Standardizace bezpečnosti komunikace vlak-řídící centrum

Standardization of communication security train-control centre

RNDr. Jan Procházka, Ph.D.[1,3], Petr Novobilský[1], Doc. RNDr. Dana Procházková, DrSc.[2,3],

[1] Q-media s.r.o., Počernická 272/96, 10800 Praha 10, ČR,

[2] České vysoké učení technické v Praze, Fakulta strojní, Technická 4, 16607, Praha 6, ČR

[3] Vysoké učení technické v Brně, Ústav soudního inženýrství, Purkyňova 464/118, 612 00, Brno, ČR

Abstrakt:

Železniční infrastruktura je SoS (System of Systems) a skládá se z mnoha různých částí. Předmětné pod-systémy mají tendenci být propojeny jak fyzicky, tak prostřednictvím komunikačních technologií. Zajištění bezpečné komunikace mezi subsystémy je pak klíčovým úkolem pro předcházení rizikům spojeným s propojeními pod-systémů.

Železnice má také status kritické infrastruktury. Ochrana kritických částí železniční infrastruktury je jedním ze základních cílů národní bezpečnosti. Národní železnice zahrnuje její konstrukční prvky a systém řízení, i organizaci železniční dopravy ve vztahu k evropské železniční síti.

Při zabezpečení a zajišťování bezpečí železnice jako kyber-fyzického systému je potřeba nastavit minimum požadavků, které by měly spravovat všechny systémy. Důležité jsou také postupy, kterými lze dosáhnout minimálních požadavků, stejně jako zesílení bezpečnosti systému. K danému účelu slouží nejrůznější standardy pro všechny prvky železnice, stejně jako pro nastavení celého systému. Nově vzniká technická specifikace, která přenáší nejnovější poznatky v zabezpečení komunikací do potřeb železnice, prTS 50701.

Klíčová slova:

Železnice; kyber-fyzický systém; MILS; bezpečnost; komunikace.

Abstract:

The railway infrastructure is a SoS (System of Systems) and it consists of many different parts. These subsystems tend to be connected both physically and through communication

technologies. Ensuring the safe links among subsystems is then a key task to prevent risks associated with intersystem links.

The railway has also the status of Critical Infrastructure. Protecting the critical parts of rail infrastructure is one of the fundamental objectives of national security. The national railroad includes its structural components and a system of management, and organization of rail traffic in relation to the European rail network.

In order to ensure the safety of the railway as a cyber-physical system, it is necessary to set a minimum of requirements that should be managed by all systems. Also, there are important procedures by which minimum requirements can be achieved, as well as the strengthening the system security. A variety of standards for all elements of the railway serves for this purpose, as well as for setting up the system. A new technical specification is being developed that translates the latest knowledge in communication security into the needs of the railway, prTS 50701.

Key words

Railway; cyber-physical system; MILS; safety; communication.

1 Úvod:

Železnice je otevřený komplexní systém. V rámci lidského systému je propojená s řadou dalších systémů a musí tak při zajištění zabezpečení a bezpečnosti v rámci přístupu systému systémů (SoS) respektovat propojení s ostatními systémy. V rámci dlouhé historie a tradice byly zavedeny postupy na řešení konfliktů s ostatními systémy v území, jako jsou například ostatní dopravní infrastruktury, nebo lidská sídla.

V rámci nových technologií, používaných ve vlacích, na tratích nebo v rámci řídících center nám ale roste provázanost železnice s komunikačními a řídícími systémy. Železnici tak nelze brát už pouze jako fyzický systém, je nutné začít aplikovat k ní přístup jako ke kyber-fyzickému systému (CPS).

Na rozdíl od provázanosti mezi systémy ve stejném (fyzickém) prostoru se CPS vypořádává s provázaností ve dvou prostorech s vlastními pravidly fungování. Zajistit správné fungování je tak mnohem náročnější. Řešení konfliktu požadavků mezi kybernetickou a fyzickou částí je nutné ve všech fázích života CPS. Článek se zaměří pouze na problematiku první fáze, kdy

potřebujeme navrhnout bezpečnou architekturu komunikační brány vlaku tak, aby respektovala požadavky obou prostorů v rámci jejichž průniku se nachází.

