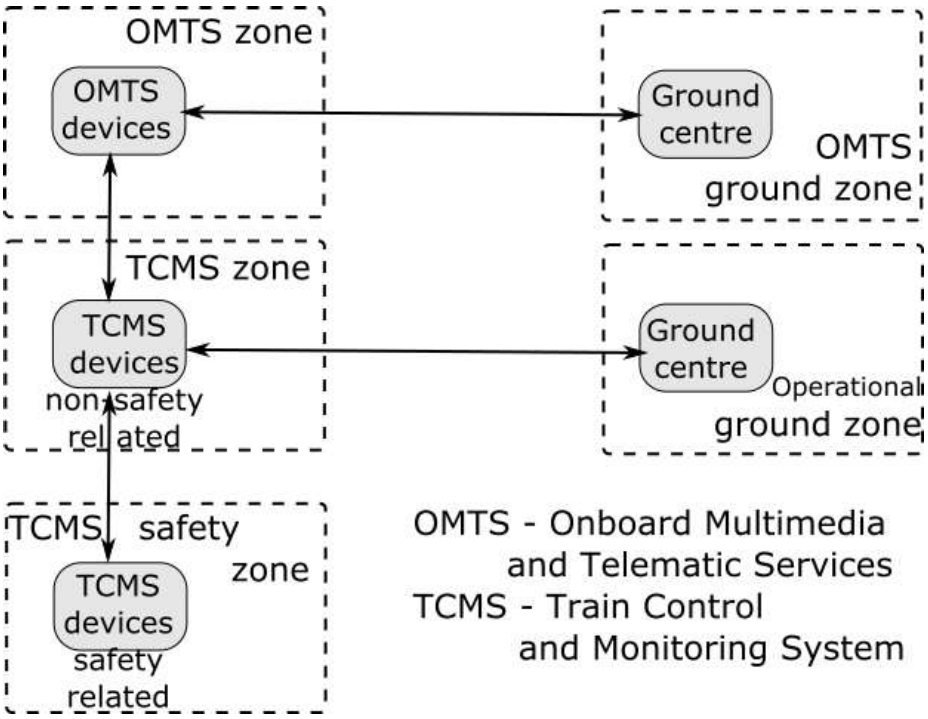


Obr. 2. Kybernetický prostor železnice prTS50701 [1].

Vzhledem k rozsáhlosti železniční infrastruktury, není vhodná komunikace přímo mezi vlakem a řídícím centrem. Komunikace probíhá skrze pozemní komunikační brány, které jsou umístěné podél železniční tratě. Komunikace mezi pozemní komunikační bránou a komunikační bránou vlaku je pak vedena vzduchem. S tím jsou spojené zvýšené požadavky na zabezpečení komunikační brány vlaku.

2.2. Segmentace sítě vlaku

Vnitřní síť vlaku můžeme v zásadě rozdělit na tři kategorie. Tyto tří kategorie odpovídají kategoriím sítí běžně používanými například v IEC 62443 [2]. Kybernetická síť v rámci CPS, kterým je železnice, je spojená s prvky a funkcemi relevantními pro bezpečí vlaku. Tato síť nese požadavky sítě kategorie 1. Ostatní funkce vlaku pak mohou být umístěny do sítě kategorie 2. Komunikační služby pro zákazníky, jako připojení k internetu skrze wifi pak odpovídá kategorii 3. Vyčlenění sítě relevantní pro bezpečí bylo již v předchozích normách, například ve standardu IEC 61375-2-6 [3]. Uvedenému standardu odpovídá schéma na obrázku 3.



Obr. 3. Zjednodušené bezpečnostní zóny vlaku, IEC 61375-2-6 [3].

S nárůstem funkcí, které jsou ve vlaku řízeny digitálně, roste počet potenciálně izolovaných segmentů, které kybernetická sít vlaku může obsahovat. Na obrázku 2 vidíme celkem 5 různých vnitřních částí sítě vlaku.

1. Veřejné služby (nejsou součástí vnitřní sítě vlaku).
2. Komfort vlaku (u našich vlaků bývá řízen lokálně).
3. Pomocné systémy (Palubní multimediální a telematické služby).
4. Řízení a kontrola (funkce vlaku pro běžný provoz).

5. Systémy pro ochranu vlaku.

Jelikož jednotlivé části sítě jsou spojené s různými požadavky na zabezpečení a sdílejí přitom společnou komunikační bránu, je potřeba zajisti důslednou ochranu hranic jednotlivých zón. Segmentace komunikace musí být zabezpečená tak, aby narušení jedné části, neohrozilo funkce jiných. Jednou z cest je aplikace platformy MILS [4], která bude rozebrána ve čtvrté kapitole.

