Dobromil Nenutil[1], Tomáš Svoboda[2]

# Architektura komplexního palubního systému ve vlacích vybavených vlakovou komunikační sítí Ethernet

**Klíčová slova:** *vlaková komunikační síť, Train Communication Network, TCN, TCMS, IEC 61375, kybernetická bezpečnost, IEC 62443*

## Úvod

Moderní vlak obsahuje vedle elektronických systémů nezbytných pro vlastní jízdu také řadu systémů, které jsou orientovány na podporu provozu, údržby a na zvýšení komfortu a bezpečnosti cestujících. Mnohé z těchto systémů jsou dále integrovány do informačního a dispečerského systému dopravce či správce infrastruktury. Pro nezbytnou vzájemnou komunikaci palubních řídicích a informačních systémů a pro jejich případnou komunikaci s pozemními systémy je třeba vybavit vozidla komunikační infrastrukturou, která splní všechny jejich nároky na přenos dat, a to jak kapacitní, tak i časové. Takovou komunikační infrastrukturou je vlakový komunikační systém využívající IP technologie a Ethernet a specifikovaný sadou norem IEC 61375 (TCN - Train Communication Network). Článek ve své první části uvádí vysokoúrovňovou architekturu palubního elektronického „ekosystému“ a z něho odvozenou architekturu sítě TCN. Podává charakteristiku TCN a blíže popisuje některé její vlastnosti specifické pro prostředí vlaku. Ve své druhé části se článek věnuje oblasti kybernetické bezpečnosti, jejíž význam pro palubní systémy vlaku významně vzrostl s použitím IP technologií a Ethernetu. Tato část je pojata obecněji a jejím cílem je poskytnout čtenáři základní orientaci týkající se kybernetické bezpečnosti v železničním sektoru. Na závěr článek zmiňuje inovační témata zaměřená na vlakovou komunikační síť řešená v rámci iniciativy Shift2Rail.

## Vysokoúrovňová architektura komplexního palubního systému vlaku

Pro návrh architektury systémů jsou obecně určující tzv. nefunkční požadavky, tj. požadavky, které určují vlastnosti nebo omezující podmínky, kladené na daný systém. Pro palubní systémy vlaku jsou takovými požadavky především požadavky na

- dostupnost: ve vlaku jsou jak systémy, které jsou nezbytné pro jízdu vlaku, tak i systémy, jejichž výpadek způsobí pouze snížení komfortu cestujících,

[1] Dobromil Nenutil, Ing., 1950, ČVUT – Fakulta elektrotechnická v Praze, obor technická kybernetika, UniControls a.s., oddělení technického rozvoje, člen pracovních skupin TC9/WG43, WG46 standardizační organizace IEC

[2] Tomáš Svoboda, Ing., 1978, ČVUT – Fakulta elektrotechnická v Praze, obor řídicí technika a technická kybernetika, UniControls a.s., oddělení technického rozvoje, odpovědný za rozvoj systému TCMS

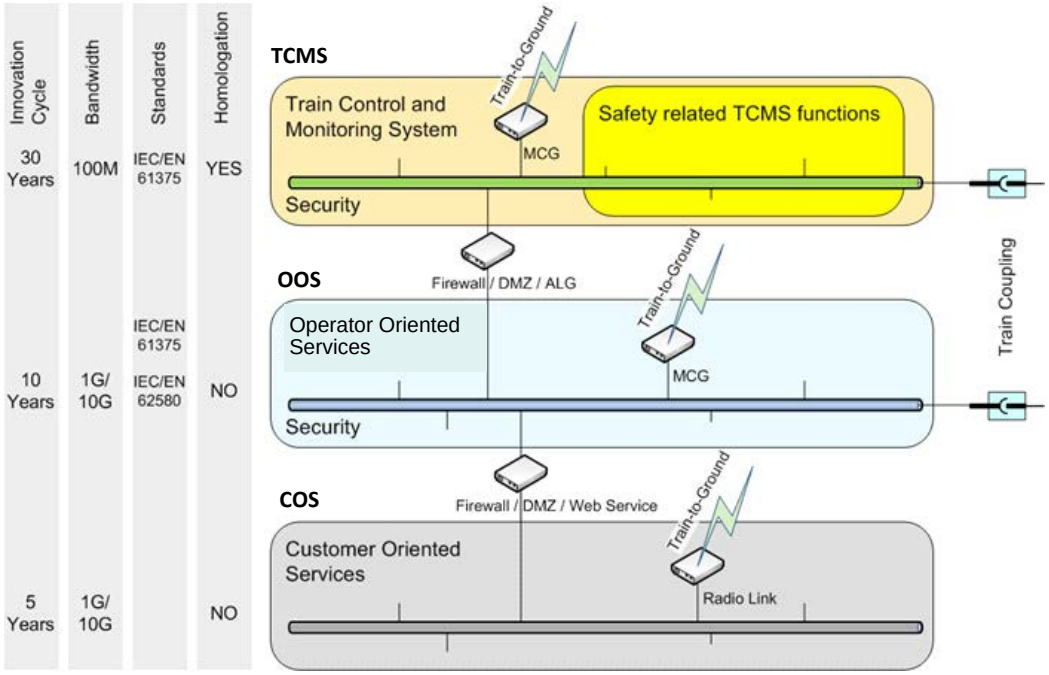
- bezpečnost: některé ze systémů mají vztah k bezpečnosti (ve smyslu „safety“),
- kybernetickou bezpečnost: palubní komunikační síť není již izolovanou sítí, je propojena s pozemními sítěmi (některé systémy vlaku komunikují s pozemními systémy) a případně se k ní připojují zařízení cestujících; systémy vlaku jsou tak otevřeny potenciálnímu útočníkovi – systémy musí být chráněny, stupeň požadované ochrany není obvykle pro všechny systémy stejný,
- interoperabilitu: je požadováno spojování vlaků různých výrobců, jejichž systémy si musí „rozumět“,
- komunikační systém: systémy vlaku jsou vesměs distribuované systémy a výkonnostní požadavky na komunikační systém, jako jsou požadavky na přenosovou rychlost, zpoždění a kolísání přenosu dat, dobu odezvy, se pro jednotlivé systémy liší,
- homologaci: pro některé systémy vlaku je požadována homologace,
- délku inovačního cyklu: inovační cyklus informačních systémů vlaku je podstatně kratší než je inovační cyklus jeho řídicích systémů,
- aplikaci standardů.

Základní architektura komplexního palubního systému, která zohledňuje požadavky uvedené výše, je znázorněna na obrázku 1. Tato architektura vznikla v projektu Roll2Rail[3] a jejími elementy jsou funkční domény a komunikační síť vlaku. Vychází z funkční dekompozice železničního vozidla specifikované v normě ČSN EN15380-4 [1]. V ní uvedené řídicí a informační funkce a tedy i (sub)systémy, které tyto funkce realizují, jsou zařazeny do jedné ze tří níže uvedených funkčních domén.

- Doména TCMS (Train Control and Monitoring System): zahrnuje všechny řídicí a monitorovací funkce vlaku. Do této domény náleží funkce se vztahem k bezpečnosti a funkce a zařízení vyžadující homologaci. Délka inovačního cyklu funkcí/zařízení této domény odpovídá životnosti vozidla, přenosová rychlost 100 Mbit/s je pro ně postačující. Komunikační systém v doméně musí splňovat standard IEC 61375. Do domény TCMS náleží například trakční systém, brzdný systém, řízení dveří, osvětlení, systém vytápění, ventilace a klimatizace, vlakový rozhlas, systém nouzové signalizace pro cestující, ETCS, systém palubního záznamu jízdních dat [24], kamerový systém – zpětná zrcátka.
- Doména OOS (Operator Oriented Services): zahrnuje funkce, které nejsou pro vlastní jízdu vlaku nezbytné. Předpokládaná délka inovačního cyklu funkcí/zařízení této domény je 10 let, minimální požadovaná přenosová rychlost komunikačního systému splňujícího standard IEC 61375 je 1 Gbit/s. Standard IEC 62580 [15], který je relevantní pro tuto doménu, pracuje s pojmem „služba“, kterou chápe jako soubor funkcí (nebo jednu funkci) poskytovaný aplikací jiné aplikaci (aplikacím). Tento standard specifikuje další vrstvy (service framework, application profile) nad komunikačním profilem dle IEC 61375. Do domény OOS náleží například informační systém pro cestující, infotainment (informace a zábava) systém, kamerový systém – dohled, rezervační systém, systém počítání cestujících, systém prodeje jízdenek, asistenční systém strojvedoucího, diagnostika a CBM (condition based maintenance) systémy.
- Doména COS (Customer Oriented Services): zahrnuje například infoportal pro cestující a funkce umožňující cestujícím přístup na internet z jejich vlastních

[3] Roll2Rail, projekt programu výzkumu a inovací Horizon 2020, 05/2015 – 10/2017, byl zaměřen na technické inovace různých systémů vozidla včetně vlakové komunikační sítě (www.roll2rail.eu)

zařízení, například prostřednictvím vozidlové WiFi sítě, která je součástí domény. Předpokládaná délka inovačního cyklu funkcí/zařízení této domény je 5 let, minimální požadovaná přenosová rychlost komunikačního systému je 1 Gbit/s. Pro komunikaci uvnitř této domény je k dispozici řada široce používaných standardů.