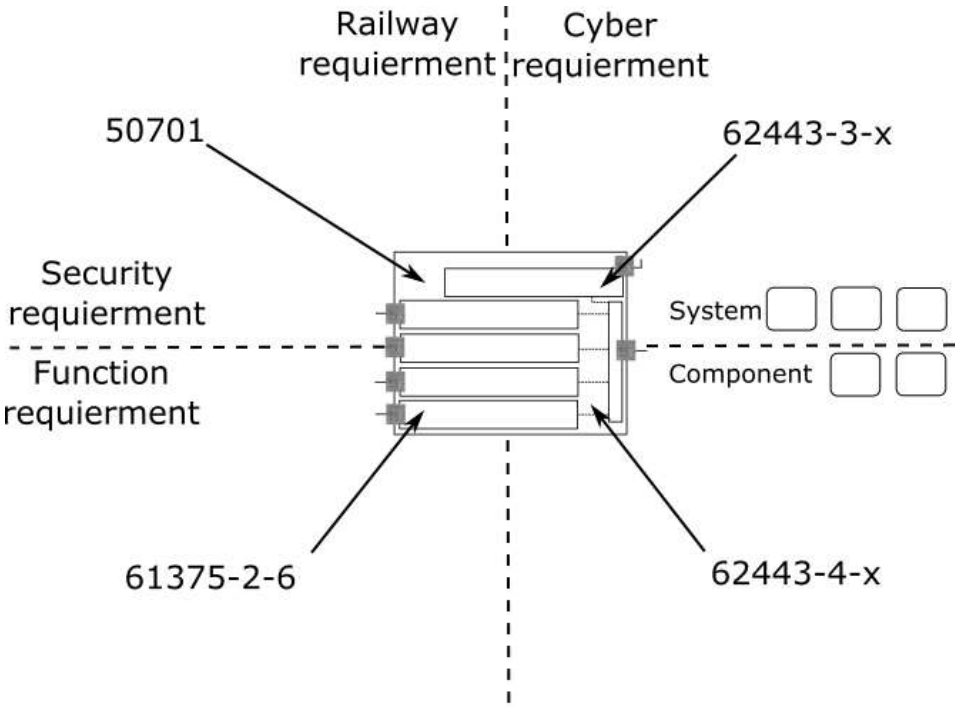
V dalších kapitolách článku se nejprve seznámíme s normami, kterými se musí komunikační brána vlaku řídit, kapitola 1. V kapitole 2 načrtneme architekturu brány. Konkrétní funkční a bezpečnostní požadavky pak budou v kapitole 3.

2 Certifikační rámec:

Než se spustí celá fáze ověřování a certifikace produktu na základě požadovaných standardů, je potřeba produkt definovat. Definování produktů vyžaduje obecný náhled do standardů. Při vytváření standardizačního rámce musíme zvažovat vnitřní a vnější rámec.

2.1 Vnitřní rámec:

V rámci vnitřního rámce vyžadujeme správné plnění funkcí certifikovaným produktem. Funkční požadavky mohou vycházet jak z kybernetické, tak z fyzické části systému. Vedle funkčních požadavků pak sledujeme i bezpečnostní požadavky, obrázek 1. Systém musí být opět zabezpečen proti hrozbám a ohrožením fyzické i kybernetické povahy.



Obrázek 1: Vnitřní certifikační rámec kybernetické brány vlaku.

V případě průniku komunikační sítě a železniční infrastruktury tak dostáváme 4 oblasti požadavků, které je nutné implementovat a ověřit. V případě kybernetické části našeho CPS vychází požadavky z normy IEC 62443 (2019). Problém si pak můžeme rozdělit na funkčnost jednotlivých komponent.

Požadavky pro fyzickou část, tedy železnici, jsou rozděleny do více norem. V našem případě komunikační brána vlaku má definované požadavky v normě IEC 61375-2-6 (2018). Na obrázku 1 máme ještě zmíněnou jednu normu z drážního prostředí, tj. normu prTS 50701 (2020), která je v době tvorby článku ještě v procesu schvalování. Norma prTS 50701 si dává za cíl zajistit hladkou aplikaci požadavků na kybernetickou bezpečnost v oblasti železnice. Vedle toho se jedná o styčný bod pro vnější certifikační rámec.