3. Segmentace kybernetické sítě

Rozdělení prostoru na oblasti s různou mírou zabezpečení, přístupem a způsobem řízení je běžný princip užívaný v zařízeních s velkými požadavky na bezpečnost jako jsou jaderné elektrárny, chemické továrny, ale může jít i o důležité kanceláře. Prostor může být členěn ve větším měřítku na jednotlivé areály a pracovní oddělení a v menším měřítku na pracovní jednotky přidělené jednotlivým osobám, například kanceláře.

Standard IEC 62443 [2] převádí řadu ověřených přístupů řízení bezpečnosti z oblasti fyzického prostoru do prostoru kybernetického. Jmenovat můžeme například strategii obrany do hloubky (defence in depth) v rámci bezpečnostních opatření, zabezpečenou, popřípadě bezpečnou architekturu, nebo právě segmentace kybernetického prostoru do zón a nastavení pravidel komunikace mezi nimi.

Problematiku můžeme tedy rozdělit na vytvoření jednotlivých zón a na zajištění nakonfigurovaných pravidel komunikace mezi nimi. Zóny pak mohou obsahovat více výpočetních jednotek, kdy výpočetní jednotky mezi sebou mohou volně komunikovat. Komunikace s dalšími zónami, či vnějším prostorem ale probíhá skrze „firewally“. Konfigurace zón a komunikace mezi nimi je tak zajištěna systémem těchto firewallů.

Uvedené řešení není ovšem použitelné pro systém s omezeným prostorem, jako je vlak. V případě vlaku v provozu, podobně jako v případě jiných dopravních prostředků, můžeme využít pouze omezené množství výpočetních jednotek. Zón nebo dokonce procesů, které potřebujeme od sebe oddělit však může být více než jednotek. Segmentaci a dodržování pravidel nastavené komunikace však musíme zajistit na jedné výpočetní jednotce.

Vytváření oddělení (Partitioning) je postup vytvoření segmentované sítě, kde jednotlivé oddíly mají přidělené vlastní zdroje a podporují vlastní procesy. V některých odvětví lidského systému je tento přístup povinný a má nastavená standardizovaná pravidla, například ARINC 653 [5] pro leteckou dopravu. V případě specifikace prTS 50701 [1] se zatím počítá pouze s doporučením užívání „partitioningu“. Situace se ale v budoucnosti může změnit.