*Obrázek 1: Základní architektura – funkční domény (Zdroj: [23])*

Architektura komunikační sítě vlaku zohledňuje uvedené rozdělení do funkčních domén tak, že požaduje nezávislou síť pro každou z nich (síť TCMS, síť OOS, síť COS). Tuto nezávislost lze zajistit oddělenými fyzickými sítěmi, nebo, není-li fyzické oddělení požadováno, pak logickým oddělením (např. využitím VLAN). Ke komunikačním sítím jednotlivých funkčních domén se vztahují dále uvedené požadavky.

- Síť TCMS musí být necitlivá na změny v jiných sítích.
- Přidání zařízení do sítě OOS, například za účelem přidání nové funkce, nesmí ovlivnit síť TCMS.
- Je třeba počítat s inovací funkcí a zařízení v síti OOS během životnosti železničního vozidla.
- Je třeba počítat s častou inovací funkcí a zařízení v síti COS během životnosti železničního vozidla.
- Obvykle je požadována datová komunikace mezi sítěmi jednotlivých domén. Týká se však pouze vybraných dat. Vzhledem k tomu, že požadovaný stupeň ochrany proti bezpečnostním hrozbám se pro jednotlivé domény liší, je třeba vložit do komunikačního kanálu mezi nimi síťové komponenty řídicí datové toky. Mohou jimi být například firewall nebo komunikační brána aplikační vrstvy (ALG), které mohou být navíc umístěny v demilitarizované zóně (DMZ). Příkladem datového toku z domény OOS do domény COS je video stream z čelní kamery vlaku.
- Přímá komunikace mezi sítí COS a sítí TCMS není povolena.

- Spojení TCMS a OOS sítí mezi jednotkami (consist) je provedeno odděleně (fyzicky nebo logicky), tak aby tyto sítě byly separovány v rozsahu celého vlaku. Sítě COS jsou omezeny na jednotku.
- Komunikace s pozemními systémy je realizována prostřednictvím mobilní komunikační brány (MCG – Mobile Communication Gateway[4]). Sítě TCMS a OOS mohou mít vlastní nebo společnou MCG.

## Vlaková komunikační síť TCN

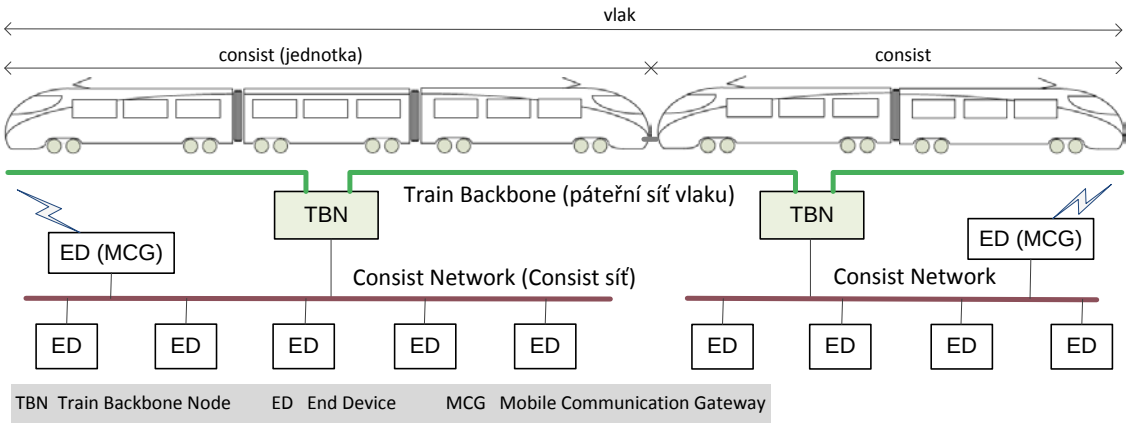
Síť TCN je, jak znázorňuje obrázek 2, hierarchickou sítí dvou úrovní. Vyšší úroveň TCN tvoří páteřní síť vlaku Train Backbone (TB), k síti nižší úrovně se připojují koncová zařízení, tj zařízení, která jsou primárně zdrojem a cílem přenášených dat. Síť nižší úrovně je nazvána Consist Network, neboť propojuje zařízení v pevné sestavě vozů označované jako consist. V dalším textu budeme používat pro consist termín jednotka. Limitním případem jednotky je jediný vůz. Consist síť, může jich být v jednotce i více, je připojena k Train Backbone jedním komunikačním uzlem Train Backbone Node (TBN), který může být zálohován.
Dvouúrovňová architektura sítě TCN přináší obecně níže uvedené výhody.

- Consist síť je na rozdíl od Train Backbone statická, předem nakonfigurovaná, komunikační síť. TB je dynamická síť, která mění svoji topologii, kdykoliv dojde ke změně kompozice vlaku. Během rekonfigurace TB je přenos aplikačních dat na této síti přerušen, což však nemá vliv na komunikaci v Consist síti.
- Není-li jedna z Consist sítí v provozu (např. napájení je vypnuto), není tím ovlivněna komunikace mezi ostatními Consist sítěmi vlaku.
- Train Backbone není zatěžována přenosem všech dat, která si vyměňují jednotlivá koncová zařízení ve vlaku. Pouze data adresovaná zařízením v jiných Consist sítích jsou transportována přes TB.

Koncová zařízení, v obrázku označená jako ED (End Device), mohou představovat například:

- Inteligentní zařízení jako je VCU (Vehicle Control Unit) nebo displej strojvedoucího, tj. zařízení, která výlučně nenáleží určitému subsystému vlaku,
- řídicí jednotky inteligentních subsystémů (např. řízení trakce, řízení brzd, HVAC),
- Vzdálené I/O jednotky, které připojují ty části technologie vlaku, které nejsou řízeny/monitorovány vyhrazenou řídicí jednotkou (např. ovládací prvky a indikátory na pultu strojvedoucího).

[4] MCG dle současné verze normy IEC 61375 nezajišťuje přenos dat se vztahem k bezpečnosti (safety related data) a nemůže být proto například použita systémem vlakového zabezpečovače.




*Obrázek 2: Základní architektura sítě TCN*

Součástí sítě TCN je i datové komunikační rozhraní k pozemním systémům, které je realizováno mobilní komunikační bránou MCG. Typicky je MCG umístěna v každé jednotce.

Síť TCN je možné realizovat komunikačními technologiemi dvou tříd: třídou sběrnicových (bus) technologií a třídou přepínaných (switched) technologií, přičemž technologie obou tříd mohou být kombinovány.

Třída sběrnicových technologií je charakterizována tím, že síťová nebo koncová zařízení jsou připojena k jednomu přenosovému médiu, přičemž celá sběrnice tvoří jeden segment sítě a tedy jednu kolizní a "broadcast" doménu. Do této třídy náleží komunikace WTB, MVB a CAN. V sítích WTB a MVB je provoz řízen jedním z uzlů, v síti CAN je v jejích uzlech implementován algoritmus řídicí přístup na linku.

Třída přepínaných technologií se vyznačuje tím, že každé síťové nebo koncové zařízení je připojeno k přepínači (switch), který data přijatá na svých portech vysílá na porty, přes které jsou dostupná adresovaná koncová zařízení. Sítě založené na této technologii mají možnost omezit kolizní a „broadcast" domény. Do této třídy náleží komunikace ETB (Ethernet Train Backbone) a ECN (Ethernet Consist Network), o které byla, vedle komunikace CAN, norma IEC 61375 nově rozšířena.

Jak bude síť TCN v konkrétním vlaku realizována, záleží zcela na uživateli. Může například použít síť WTB/MVB pro systémy řízení vlaku, čili jako síť TCMS, a síť OOS realizovat jako síť ETB/ECN. Vzhledem k dobré dostupnosti koncových zařízení s rozhraním MVB pro doménu TCMS a s ohledem na požadavky na bezpečnost a kybernetickou bezpečnost můžeme síť TCN s touto architekturou nalézt i v nově projektovaných vlacích. Počet sítí ETB ve vlaku omezuje norma na čtyři.

## Struktura normy IEC 61375

Tabulka 1 uvádí seznam norem nové sady *IEC 61375 Railway equipment - Train communication network (TCN)* a jejich aktuální stav. Dokument ve stavu FDIS (Final Draft International Standard) lze považovat za dokument, který se již nebude měnit, čili je možno jej implementovat. Dokument ve stavu CD (Committee Draft) je prvním návrhem. Stupněm mezi CD a FDIS je CDV (Committee Draft for Voting). Obsah dokumentů uvedených v šedě označených polích vznikl přenosem z normy IEC 61375:2007.