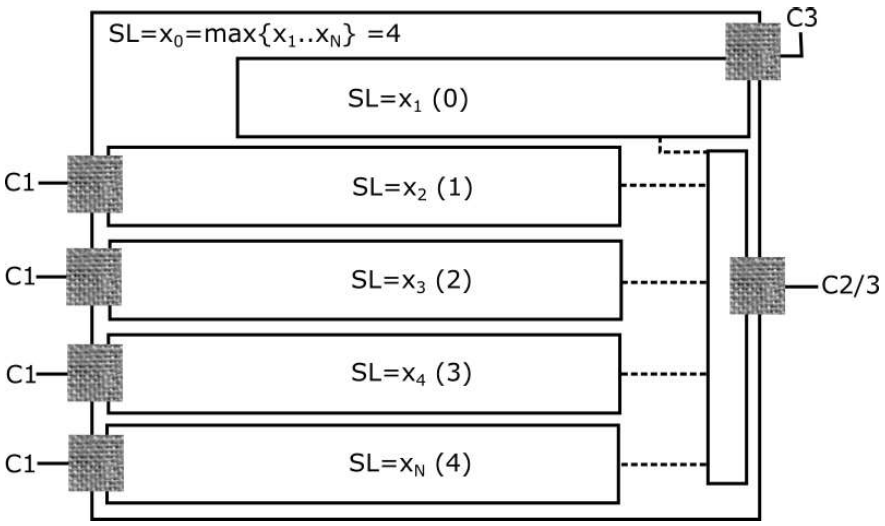
2.2 Vnější rámec:

Zatímco vnitřní certifikační rámec klade požadavky přímo na certifikovaný produkt, vnější certifikační rámec se dotýká spíše prostředí vývoje a prostředí instalace. Nebývá tak certifikován přímo s produktem. Roli hrají především dvě normy. První se zabývá řízením zabezpečení informací v prostředí vývoje ISO 27001 (2017). V případě snadného odcizení informací o produktu klesá i jeho důvěryhodnost.

V celém rámci funkčních a bezpečnostních požadavků chybí ještě požadavky, které jsou spojené s nejdůležitějšími veřejnými zájmy lidského systému. CPS proto vyžaduje zvážení i požadavků na bezpečí lidí. Zvážení a implementace těchto požadavků je explicitně požadováno standardem prTS 50701. Jejich určení je však velmi specifické vzhledem k místu instalace a jeho okolního prostředí. V souvislosti s tím lze zmínit normu EN 50126 (2017), v rámci které lze předmětné požadavky definovat.

3 Kybernetická brána vlaku

V druhé kapitole jsme uvedli, kterými se musí kybernetická brána vlaku řídit. Začneme-li normou prTS50701, pak musíme počítat s pěti různými vnitřními sítěmi vlaku, každá s jiným požadavkem na úroveň zabezpečení (SL). Úroveň zabezpečení určujeme na základě normy IEC 62443. Na vstupu musíme počítat s veřejnou sítí kategorie 3, jedna z pěti vlakových sítí je internet pro cestující také kategorie 3. Další vnitřní vlakové systémy by na základě požadavků normy IEC 61375-2-6 měly být kategorie 1. Požadavky na kategorie sítí opět definujeme podle normy IEC 62443. Výsledná struktura je znázorněná na obrázku 2.



Obrázek 2: Diagram komunikačních kanálů v kybernetické bráně vlaku.

Jednotlivé vnitřní sítě vlaku můžeme ve stručnosti popsat od SL 0 po SL 4:

1. Internet pro cestující.
2. Komfort cestování.
3. Pomocné funkce.
4. Řídící funkce.
5. Nouzové funkce.

Na obrázku 2 je vidět, že vedle jednotlivých komunikačních kanálu máme i prostředí platformy, ve které dochází k dělení jednotlivých komunikací. Vytvořit pro jednotlivé sítě vlastní komunikační vysílač by bylo drahé a náročné na prostor. Z důvodu zabezpečení, jednotlivé sítě ale musí být na sobě nezávislé. Přijatelné řešení nabízí aplikace přístupu vícero nezávislých úrovní bezpečnosti (MILS), Harrison (2005).

Platforma MILS slouží k vytváření nezávislých oddělení na jedné výpočetní jednotce. Architektura několika nezávislých oddílů je vhodná v místě, kde se jednotlivé oddíly liší v míře zabezpečení, osobách, které mají přístup k datům, anebo úkolech, za které osoby odpovídají. Jsou oblasti lidské činnosti, kde je členění na nezávislé oddíly již normativně stanoveno, například standard ARINC 653 (2012) v letectví. Na železnici se zatím počítá pouze s doporučením. Dá se předpokládat, že v rámci rozšiřujícího se využívání telemetrie a vzdálených přístupů, se dělení řídících funkcí vlaku do nezávislých oddílů také stane předmětem norem.