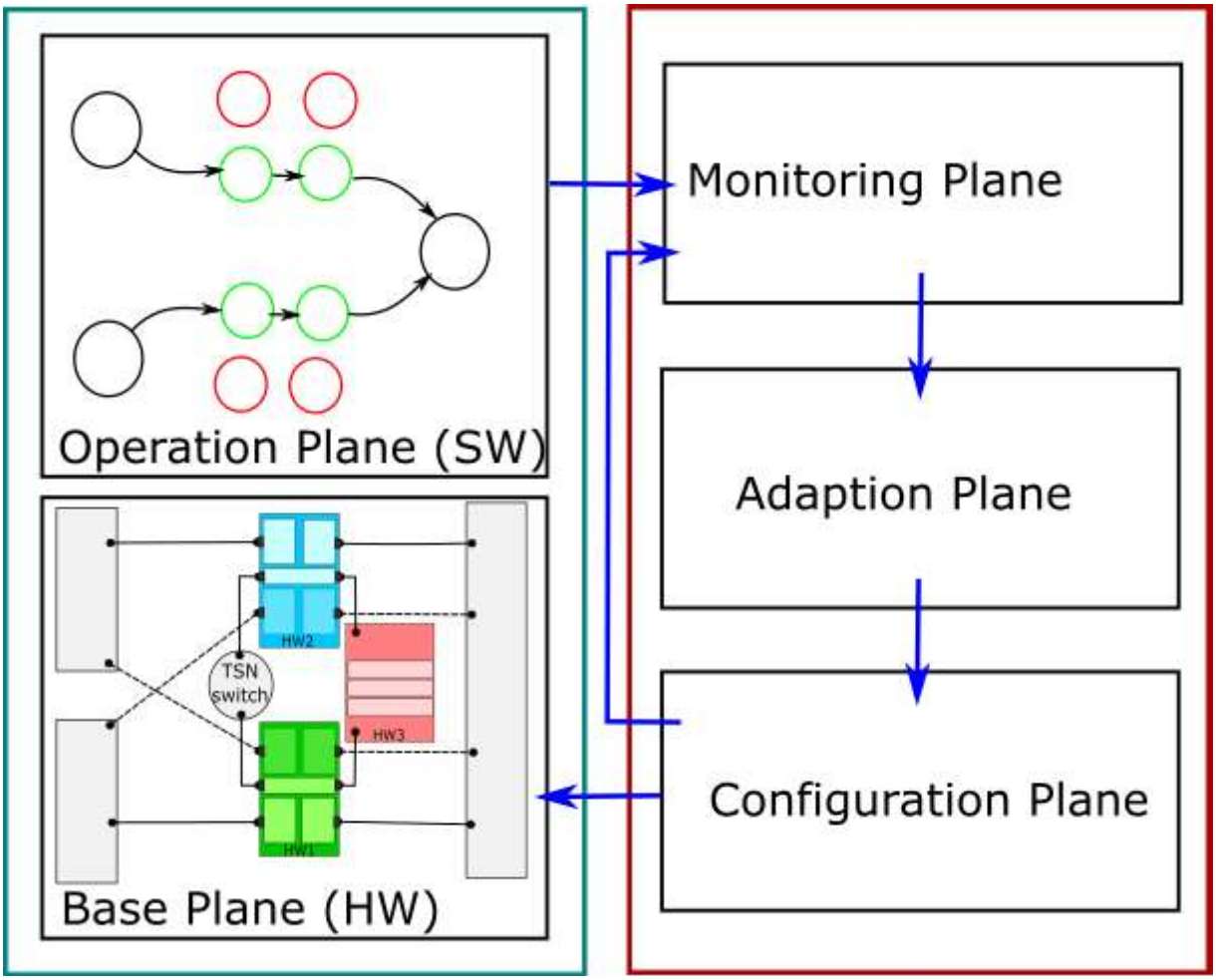
4. MILS platforma

Platforma vícero nezávislých úrovní bezpečnosti MILS (multiple independent level of security) vznikla v rámci koncepce kybernetické bezpečnosti americké armády. Nahradila tak předchozí přístupy, které v rámci aplikace obrany do hloubky vyžadovaly vícero bezpečnostních opatření, ale opomíjely riziko, že selhání jedné bariery může vést k překonání ostatních.

V dnešní době je platforma MILS požívána v nejrůznějších oblastech lidského systému s vysokou kritičností rizik v kyberprostoru. Vnitřní prostředí výpočetní jednotky je rozděleno do nezávislých oddílů, které mohou sloužit pro zajištění bezpečnosti, ale i pro poskytování dalších funkcí. Platforma MILS tak může souběžně podporovat kritické funkce s vysokými

požadavky na zabezpečení a služby v otevřeném prostoru pro cestující s širokým vektorem útoku. Ztráta důvěryhodnosti otevřené části přitom nijak neohrožuje ostatní oddělení.

Aby zmíněná nezávislost jednotlivých oddělení byla možná, musí být zajištěna již na úrovni hardwaru. Celý systém platformy MILS pak stojí na specializovaném operačním systému, hypervisoru, který zajistí rozdělení hardwarových zdrojů a softwarových procesů [6]. Platformu MILS, která stojí na hypervisoru, si můžeme promítnout do několika rovin, obrázek 5. Nalevo máme roviny, zajišťující funkce, požadované po výpočetní jednotce, a to: Základní rovina (hardware); a Operační rovina (software). Napravo jsou roviny zajišťující řízení platformy. Jde především o: Monitorovací rovinu; a Konfigurační rovinu. Konfigurační rovina je kritickou součástí platformy MILS, z důvodu přístupu ke všem ostatním rovinám, a její zabezpečení je tak velmi důležité.