*Tabulka 1: Sada norem IEC 61375*

| Označení | Název části | Stav |
|---|---|---|
| IEC[**)] 61375-1[*)] | Part 1: General Architecture | publikována 2012 |
| IEC 61375-2-1[*)] | Part 2-1: Wire Train Bus (WTB) | publikována 2012 |
| IEC 61375-2-2[*)] | Part 2-2: WTB Conformance Testing | publikována 2012 |
| IEC 61375-2-3[*)] | Part 2-3: Communication Profile | publikována 2015 |
| IEC TS 61375-2-4 | Part 2-4: Application Profile | publikována 2017 |
| IEC 61375-2-5[*)] | Part 2-5: Ethernet Train Backbone (ETB) | publikována 2014 |
| IEC 61375-2-6 | Part 2-6: On-board to ground communication | FDIS odevzdán v 10/2017 |
| IEC TR 61375-2-7 | Part 2-7: Wireless Train Backbone (WLTB) | publikována 2014 |
| IEC 61375-2-8 | Part 2-8: TCN conformance test | zahájeny práce na CD |
| IEC 61375-3-1[*)] | Part 3-1: Multifunction Vehicle Bus (MVB) | publikována 2012 |
| IEC 61375-3-2[*)] | Part 3-2: MVB Conformance Testing | publikována 2012 |
| IEC 61375-3-3[*)] | Part 3-3: CANopen Consist Network (CCN) | publikována 2012 |
| IEC 61375-3-4[*)] | Part 3-4: Ethernet Consist Network (ECN) | publikována 2014 |

[*)] Tyto části normy byly již převzaty jako normy ČSN EN[**)], viz kapitola Literatura.
[**)] Normy sady IEC 61375 vypracované v IEC/TC9 jsou předkládány k paralelnímu hlasování IEC-CENELEC a schvalovány organizací CENELEC jako normy sady EN 61375.

Poznámka 1
Část 2-4: Application Profile byla publikována pouze jako technická specifikace (TS). V průběhu práce na této části normy se ukázalo, že je nezbytné, aby se na jejím vytvoření přímo podíleli i zástupci dopravců – uživatelů vlaků. Ti jsou sdruženi v organizaci UIC. Proto v rámci IEC/TC9 vznikla poradní skupina IEC-UIC TRAINET, která určuje obsah této části normy. Aktuální vydání dokumentu specifikuje obecnou architekturu aplikací, provozní režimy vlaku a aplikační profil pro aplikaci Řízení dveří. Po doplnění o aplikační profily dalších aplikací (řízení trakce, řízení brzd, …) bude tato technická specifikace vydána jako norma.

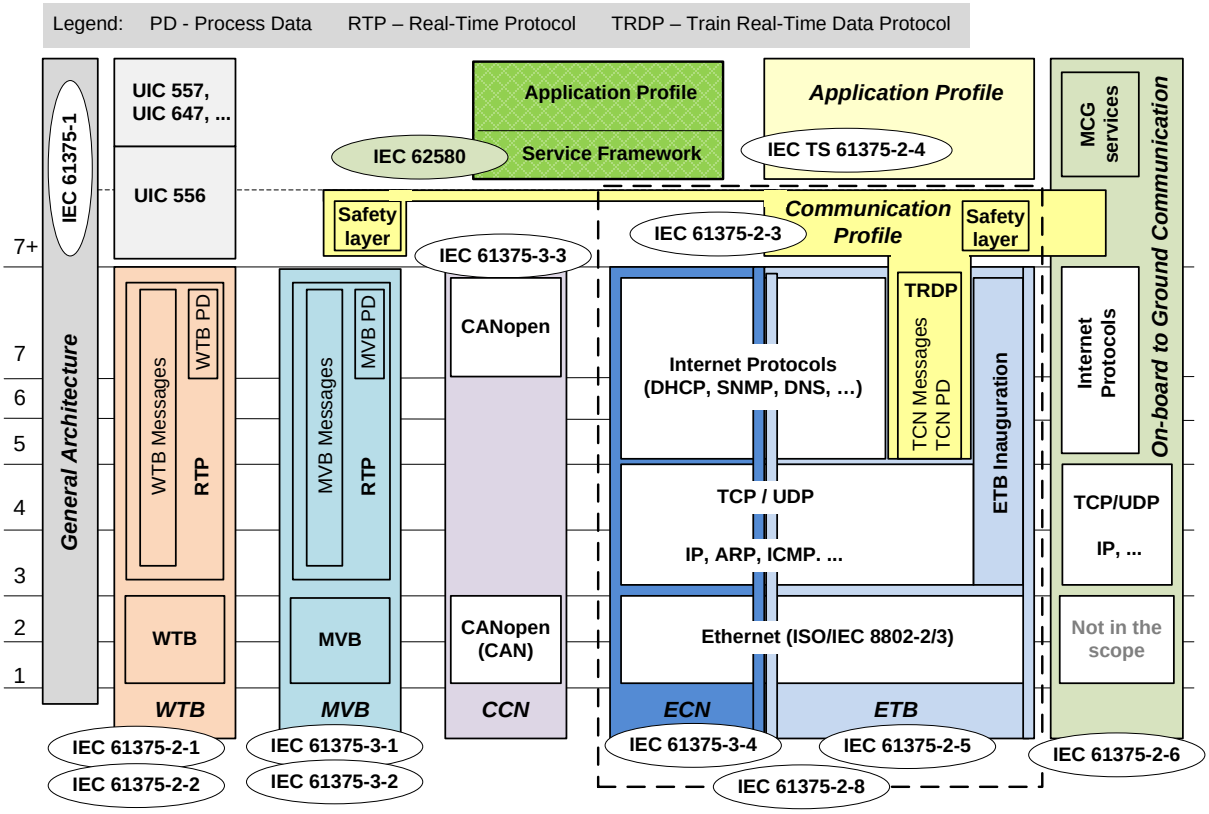
Poznámka 2
Část 2-7: Wireless Train Backbone (WLTB) byla vydána pouze jako technická zpráva (TR – Technical Report). Specifikuje bezdrátovou vlakovou páteřní síť, jejíž typické použití je v dlouhých nákladních vlacích, ve kterých umožní komunikaci mezi lokomotivami zařazenými na různých místech vlaku. Standardizovaná WLTB však bude jiná. Její návrh vzejde z projektu řešeného v rámci Shift2Rail[5] a ten bude předán ke standardizaci. První kroky v tomto směru byly učiněny v projektu Roll2Rail, ve kterém bylo demonstrováno použití LTE pro realizaci WLTB. Výsledky projektu Roll2Rail jsou pak vstupem do navazujících projektů řešených již v rámci Shift2Rail.

Obrázek 3 znázorňuje vztah jednotlivých částí normy ke standardnímu sedmivrstvému referenčnímu komunikačnímu modelu ISO-OSI (Open System Interconnection). Dále uvádí jak komunikační protokoly, které jsou v jednotlivých

[5] Shift2Rail je společný podnik firem železničního sektoru a Evropské unie. V rámci jeho inovačních programů jsou a budou řešeny výzkumné a inovační projekty k dosažení konkurenceschopného a efektivního železničního dopravního systému (www.shift2rail.org).

částech normy specifikovány (WTB, MVB, RTP, TRDP, …), tak i podstatné protokoly, které jsou specifikovány v jiných normách a v IEC 61375 jsou využívány (IP, TCP/UDP, …). Ty jsou zobrazeny na bílém pozadí. Komunikační profil lze chápat jako rozšíření aplikační vrstvy (vrstva 7). Nad ním je dále umístěn aplikační profil, který definuje interakce mezi jednotlivými funkcemi vlaku a formát vyměňovaných dat. Komunikační profil specifikuje zejména způsob, jakým je vytvářen popis topologie vlaku (Train Topology Database – viz dále), pravidla pro jeho korekci, algoritmus volby vedoucí jednotky vlaku a schéma funkčního adresování. Z obrázku 3 je dále patrné, že

- nedošlo k začlenění vyhlášek UIC, které pro páteřní síť WTB představují komunikační profil a aplikační profily; norma TCN tedy pokryje plně pouze systémy s vlakovou páteřní sítí Ethernet (ETB),
- komunikační profil a aplikační profil se vztahují, stejně jako UIC vyhlášky, ke komunikaci na vlakové páteřní síti (na této síti je vyžadována interoperabilita),
- dodatečně byla vyspecifikována bezpečnostní vrstva (safety layer) pro síť MVB,
- specifikace IEC 62580 navazuje na komunikační profil IEC 61375-2-3.