V článku se dále zabýváme využitím MILS platformy pro potřeby komunikačního dělení na kybernetické bráně vlaku. Bránu využívá pro separaci jádra operační systém PikeOS (2019), který běží na Power PC. Předmětné nastavení umožňuje, že v rámci konfigurace MILS za pomocí PikeOS máme větší kontrolu nad nastavením pravidel dělení komunikačních toků. Jednotlivá opatření pro dosažení požadované úrovně zabezpečení (SL) pak lze aplikovat v rámci stejné výpočetní jednotky a prostředí PikeOS. Z pohledu nároků na výpočetní výkon v našem případě počítáme s jejich aplikací až v rámci jednotlivých vnitřních sítí. Cílem architektury brány a její realizace je zajistit, aby kompromitace méně zajištěných sítí neohrozila kritičtější části sítě vlaku. Analýza možností a rizik brány je předmětem evropského projektu ADMORPH (2020).

4 Požadavky:

Optimalizace certifikačního cyklu platformy MILS je předmětem evropského projektu certMILS (2017). Sestavení požadavků a jejich verifikace pro různá prostředí se vyvíjí pod vlivem nových norem. Jak bylo uvedeno v předchozích kapitolách, požadavků na komunikační bránu je celá řada. Vypisovat a zdůvodňovat všechny není v rámci jednoho článku možné. Níže proto nejprve probereme požadavky železničních a kybernetických norem v obecné rovině. Hlubší pozornost budeme věnovat těm požadavkům, které souvisí s členěním kybernetického systému na nezávislé oddíly. Tyto požadavky mají totiž zvláštní význam pro platformu MILS a naši architekturu.

4.1 Železniční požadavky:

Funkční požadavky normy prTS 50701 (2020) na komunikační bránu jsou již promítnuté do designu na obrázku 2. Vedle toho má norma prTS 50701 bezpečnostní požadavky na vývoj produktu podle normy ISO 27001 (2017) a na kybernetické zabezpečení podle normy IEC 62443 (2019), kterou se budeme zabývat níže. Norma prTS 50701 vedle funkčních požadavků řeší propojení bezpečnostních požadavků a případné konflikty s požadavky na bezpečí, určené podle EN 50126-1 (2017).

Požadavky na zabezpečení jsou relevantní místu instalace produktu a lze je identifikovat až na základě spolupráce s případným provozovatelem. Obě uváděné drážní normy, prTS 50701 a IEC 61375-2-6 (2018) s nimi již počítají. Opatření a funkce, určené jako relevantní k zajištění bezpečí jsou umístěna do vlastní části sítě, která může mít přímé připojení pouze na

bezpečnostní síť s nejvyšším zabezpečením, SL4, na obrázku 2 dole. Část 4.9 normy EN 50126-1 definuje požadavky na komunikační zabezpečení a při implementaci normy IEC 62443 je nutnost dbát, aby nedošlo ke konfliktu mezi jednotlivými požadavky.

4.2 Kybernetické požadavky:

Požadavky Evropského projektu certMILS vychází především z normy IEC 62443 (2019). Projekt jako takový vychází i ze zkušeností a postupů starších standardů, například „Common Criteria“ ISO 15408 (1999). Seznámit se blíže s procesem řízení platformy MILS je možné v pracích Procházka (2019) a Schulz (2018 a 2019).

Norma IEC 62443 se skládá z mnoha částí. Některé z nich řeší proces vývoje produktu, v dalších částech najdeme odvolání na normu ISO 27001, aplikaci přístupu obrany do hloubky, implementaci bezpečnosti již do původní architektury, životní cyklus produktu, anebo pravidla kontroly produktu, IEC 62443-4-1.

Část normy IEC 62443-4-2 řeší v jednotlivých odstavcích nástroje, které jsou potřebné pro zabezpečený chod v kybernetickém prostoru. Je potřeba:

1. Určit množství a typ identifikátorů, kterými se bude řízení prokazovat a způsob jejich ověření (FR1).
2. Určit pravidla řízení a údržby prvku (FR2).
3. Nastavit monitoring a ochranu integrity systému (FR3).
4. Definovat potřebu a zajištění důvěrnosti informací (FR4).
5. Segmentovat síť a nastavit povolené toky mezi jejími jednotlivými oddíly (FR5).
6. Sledovat a zaznamenávat jevy, které se v systému během života odehrají pro případnou prevenci či odezvu na problémy (FR6).
7. Zajistit správu zdrojů systému během normálních a nouzových stavů (FR7).