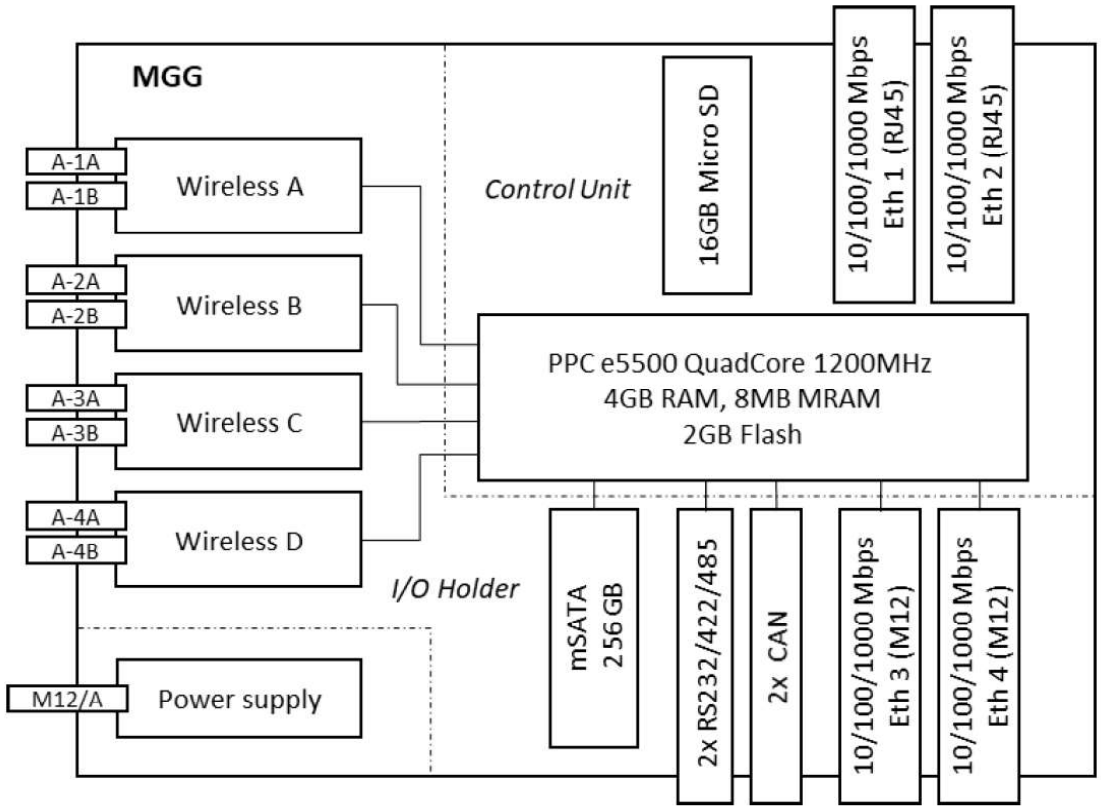
Obr. 5. Platforma MILS, funkční roviny nalevo a řídící roviny napravo.

Vedle výše zmíněných rovin máme na obrázku 5 i rovinu Adaptační. MILS platforma může fungovat i bez implementace adaptační roviny ve statickém režimu. Pro efektivní využití zdrojů a rychlou odezvu na změny v kyberprostoru je implementace Adaptační roviny vhodná. Při jejím nastavení je pak nutné ohlídat, aby nedošlo ke kompromitaci bezpečnosti platformy. Dynamičnost adaptace pak není odvislá pouze od technického zajištění změny konfigurace systému. Důležitý je i proces ověření bezpečnosti „nové“ konfigurace systému.

Možnostmi rychlé verifikace a certifikace platformy MILS se zabývá Evropský projekt certMILS [7]. V rámci projektu certMILS se analyzují možnosti přírůstkové certifikace. Základní část systému zůstane nezměněna (hypervisor a některé oddíly). Nad základní částí jsou ale dodávány, či pozměňovány další oddíly. Verifikace je pak opakována jen pro pozměněnou část. Předmětný postup však vyžaduje nastavení pravidel adaptace, která nenaruší bezpečnost základní kompozice. Blíže je tato problematika rozebrána v článcích [8-10].

Jako příklad využití platformy MILS ve vztahu k železniční kybernetické síty, popsané v kapitole 2, si můžeme vzít kybernetickou bránu vlaku. Platforma MILS je vhodná i pro segmentaci vnitřní sítě vlaku, ne jenom na vstupu komunikace. Evropský projekt ADMORPH [11] připravuje testování využití platformy MILS v rámci železnice s důrazem na odezvu na nežádoucí události již v rámci komunikační brány vlaku. Aby byla mobilní komunikační brána vlaku schopna reagovat na problémy, které mohou během provozu nastat, musí být na to připravena dopředu. Na obrázku 6 vidíme schéma navrhované brány.

Komunikační brána vlaku na obrázku 6 podporuje 2 wifi komunikační kanály, první pro komunikaci se stacionárními komunikačními jednotkami podél trati (spojení s operačním střediskem) a druhý pro zajištění služeb pro pasažéry. Pro obě dvě komunikace jsou vyhrazena dvě bezdrátová rozhraní pro případné selhání. Zbylé komunikační kanály jsou realizovány skrze ethernetová připojení uvnitř vlaku. Operační systém komunikační brány je PikeOS [12]. PikeOS jako hypervisor zajišťuje pevné rozdělení zdrojů jednotlivým oddělením. Jde především přidělení komunikačních zdrojů (ethernet, wifi) jednotlivým oddělením. Napevno jsou ale přiděleny i místo v pevné paměti, operační paměť, nebo výpočetní výkon procesoru.