*Obrázek 3: IEC 61375 v referenčním modelu ISO-OSI*

## TCN se sítěmi ETB a ECN

Jako příklad sítě TCN realizované výlučně sítěmi ETB a ECN je na obrázku 4 znázorněna síť ve vlaku sestávajícího ze dvou jednotek. Tato TCN síť je složena ze dvou samostatných sítí určených pro domény TCMS a OOS, které jsou komunikačně

propojeny. Sítě ECN v jednotlivých doménách se liší svojí topologií. Kruhová síť ECN je použita v doméně TCMS, lineární v doméně OOS.

V síti s lineární topologií může mít porucha přepínače, pokud tento prvek není zálohován, nebo přerušení jednoho segmentu sítě za následek ztrátu celé sítě. Z tohoto důvodu se použití ECN s touto topologií v doméně TCMS nepředpokládá.

Kruhové sítě jsou tolerantní vůči jedné poruše, jak vůči přerušení spojení, tak i poruše uzlu. Aby nedošlo k vytvoření smyčky, je nutné v kruhové síti implementovat algoritmus jejího řízení. Tento algoritmus nebyl předmětem standardizace, neboť nesouvisí s dosažením interoperability požadované na rozhraní ETB. Norma obsahuje pouze požadavek na dobu zotavení kratší než 50 ms.

Vedle sítí ECN s lineární a kruhovou topologií připouští norma ještě žebříčkovou síť. Ta je používána výlučně japonskými výrobci a jimi byla také do normy prosazena. Jak ukázal výpočet, není rozdíl ve spolehlivosti kruhové a žebříčkové sítě ve prospěch žebříčkové sítě významný.

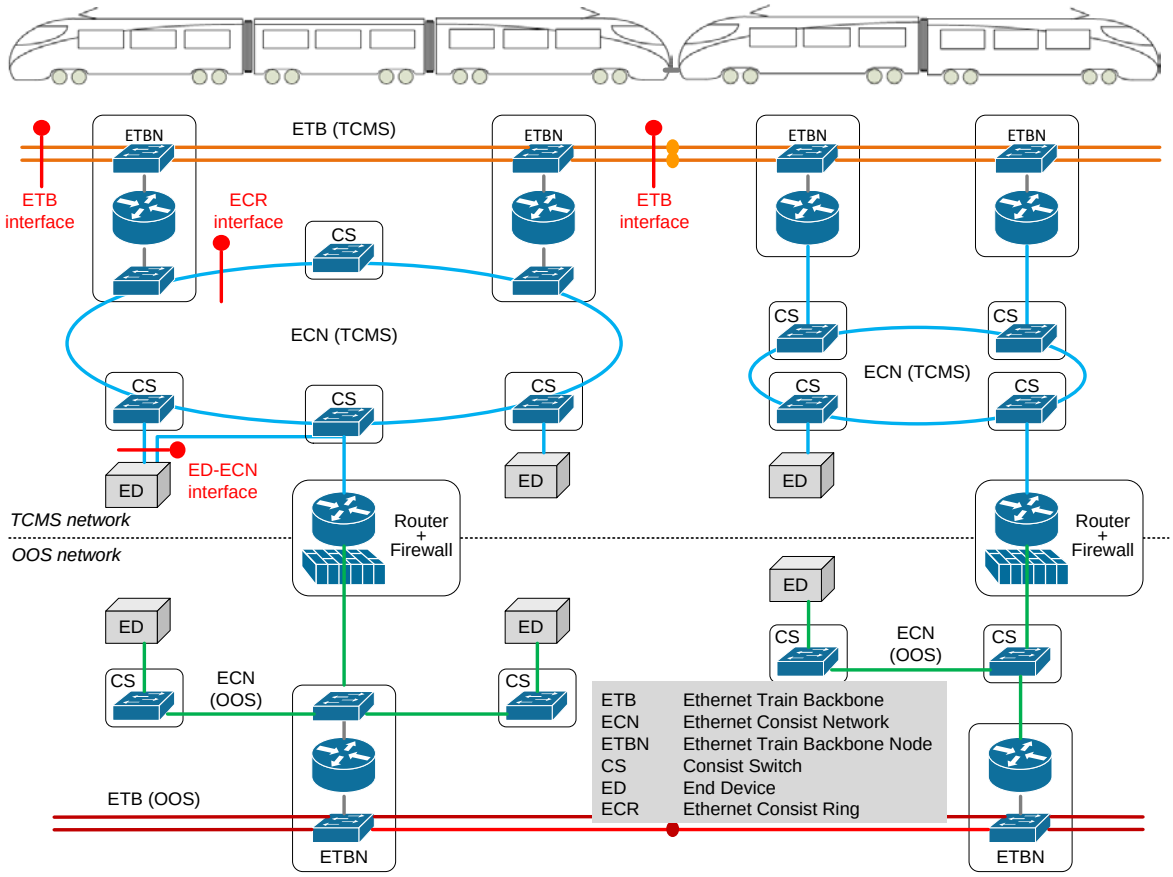
Koncová zařízení jsou k síti ECN připojena přes přepínače (CS – consist switch). Každé koncové zařízení je připojeno na samostatný segment sítě, to znamená, že kolize v přístupu zařízení k médiu nenastávají. Komunikace je plně duplexní. Koncová zařízení mohou být zálohována tak, že jsou připojena samostatnými linkami ke dvěma přepínačům.

Část IEC 61375-3-4 normy specifikuje požadavky na komunikační rozhraní, které musí splňovat zařízení připojená k ECN. Těmi jsou jednak koncová zařízení a jednak přepínače. V obrázku 4 jsou tato rozhraní označena jako ED-ECN a ECR rozhraní.

Sítě Train Backbone musí obecně zajistit komunikaci na zdvojeném přenosovém mediu a také to, že uzly TBN bez napětí nebo v poruše nepřeruší linku. Pro síť ETB připouští norma použití až 4 násobného přenosového média, s tím že kapacita jednotlivých linek může být agregována. Uzly ETBN jsou vybaveny přemosťovacími relé, které umožní provoz na síti ETB i v případě jejich výpadku.

Každá Consist síť jednotky může být k ETB připojena prostřednictvím jednoho nebo dvou uzlů ETBN, kdy tato dvojice tvoří redundantní pár. Algoritmus řízení redundance lze realizovat bez použití vyhrazeného kanálu spojujícího redundantní uzly ETBN. Ty tak mohou být bez problému umístěny například v protilehlých čelních vozech jednotky. Algoritmus řízení redundance uzlů ETBN nesouvisí s interoperabilitou a proto nebyl předmětem standardizace.

Kromě vlastního přenosu dat je úkolem ETBN provedení inaugurace vlaku. Tato funkce a vybrané charakteristiky sítě ETB/ECN jsou popsány v následujících podkapitolách.




*Obrázek 4: Příklad sítě TCN (ETB/ECN) ve vlaku*

**Třídy přenášených dat**

Síť ETB/ECN zajišťuje přenos dat níže uvedených tříd.

- Procesní data (časově kritická data): například data pro řízení pohonů a brzd. Jejich délka je omezena, doba jejich doručení je garantována, data jsou přenášena periodicky a nejsou potvrzována. Ztratí-li se, jsou přenesena v další periodě. V cílovém uzlu poskytuje TCN aplikacím informaci o stáří dat, tj. jak dlouho nebyla aktualizována, a aplikace si stanoví, kdy už data nemůže pro daný účel (např. pro řízení) použít a bude je tedy považovat za neplatná.
- Zprávy: například diagnostické zprávy, informace pro cestující. Jejich délka není omezena, doba doručení není garantována a přenos je potvrzován. Není-li potvrzení doručeno, je vysílání zprávy opakováno.
- “Stream“ data: kontinuální tok dat pro audio a video, např. pro kamerový systém, zábavní video, provozní video (kamerová zpětná zrcátka), vlakový rozhlas.
- “Best effort“ data: rozsáhlé soubory, například obsah diagnostické databáze přenášený na pozemní server, data pro informační systém pro cestující, nové verze softwaru.

Síťová zařízení musí podporovat prioritizaci. To znamená, že pakety jednotlivých tříd dat mohou být opatřeny příznakem priority a přepínač musí pakety zpracovávat dle jeho nastavení. Priorita je přidělena takto (od nejvyšší): Procesní data, Stream data, Data zpráv a Best-effort data. Označení „Best-effort“ čili „nejlepší snaha“ je odvozeno od toho, že síť se snaží tato neprioritní data přenést co nejefektivněji.

Pro přenos procesních dat a zpráv norma specifikuje protokol TRDP (Train Real-Time Data Protocol). Pro přenos audio a video dat a Best-effort dat je norma otevřena pro použití standardních protokolů pro daný účel.

**Komunikační protokol TRDP**

Část normy IEC 61375-2-3 specifikuje protokol TRDP určený pro přenos aplikačních dat po vlakové komunikační síti. Protokol podporuje přenos procesních dat a zpráv a využívá protokoly UDP a TCP ze sady internetových protokolů.