Všechny uvedené požadavky mají SL od 0 do 4. Stav systému můžeme zapsat pomocí vektoru (FR1, FR2, FR3, FR4, FR5, FR6, FR7). Dosažení požadovaného stupně SL je možné zajistit několika způsoby. Z uvedených oblastí je pro platformu MILS zajímavá zejména část FR5. Právě segmentace sítě a kontrola nad komunikací mezi jednotlivými oddíly je hlavní devizou tohoto přístupu.

4.3 Zabezpečení hranic zón:

Kybernetická brána vlaku je síťovým prvkem kyberprostoru. V rámci normy IEC 62443-4-2 se na ni vztahují požadavky na síťová zařízení (NDR). Komunikace vlaku s řídícím centrem probíhá přes otevřenou síť. Je proto potřeba nastavit způsob schvalování (FR1) jednotlivých příkazů (NDR-1.13).

Architektura brány je v případě MILS definována v konfiguračním souboru. Konfigurační soubor určuje jednak segmentaci jednotlivých oddílů a nastavení komunikace mezi nimi (FR5). Konfigurace také přiděluje jednotlivé zdroje systémů pro jednotlivé oddíly, a to jak ve výchozím, tak v pozměněném (nouzovém) stavu (FR7). Ochrana konfiguračního souboru, stejně jako ochrana jeho bootování vyžaduje zvláštní kontrolu (NDR-3.14).

Dodržování konfigurovaných pravidel komunikace je pak nutné monitorovat (FR3). Jednotlivé oddíly by měly být schopny odmítnout komunikační toky v nežádoucích směrech, anebo bez požadovaných ověřených identifikátorů, a v případě nutnosti uzavřít daný komunikační kanál (NDR-5.2).

5 Závěr:

S novými komunikačními technologiemi rostou i požadavky na zabezpečení komunikačních systémů jednotlivých infrastruktur. V případě železnice jde o vytvoření nové technické specifikace 50701, která přenáší kybernetické požadavky do prostředí dráhy. Nové požadavky se v něčem překrývají s požadavky starými a v něčem je rozšiřují. Jsou i aspekty kybernetických norem, jejichž překlad pro potřeby praxe může vytvořit jisté kontroverze.

V článku jsou rozepsány předpokládané požadavky na kybernetickou bránu vlaku na základě nových standardů a specifikací. Hlavní devizou vyvíjené brány je aplikace technologie MILS, která může implementaci požadavků postupů z oblasti IEC 62443 zjednodušit v prostředí dráhy prTS 50701.

Uvedené postupy se týkají produktu, jehož certifikace v současné době probíhá. Certifikační rámec byl definován na základě zkušeností s již instalovanými produkty. Před jeho dokončením však může dojít i ke změnám na základě nových poznatků.

Poděkování:

Výsledky zveřejněné v článku byly vytvořeny s podporou evropských projektů „**certMILS**" ID: 731456 a „**ADMORPH**" ID: 871259. Článek vznikl v rámci projektu PRKODI,

financovaného TAČR v rámci programu „**DOPRAVA 2020+**“, s identifikačním kódem CK01000095.

Použitá literatura:

ADMORPH, 2020. Towards Adaptively Morphing Embedded Systems. *Horizon 2020*, no 871259, EU.

ARINC 653, 2012. *Avionics Application Software Standard Interface*, Airlines Electronic Engineering Committee.

certMILS, 2017. Compositional security certification for medium- to high-assurance COTS-based systems in environments with emerging threats. *Horizon 2020*, no 731456, EU.

EN 50126-1, 2017. *Railway applications – The specification and demonstration of Reliability, Availability, Maintainability and Safety (RAMS)*. CENELEC.

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

IEC 61375-2-6, 2018. *Electronic railway equipment - Train communication network: On-board to ground communication*. International Electrotechnical Commission.

IEC 62443, 2019. *Security for industrial automation and control systems*. International Electrotechnical Commission / International Society of Automation.

ISO 27001, 2017. *Information technology. Security techniques. Information security management systems*. *Requirements*, International Organization for Standardization.

ISO / IEC 15408, 1999. *Common Criteria for Information Technology Security Evaluation*. International Organization for Standardization / International Electrotechnical Commission.

PikeOS, 2019. *PikeOS® 4.2 Certified Hypervisor*, SYSGO.

PROCHAZKA J., NOVOBILSKY P., PROCHAZKOVA D., 2019. 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, pp. 4107 - 4413, doi:10.3850/978-981-11-2724-3_0220-cd.

prTS 50701, 2020. *Railway applications – Cybersecurity*, draft version D7E4, CENELEC.

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