Obr. 6. Komunikační brána vlaku.

V rámci adaptibility je pak možné převést některé zdroje přidělené v normálním režimu méně kritickým oddělením (veřejné služby) pro nouzový režim oddělením s vyšší kritičností (kontrola a řízení nebo ochrana vlaku).

5. Závěr

S rozvojem technologie se do kybernetického prostoru vlaku přesouvá více a více funkcí, které byly dříve zajišťovány čistě v prostoru fyzickém. Funkce a procesy uvnitř vlakové kybernetické sítě pak slouží nejrůznějším účelům, mohou být řízeny rozdílnými osobami a mají různou kritičnost. Řešení takové situace pak vyžaduje segmentaci vnitřního kyberprostoru vlaku podle sledovaných parametrů, aby případná selhání a narušení bezpečnosti nevedla ke kritickým následkům.

Odpovědí na uvedené potřeby je platforma MILS, která se dá snadno implementovat i v podmínkách pohybujícího se dopravního prostředku. Zajištění nezávislosti jednotlivých oddělení platformy MILS vyžaduje implementaci bezpečnostní architektury ve všech rovinách technologie, ať už se jedná o roviny řídící, nebo funkční. V případě komunikační brány, která je sledována v článku, je použit operační systém PikeOS jako hypervisor. Zařízení je ve fázi verifikace a certifikace v rámci evropského projektu certMILS a připravuje se jeho testování v podmínka české železnice v rámci projektu ADMORPH.

Poděkování: Článek vznikl díky podpoře Evropského projektu certMILS ID 731456 a Evropského projektu ADMORPH ID 871259 v rámci programu Horizont 2020. Článek byl zpracován částečně i v rámci projektu PRKODI, financovaného TAČR v rámci programu „DOPRAVA 2020+“, s identifikačním kódem CK01000095.

Literatura

[1] CENELEC. *prTS 50701. Railway Applications – Cybersecurity*, draft version D8E4, CENELEC. Brussels: EU 2020.

[2] IEC. *IEC 62443. (2019). Security for Industrial Automation and Control Systems*. International Electrotechnical Commission / International Society of Automation. IEC and ISA. Brussels: EU 2019.

[3] EU. *IEC 61375-2-6. Electronic Railway Equipment - Train Communication Network: On-board to Ground Communication*. International Electrotechnical Commission. Brussels: EU 2018.

[4] MILS Community. MILS Community 2019. http://mils.community

[5] EU. *ARINC 653.* (2012). *Avionics Application Software Standard Interface*, Airlines Electronic Engineering Committee. Brussels: EU 2012.

[6] HARRISON W. S. *The MILS Architecture for a Secure Global Information Grid*. The CrossTalk. *Journal of Defense Software Engineering* 2005.

[7] EU. *certMILS. Compositional Security Certification for Medium- to High-Assurance COTS-Based Systems in Environments with Emerging Threats*. Horizon 2020, no 731456. Brussels: EU 2020.

[8] PROCHAZKA J., NOVOBILSKY P., PROCHAZKOVA D. Cyber Security of Urban Guided Transport Management according MILS Principles. In: *Proceedings of the 29th European Safety and Reliability Conference (ESREL).* ISBN 978-981-11-2724-3. Singapore: ESRA 2019,

Research Publishing 2019, pp. 4107-4413, doi:10.3850/978-981-11-2724-3_0220-cd, e:enquiries@rpsonline.com.sg,

[9] SCHULZ T., GRIEST C., GOLATOWSKI F., TIMMERMANN D. Strategy for Security Certification of High Assurance Industrial Automation and Control Systems. In: *I EEE 13th SIES,* 2018, ISSN 2150-3117, DOI: 10.1109/SIES.2018.8442081.

[10] SCHULZ T., GOLATOWSKI F., TIMMERMANN D. *Integration Approach for Communications-based Train Control Applications in a High Assurance Security Architecture.* Springer Nature Switzerland AG 2019. https://doi.org/10.1007/978-3-030-18744-6_18

[11] EU. *ADMORPH. Towards Adaptively Morphing Embedded Systems*. EU, Horizon 2020, no 871259. Brussels: EU 2020.

[12] EU. PikeOS. *PikeOS® Certified Hypervisor*, SYSGO, 2019. Brussels: EU 2019. https://www.sysgo.com/products/pikeos-hypervisor