TRDP používá pouze dva typy rámců. První pro přenos procesních dat (PD-PDU), který je vždy šířen prostřednictvím UDP protokolu, druhý pro přenos zpráv (MD-PDU), který může být šířen jak pomocí UDP, tak i TCP protokolu.

Oba typy TRDP rámců mají v hlavičce prostor jak pro číslo verze topologie vlakové sítě (mění se při každé změně kompozice vlaku), tak i číslo verze aktuálního operačního stavu vlaku (mění se např. při změně aktivního stanoviště). Aplikace využívají tyto čítače podle své potřeby. Při komunikaci v lokální Consist síti není jejich použití nutné. Naproti tomu při komunikaci přes dynamickou páteřní síť je možné pomocí kontroly uvedených čísel verzí zajistit, že jak producent, tak i konzument dat mají stejné informace o topologii a operačním stavu vlaku a odstranit tak hazardy spojené s přechodovými stavy při jejich změnách.

Protokol TRDP podporuje několik komunikačních vzorů. Pro přenos procesních dat je typické použití vzoru Push, ve kterém producent dat periodicky vysílá PD-PDU rámec na před-konfigurovanou cílovou adresu. Velmi často se tento vzor používá ve variantě bod-mnohobod, kdy jeden producent vysílá data skupině konzumentů prostřednictvím IP multicast. Pro přenos zpráv je naopak typický vzor Pull, kdy konzument dat (klient) nejprve vyšle žádost producentovi (serveru), ten žádost zpracuje a zašle zpět odpověď.

Norma vyžaduje použití protokolu TRDP pro zajištění interoperability při přenosu aplikačních dat po vlakové páteřní síti. Z pohledu návrhu komunikačního systému je výhodné použít TRDP protokol i pro přenos aplikačních dat v rámci Consist sítě. V takovém případě je možné realizovat spojení mezi Consist sítí a páteřní sítí prostřednictvím ETBN implementovaným jako IP směrovač. V opačném případě by bylo nutné ETBN implementovat jako výrazně komplikovanější aplikační bránu (ALG), která by prováděla transformaci dat mezi protokolem TRDP a aplikačním protokolem použitým v Consist síti.

Otevřená a volně šiřitelná implementace TRDP protokolu je vyvíjena v rámci iniciativy TCNOpen (http://www.tcnopen.eu/).

**Bezpečný přenos dat – bezpečnostní vrstva**

Část normy IEC 6175-2-3 obsahuje specifikaci bezpečnostní vrstvy pro protokoly TRDP a MVB nazvané SDTv2 (Safe Data Transmission version 2), která umožňuje bezpečný přenos dat mezi koncovými zařízeními s úrovní integrity bezpečnosti 2 (SIL 2). Bezpečnostní vrstvu SDTv2 je možné použít jak při komunikaci v rámci Consist sítě, tak i pro komunikaci přes Train Backbone.

Vrstva SDTv2 umístěná mezi aplikací a aplikačním protokolem (TRDP, MVB) přidává při vysílání k datovým paketům integritní informaci, kterou při příjmu použije k ověření toho, zda při přenosu nedošlo k poruše. Je schopna se vypořádat se všemi druhy poruch definovanými normou pro funkční bezpečnost průmyslových komunikačních sběrnic [25], kterými jsou: poškození, ztráta, vložení, opakování,

chybná sekvence, nepřijatelné zpoždění, chybná adresa, maškaráda, jakož i s nepřijatelnou četností chyb komunikačního kanálu a s poruchou redundance, kdy je schopna detekovat, že z redundantních zdrojů dat jich je více aktivních.

Při použití bezpečnostní vrstvy nejsou kladeny žádné bezpečnostní požadavky na přenosový kanál, tj. na komunikační protokoly nižších vrstev. Všechna opatření na ochranu přenášených dat jsou soustředěna v bezpečnostní vrstvě. Takto realizovaný komunikační systém je označován jako „Black Channel“ komunikační systém.

**Inaugurace vlaku**

Jak síť TCN, tak i aplikace se musí umět vyrovnat s dynamickým charakterem vlakové soupravy. Během provozu se může se změnit typ a počet jednotek soupravy – vlaky jsou spojovány a rozpojovány, jednotka vstoupí do soupravy později než ostatní (její uzel ETBN je aktivován později) nebo se stane nedostupnou (např. díky poruše uzlu ETBN). Dále, stane-li se aktivním stanovištěm strojvedoucího stanoviště na druhém konci vlaku, změní se atributy vlaku, jako jsou směr (vpřed, vzad) a orientace (vpravo, vlevo). Změní se tedy i relativní směr a orientace jednotek a vozů vzhledem ke směru a orientaci vlaku (stejný směr, opačný směr). To znamená, že všechny informace úrovně vlaku vztahující se ke směru nebo orientaci (např. povel strojvedoucího „otevři levé dveře“), musí být na úrovni jednotky přeloženy dle jejího relativního směru a relativní orientace a naopak.

Informace o aktuální topologii vlaku, která zahrnuje pořadí všech uzlů ETBN, směry a orientace, doplněná daty definovanými uživatelem, která popisují vlastnosti jednotlivých jednotek vlaku a funkce v nich implementované, jsou obsaženy v databázi nazvané Train Topology Database (TTDB). Tato databáze je výstupem funkce Inaugurace vlaku (Train inauguration).

Funkce inaugurace je implementována v uzlech ETBN a na její exekuci se podílí všechny aktivní uzly ETBN vlaku s tím, že po provedení inaugurace se v každém z nich nachází jedna instance databáze TTDB. To znamená, že všechny statické i dynamické informace o vlaku, které aplikace potřebují, jsou jim k dispozici lokálně, tj. v ETBN téže jednotky. Specifikace rozhraní pro přístup k těmto informacím, která ale není normativní, je uvedena v normě.

Funkce inaugurace vlaku musí zajistit správnost databáze TTDB ve všech situacích, které mohou za provozu nastat. V případě, že Train Backbone podporuje bezpečnou komunikaci, je tato funkce funkcí se vztahem k bezpečnosti.

Proces inaugurace vlaku musí být ukončen do 1 sekundy. Během tohoto procesu je přerušen přenos aplikačních dat po páteřní síti vlaku. Aplikace se musí s touto situací umět vyrovnat.

**Adresace**

V TCN síti je možné adresovat na síťové úrovni jednotlivá fyzická zařízení a na aplikační úrovni jak fyzická zařízení, tak i logické celky (funkce).

Na síťové úrovni jsou zařízení v TCN síti stejně jako v jiných sítích používajících sadu protokolů TCP/IP adresována IP adresou. Současná verze standardu IEC 61375 pracuje pouze s IP adresami formátu IPv4. Na aplikační úrovni jsou zařízení a funkce adresovány tzv. funkční adresou, která je definována jako URI (Universal Resource Identifier dle RFC3986), což je identifikátor standardně používaný k jednoznačné identifikaci objektů ve světě internetu.

### Síťová adresace v Consist síti

Koncová zařízení mají v rámci Consist sítě pevnou IP adresu. Pevné přiřazení IP adres umožňuje mimo jiné výrobu identických, tj. totožně nakonfigurovaných jednotek (consist). IP adresy mohou být nastavovány přímo na zařízeních nebo přidělovány DHCP serverem umístěným obvykle v komunikačním uzlu TBN. Server je nakonfigurován tak, že danému zařízení přidělí vždy tutéž IP adresu, což je podmínkou k dosažení „plug-and-play“ chování.

### Síťová adresace v Train Backbone

Zařízením v Train Backbone, tj. komunikačním uzlům ETBN, není přidělována pevná IP adresa. Jejich adresy jsou konstruovány tak, že obsahují pořadové číslo příslušného uzlu ETBN, které mu je přiděleno při inauguraci. Tím je zajištěna nutná unikátnost IP adres ETBN uzlů na Train Backbone v celém vlaku.

Vzhledem k tomu, že IP adresy koncových zařízení jsou unikátní pouze v rámci Consist sítě, do které je zařízení připojeno, může ve vlaku existovat více zařízení se stejnou IP adresou. Nelze proto pevně přidělenou IP adresu zařízení přímo použít při komunikaci do jiných jednotek vlaku. Řešením je zavedení adresního prostoru vlakové úrovně. IP adresy koncových zařízení jsou v tomto prostoru konstruovány ze statické IP adresy zařízení v Consist síti a z pořadí jednotky v rámci vlaku. IP adresy zdrojového a cílového zařízení jsou tedy ve zprávách přenášených na Train Backbone vždy z adresního prostoru vlakové úrovně. Jejich překlad na IP adresu v Consist síti a opačně zajišťují uzly ETBN v rámci směrování mezi sítěmi dle překladové tabulky vytvořené při inauguraci.

### Aplikační adresace - funkční adresa

Základní notace URI reprezentujícího funkční adresu je uvedena na obrázku 5.


*Obrázek 5: Notace URI reprezentujícího funkční adresu*

Význam jednotlivých částí identifikující umístění funkce:

- fctdev: identifikuje zařízení, na kterém je funkce umístěna, případně jméno skupinové adresy,
- vehicle: identifikuje vůz,
- consist: identifikuje jednotku (pevnou sestavu vozů),
- cltrain: nepovinná část identifikující pevnou skupinu jednotek označovanou termínem uzavřený vlak[6],
- train: identifikuje vlak; tato část je určena pro identifikaci konkrétního vlaku např. při komunikaci z pozemního systému.

[6] V novém vydání normy IEC 61375 byl zaveden termín uzavřený vlak (closed train) jako vlak sestávající z jedné nebo více jednotek (consist), jehož kompozice se nemění během normálního provozu, například vlak metra, předměstský vlak, vysokorychlostní vlakové jednotky

Část URI identifikující umístění funkce je možné přeložit na IP adresu. Překlad zajišťuje služba TCN-DNS, která je zpravidla umístěna v komunikačním uzlu ETBN. Služba TCN-DNS provádí překlad s využitím databáze TTDB, která je výstupem funkce inaugurace vlaku. Proto je nutné opakovat překlad URI na IP adresu po každé inauguraci. Tuto událost detekuje zařízení na základě změny čísla verze operačního stavu obsaženého v TTDB.

Pro ilustraci uveďme příklad URI reprezentujícího funkční adresu:

trn://diag@vcu.car02.cst01.lTrain – adresátem je funkce diagnostiky v řídicí jednotce (vcu) vozu 2, jednotky 1 vlaku (lTrain značí local Train).

Aby bylo možno adresovat funkce v nově připojené jednotce, aniž by bylo nutné znát její vnitřní strukturu, umožňuje schéma URI adresovat funkce bez znalosti jejich přesného umístění. Čili namísto konkrétního zařízení adresovat například skupinu zařízení daného typu v jednotce nebo všechna zařízení daného vozu / jednotky.

## Architektura distribuovaných aplikací TCMS

Aplikace dálkového řízení v doméně TCMS, tj. řízení v rámci celého vlaku jsou distribuované aplikace. Takovými aplikacemi (funkcemi v terminologii IEC TS 61375-2-4) jsou například řízení dveří, řízení trakce, řízení brzd. Na obrázku 6 jsou znázorněny komponenty generické funkce dálkového řízení a jako příklad je uvedena dekompozice funkce Řízení dveří.

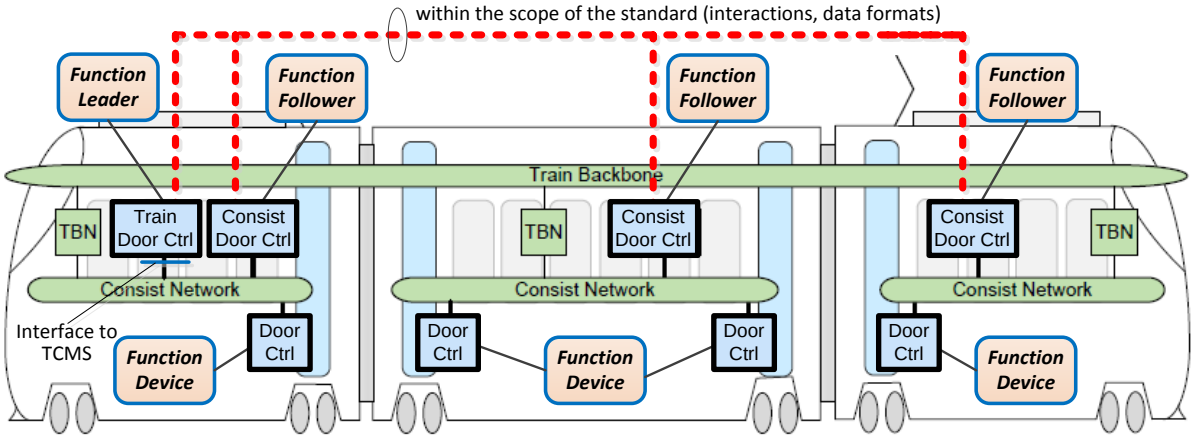
Dle IEC TS 61375-2-4 sestává generická funkce dálkového řízení z komponent s níže uvedenými rolemi.

- Function Leader (řídicí část funkce): poveluje jednotlivé komponenty Function Follower a získává informaci o jejich stavu. Tyto interakce přes Train Backbone a formát vyměňovaných dat jsou standardizovány. Přes rozhraní s TCMS, které ale není standardizováno, je komponenta Function Leader povelována a předává stavovou informaci.
- Function Follower (řízená část funkce): přijímá povely z komponenty Function Leader a zasílá je jedné nebo více komponentám Function Device a v opačném směru předává stavovou informaci kumulovanou ze všech komponent Function Device. Rozhraní ke komponentám Function Device nejsou standardizována, čili Function Follower musí transformovat informaci ze standardizovaného rozhraní k Function Leader do specifického rozhraní k Function Device a naopak.
- Function Device (koncové zařízení funkce): provádí operace definované funkcí a informuje komponentu Function Follower o výsledku.

Role function leader je implementována v jednotkách, které se mohou stát vedoucími jednotkami, čili jsou vybaveny stanovištěm (stanovišti) strojvedoucího. Je-li ve vlaku více takových jednotek, je třeba určit, která z nich je aktuální vedoucí jednotkou. V ní je pak role function leader aktivována. Příslušný mechanismus je definován v komunikačním profilu.

Ve funkci Řízení dveří je komponenta označená na obrázku 6 jako Train Door Ctrl odpovědná za řízení dveří celého vlaku. Plní roli Function Leader a její rozhraní k TCMS ji spojuje například se zařízeními rozhraní strojvedoucího (displej a pult strojvedoucího). Komponenta Consist Door Ctrl je Function Follower a je agentem pro jednu jednotku. Komponenta Door Ctrl je Function Device a ovládá fyzické dveře. Bývá implementována v samostatném zařízení, zatímco komponenty Train Door Ctrl

a Consist Door Ctrl můžeme například najít v displeji strojvedoucího nebo ve VCU.




*Obrázek 6: Architektura distribuovaných aplikací TCMS (Zdroj [6] – modifikováno)*

Je představa, že budoucí verze normy bude specifikovat funkcionalitu „Functional Open Coupling“ (FOC), která umožní spojení dvou nebo více jednotek různých výrobců na základě strojově zpracovatelného popisu funkčních modelů spojovaných jednotek. Každá jednotka musí zveřejnit popis svého funkčního modelu a načíst si popisy funkčního modelu ostatních jednotek vlaku. Nebude nutné prokazovat vzájemnou funkční kompatibilitu jednotek. Homologována bude pouze FOC funkce jednotky, to znamená, že tato jednotka bude kompatibilní se všemi jednotkami s homologovanou FOC funkcí.

## Kybernetická bezpečnost v železničním sektoru

Použití otevřených síťových technologií pro komunikaci palubních systémů s pozemními systémy dopravce i pro jejich komunikaci navzájem, poskytuje příležitost ke kybernetickému útoku na jejich hardware a software s možnými negativními důsledky na zdraví, bezpečnost a životní prostředí (HSE – health, safety, environment) a na finance či reputaci organizace, tj. dopravce.

Požadavky na kybernetickou bezpečnost palubních systémů vlaku se během krátké doby staly nedílnou součástí jejich specifikací. V důsledku novosti problematiky kybernetické bezpečnosti v železničním sektoru a zejména neexistence norem v této oblasti však zainteresované subjekty často neví, jak mají problematiku kybernetické bezpečnosti vůbec uchopit. Následující podkapitoly mají poskytnout čtenáři základní orientaci v této problematice a jsou proto pojaty obecněji.

### Normy pro kybernetickou bezpečnost v železničním sektoru

Významnou pomoc organizacím při zvládání problematiky kybernetické bezpečnosti představují normy. Zatímco oblast IT systémů je v tomto směru ve velké míře pokryta, oblast průmyslových řídicích systémů stále ještě na dokončení své normy

čeká. Bude jí souborná norma IEC 62443[7], která je vytvářena s cílem aplikovatelnosti ve většině průmyslových sektorů. Některé z jejích 13 částí již byly publikovány, zbylé jsou ve stádiu návrhu.

Norma IEC 62443 by se měla stát normou, ze které budou odvozovány normy pro kybernetickou bezpečnost v jednotlivých průmyslových sektorech. Takové postavení má například norma IEC 61508 v oblasti funkční bezpečnosti. Z ní byl pro železniční sektor odvozen soubor standardů obsahující normy EN 50126, EN 50129, EN 50128, který byl pro pokrytí problematiky bezpečných komunikací (ve smyslu safety) doplněn o normu EN 50159.

Kybernetická bezpečnost je v železničním sektoru v současné době jedním z prioritních témat. Je například významným tématem v projektech CONNECTA (CONtributing to Shift2Rail's NExt generation of high Capable and safe TCMS and brAkes), SAFE4RAIL (SAFE architecture for Robust distributed Application Integration in roLling stock) a X2Rail-1 (Start-up activities for Advanced Signalling and Automation Systems) a hlavním tématem projektu CYRail (Cybersecurity in the RAILway sector), které jsou řešeny v rámci Shift2Rail[8]. V rámci UNIFE byla ustavena technická pracovní skupina Cyber-Security jako platforma pro spolupráci členů této organizace v oblasti kybernetické bezpečnosti. Výsledky těchto a dalších aktivit se promítnou do budoucích norem vztahujících se ke kybernetické bezpečnosti v železničním sektoru. Za první významný výsledek lze považovat shodu na normě IEC 62443 jako „master“ normě pro železniční sektor.

**Charakteristika normy IEC 62443**

Norma IEC 62443 definuje pojem „průmyslové automatizační a řídicí systémy (Industrial Automation and Control Systems – IACS)“ jako soubor pracovníků, hardwaru a softwaru podílejících se na monitorování, ovládání či řízení průmyslového procesu, přičemž tyto elementy mohou narušit nebo ovlivnit jeho bezpečnost (ve smyslu safety i security) a spolehlivost. IACS zahrnují nejen řídicí systémy pro základní úroveň řízení a dispečerské řízení, ale i přidružené informační systémy. Norma vychází ze zavedených norem pro bezpečnost univerzálních IT systémů (např. z norem řady ISO/IEC 27000), identifikuje specifika IACS a na ně se zaměřuje. Většina těchto specifik vyplývá ze skutečnosti, že bezpečnostními riziky v IACS jsou také rizika poškození zdraví, snížení bezpečnosti (ve smyslu safety) a poškození životního prostředí. Vzhledem k tomu, že stejná rizika pocházejí i z oblasti bezpečnosti (ve smyslu safety), je například třeba integrovat postupy hodnocení rizik zavedené v těchto dvou sice samostatných, ale z pohledu návrhu bezpečného systému překrývajících se oblastech.

Rozdílnost mezi IT systémy a IACS je i v prioritách bezpečnostních cílů. Bezpečnost v IT systémech se tradičně zaměřuje na dosažení tří cílů - důvěrnosti, integrity a dostupnosti, které jsou často označovány akronymem CIA. Pro typický podnikový systém klade bezpečnostní strategie na první místo důvěrnost spolu s řízením přístupu, které ji umožňuje dosáhnout. Po ní následují integrita a dostupnost, která má nejnižší prioritu.

[7] Norma IEC 62443 byla původně vytvořena jako ANSI/ISA-99 organizací ISA (International Society for Automation) a publikována ANSI (American National Standard Institute) jako norma. Poté byla převzata IEC jako IEC 62443. Nové verze jsou též vytvářeny v ISA a přebírány IEC.

[8] Informace o uvedených projektech jsou dostupné ze stránky www.shift2rail.org.

V oblasti IACS je priorita těchto cílů většinou odlišná. Následky nedostupnosti komponent systému mohou mít na řízený technologický proces největší dopad. Dostupnosti je tedy dávána nejvyšší priorita. Data jsou vesměs přenášena v „surové“ formě, a aby měla pro útočníka hodnotu, musela by být analyzována v kontextu. Důvěrnosti je proto obvykle přiřazena nejnižší priorita. Příklad, kdy tomu tak není, je například správa klíčů. Zde je důvěrnost prioritou jak pro IT systémy, tak pro IACS.

Specifickým požadavkem pro systémy IACS je také požadavek, aby aplikovaná bezpečnostní protiopatření nevyřadila tzv. esenciální funkce systému, tj. funkce, jejíž selhání znamená ohrožení zdraví, bezpečnosti, životního prostředí nebo dostupnosti řízených zařízení. Identifikace těchto funkcí je jedním z hlavních úkolů bezpečnostní analýzy systému.

Norma IEC 62443 je soubor specifikací, pokynů a osvědčených postupů týkajících se kybernetické bezpečnosti určený subjektům, které ve vztahu k IACS plní jednu ze tří níže uvedených rolí.

- Vlastník systému: je zodpovědný za IACS, to znamená za jeho specifikaci, provozování a údržbu, vyřazení z provozování. Zde se norma zaměřuje na vytvoření a údržbu efektivního systému řízení bezpečnosti v organizaci. Elementy tohoto systému jsou mimo jiné politiky, standardy, procedury a směrnice, které definují určitá závazná pravidla a postupy, tj. elementy reprezentující administrativní bezpečnostní protiopatření.
- Integrátor systému: integruje IACS z jednotlivých produktů, připravuje jej pro nasazení v konkrétním prostředí (vytváří tzv. řešení) a uvádí jej do provozu. Zde norma poskytuje návod pro návrh systému s požadovanou úrovní bezpečnosti a specifikuje soubor bezpečnostních požadavků na systém. Bezpečnostní analýza určí ty, které musí být pro daný systém splněny.
- Dodavatel produktů: jeho úlohou je vývoj, výroba, údržba a vyřazení produktů, tj. komponent (např. zařízení, subsystémy) použitých v IACS. Norma specifikuje soubor bezpečnostních požadavků na komponenty a uvádí pokyny a osvědčené postupy týkající se jejich vývoje.

Jak je patrné z výše uvedeného, postihuje norma celý bezpečnostní životní cyklus IACS.

Norma definuje pojem úroveň bezpečnosti (security level – SL) jako měřítko důvěry, že IACS je prost zranitelností, které by útočník mohl využít, a že se chová tak, jak bylo zamýšleno. K dosažení vyšší úrovně bezpečnosti – jsou definovány 4 úrovně (SL1 až SL4) – je třeba splnit náročnější bezpečnostní požadavky. Norma poskytuje dva seznamy bezpečnostních požadavků, jeden pro systém a druhý pro komponenty. Tyto seznamy jsou strukturovány dle jednotlivých aspektů bezpečnosti do sedmi kategorií nazvaných Foundational Requirements. Jsou jimi: identifikace a autentikace, řízení použití (autorizace), integrita systému, důvěrnost dat, omezení datových toků, včasná odpověď na událost a dostupnost zdrojů. Pro každý požadavek je uvedeno, pro které úrovně bezpečnosti musí být splněn.

Požadavky kategorie „omezení datových toků“ jsou požadavky na segmentaci systému do zón a tzv. conduitů, čili požadavky na protiopatření, která jsou realizována na úrovni architektury systému. Vzhledem k tomu, že architektura systému je předmětem tohoto článku, je segmentaci systému věnována následující podkapitola.

**Segmentace systému, bezpečnostní zóny**

V rozsáhlých a složitých systémech, mezi něž palubní elektronický „ekosystém“ bezesporu náleží, není zpravidla nutné aplikovat stejnou úroveň bezpečnosti na všechny komponenty. Metoda vyžadovaná normou IEC 62443 pro řešení bezpečnosti v systémech s více požadovanými úrovněmi bezpečnosti je segmentace systému do zón a jejich propojení tzv. conduity. Jsou tedy definovány dva koncepty:

- Zóna: je logické nebo fyzické seskupení fyzických, informačních a aplikačních elementů, které sdílí společné bezpečnostní požadavky; má jasně stanovené hranice, takže je možné jednoznačně určit, který element do zóny patří a který ne,
- Conduit: je spoj pro tok informací mezi dvěma zónami; poskytuje bezpečnostní funkce, které umožňují zónám bezpečně komunikovat.

Jakákoliv komunikace mezi zónami musí být vedena přes conduit. Conduity řídí přístup do zón, brání zónu proti DoS útokům nebo přenosu škodlivého softwaru (malware), zajišťují ochranu integrity a důvěrnosti přenášených dat. Protiopatření realizovaná conduitem jsou typicky zaměřena na vyrovnání rozdílu mezi požadovanou úrovní bezpečnosti zóny a úrovní, kterou je zóna schopna zajistit. Vyrovnat tento rozdíl protiopatřeními realizovanými v conduitu je obvykle významně levnější než zvyšovat úroveň bezpečnosti každého zařízení zóny.

Norma IEC 62443 požaduje posuzování bezpečnostních rizik na dvou úrovních. Na první úrovni se posuzování provádí pro systém jako celek s cílem identifikovat rizika pro organizaci, která vyplývají z nejhorších případů kompromitování systému. Na základě výsledků tohoto vysokoúrovňového posouzení jsou určeny zóny a conduity. Poté je provedeno detailní posouzení rizik každé zóny a každého conduitu. Výsledkem je soubor protiopatření a korespondujících bezpečnostních požadavků.

V článku uvedená vysokoúrovňová architektura kompletního palubního systému respektuje požadovanou segmentaci systému. Každá z funkčních domén (TCMS, OOS, COS) je bezpečnostní zónou. Propojeny jsou, jak je znázorněno na obrázku 1, conduity obsahujícími například zařízení typu firewall nebo aplikační brána. Zvláštní zónu tvoří subsystémy realizující funkce se vztahem k bezpečnosti. Ta je podzónou zóny TCMS se samostatným segmentem sítě TCN.

## Závěr

Prezentovanou architekturu palubního elektronického „ekosystému“ vlaku, jejímž klíčovým elementem je vlaková komunikační síť TCN, lze považovat za standardizovanou architekturu palubního elektronického „ekosystému“ moderního vlaku současnosti i blízké budoucnosti. V rámci inovačního programu IP1 iniciativy Shift2Rail nazvaném „Cost-efficient and reliable trains, including high-capacity trains and high-speed trains“ jsou však již řešeny projekty zaměřené na inovaci TCMS a tedy i palubní vlakové sítě. Za hlavní inovační témata lze označit:

- rozšíření vlakové komunikační sítě o bezdrátové sítě,
- realizace konceptu „drive-by-data“,
- specifikace funkcionality „Functional Open Coupling“ (FOC).

Budoucí síť TCN bude možno realizovat jako kombinaci drátových a bezdrátových sítí, přičemž bezdrátově bude možné realizovat jak Consist síť, tak i páteřní síť vlaku.

Bezdrátové spojení jednotek vlaku umožní odstranit fyzické komunikační rozhraní ve spřáhlech jednotek.

Koncept „drive-by-data“ vyžaduje, aby vlaková komunikační síť zajistila v rámci celého vlaku bezpečnou komunikaci pro funkce s úrovní integrity bezpečnosti 4 (SIL 4). Nebude tak třeba, aby tyto funkce nadále používaly jim vyhrazené drátové vodiče.

Funkcionalita FOC představuje nový přístup k interoperabilitě aplikací vlaku. Podrobněji byla popsána v kapitole Architektura distribuovaných aplikací TCMS.

Použití bezdrátových sítí nejen pro komunikaci s pozemními systémy, ale i uvnitř vlaku a realizace bezpečné komunikace SIL 4 se také projeví ve zvýšení požadované úrovně kybernetické bezpečnosti v dotčených zónách palubního elektronického „ekosystému“.

## Literatura:


[1] ČSN EN 15380-4, Železniční aplikace – Systém označování železničních vozidel – Část 4: Funkční skupiny, 2013

[2] ČSN EN 61375-1, Elektronická drážní zařízení - Vlaková komunikační síť (TCN) - Část 1: Obecná architektura, 2013

[3] ČSN EN 61375-2-1, Elektronická drážní zařízení - Vlaková komunikační síť (TCN) - Část 2-1: Vlaková sběrnice (WTB), 2013

[4] ČSN EN 61375-2-2, Elektronická drážní zařízení - Vlaková komunikační síť (TCN) - Část 2-2: Zkoušky shody vlakové sběrnice, 2013

[5] ČSN EN 61375-2-3, Elektrické drážní zařízení - Vlaková komunikační síť (TCN) - Část 2-3: TCN komunikační profil, 2016

[6] IEC TS 61375-2-4, Electronic railway equipment - Train communication network (TCN) - Part 2-4: TCN application profile

[7] ČSN EN 61375-2-5, Elektrické drážní zařízení - Vlaková komunikační síť - Část 2-5: ETB - Páteřní vlaková síť Ethernet, 2015

[8] IEC 61375-2-6 [working document at CDV stage], Electronic railway equipment - Train communication network - Part 2-6: On-board to ground communication

[9] IEC TR 61375-2-7, Electronic railway equipment - Train communication network (TCN) - Part 2-7: Wireless Train Backbone

[10] IEC 61375-2-8 [working document at initial stage],
Electronic railway equipment - Train communication network (TCN) - Part 2-8: TCN conformance test

[11] ČSN EN 61375-3-1, Elektronická drážní zařízení - Vlaková komunikační síť (TCN) - Část 3-1: Multifunkční vozidlová sběrnice (MVB), 2013

[12] ČSN EN 61375-3-2, Elektronická drážní zařízení - Vlaková komunikační síť (TCN) - Část 3-2: Zkoušky shody MVB (Multifunkční vozidlová sběrnice), 2013

[13] ČSN EN 61375-3-3, Elektronická drážní zařízení - Vlaková komunikační síť (TCN) - Část 3-3: Síť sestavy CANopen (CCN), 2013

[14] ČSN EN 61375-3-4, Elektronická drážní zařízení - Vlaková komunikační síť (TCN) - Část 3-4: Síť Ethernet (ECN), 2014

[15] ČSN EN 62580-1, Elektronická drážní zařízení - Palubní multimediální a telematické subsystémy pro dráhy - Část 1: Obecná architektura, 2017

[16] IEC TS 62580-2, Electronic railway equipment - On-board multimedia and telematic subsystems for railways - Part 2: Video surveillance/CCTV services

[17] UIC 556 Ed.5: Information transmission in the train (train bus), UIC 2009

[18] ČSN EN 50159, Drážní zařízení - Sdělovací a zabezpečovací systémy a systémy zpracování dat - Komunikace v přenosových zabezpečovacích systémech, 2011

[19] ČSN EN 50126-1, Drážní zařízení - Stanovení a prokázání bezporuchovosti, pohotovosti, udržovatelnosti a bezpečnosti (RAMS), 2001

[20] ČSN EN 50129, Drážní zařízení - Sdělovací a zabezpečovací systémy a systémy zpracování dat - Elektronické zabezpečovací systémy, 2003

[21] ČSN EN 50128 ed. 2, Drážní zařízení - Sdělovací a zabezpečovací systémy a systémy zpracování dat - Software pro drážní řídicí a ochranné systémy, 2012

[22] ISA-62443-1-1, Security for Industrial Automation and Control Systems, Terminology, Concepts, and Models, Draft 2, 2016

[23] Projekt Roll2Rail, D2.1 Specification of the Wireless TCMS. Dostupný z: www.roll2rail.eu

[24] ČSN EN 62625-1, Systém palubního záznamu jízdních dat - Část 1: Specifikace systému, 2014

[25] ČSN EN 61784-3, Průmyslové komunikační sítě - Profily - Část 3: Funkční bezpečnost sběrnic pole - Obecná pravidla a definice profilů

## Seznam zkratek:

| | |
|---|---|
| ALG | Application Layer Gateway (brána aplikační vrstvy) |
| ANSI | American National Standard Institute |
| CAN | Controller Area Network |
| CENELEC | Comité Européen de Normalisation Électrotechnique (European Committee for Electrotechnical Standardization) |
| CIA | Confidentiality, Integrity, Availability |
| CN | Consist Network (consist síť) |
| COS | Customer Oriented Services |
| CS | Consist switch |
| DHCP | Dynamic Host Configuration Protocol |
| DNS | Domain Name Server |
| ECN | Ethernet Consist Network |
| ECR | Ethernet Consist Ring |
| ED | End Device |
| ETB | Ethernet Train Backbone |
| ETBN | Ethernet Train Backbone Node |
| FOC | Functional Open Coupling |
| IACS | Industrial Automation and Control Systems |
| IEC | International Electrotechnical Commission, Geneva |
| IEEE | Institute of Electrical and Electronics Engineers, New York |
| IETF | Internet Engineering Task Force |
| IP | Internet Protocols, definovány IETF |
| ISA | International Society for Automation |
| ISO | International Standard Organisation, Geneva |
| IT | Informační technologie |
| LTE | Long Term Evolution |
| MCG | Mobile Communication Gateway (mobilní komunikační brána) |
| MD | Message Data |
| MVB | Multifunction Vehicle Bus |
| OOS | Operator Oriented Services |
| OSI | Open System Interconnection, obecný komunikační model definovaný v ISO/IEC 7498-1 |

| | |
|---|---|
| PD | Process Data |
| PDU | Protocol Data Unit |
| RFC | Request For Comments, Internetové standardy vydané IETF |
| RTP | Real Time Protocol |
| SDTv2 | Safe Data Transmission version 2 |
| SIL | Safety Integrity Level |
| TB | Train Backbone |
| TC | Technical Committee |
| TR | Technical Report |
| TS | Technical Specification |
| TBN | Train Backbone Node |
| TCMS | Train Control and Monitoring System |
| TCN | Train Communication Network |
| TCP | Transmission Control Protocol |
| TRDP | Train Real Time Data Protocol |
| TTDB | Train Topology Database |
| UDP | User Datagram Protocol |
| UIC | International Union of Railways, the international railways operators association |
| UNIFE | Union of European Railway Industries |
| URI | Uniform Resource Identifier, definován IETF |
| VCU | Vehicle Control Unit |
| VLAN | Virtual Local Area Network |
| WG | Working Group |
| WLTB | Wireless Train Backbone |
| WTB | Wire Train Bus |

Praha, říjen 2017

Lektorovali: Dr. Ing. Ivo Myslivec
AŽD Praha s.r.o.

RNDr. Libor Forst
Univerzita Karlova, MFF