Vysoká škola logistiky o.p.s.

Bezpečnostní aspekty informačních technologií v železniční osobní dopravě

(Diplomová práce)

Přerov 2022 **Bc. Václav Nebeský, LL.M.**

Vysoká škola logistiky o.p.s.

Zadání diplomové práce

student	**Bc. Václav Nebeský**
studijní program	Logistika

Vedoucí Katedry magisterského studia Vám ve smyslu čl. 22 Studijního a zkušebního řádu Vysoké školy logistiky o.p.s. pro studium v navazujícím magisterském studijním programu určuje tuto diplomovou práci:

Název tématu: **Bezpečnostní aspekty informačních technologií v železniční osobní dopravě**

Cíl práce:

Na základě provedené analýzy informačních systémů v železniční osobní dopravě zpracovat návrhy řešení, které povedou ke zvýšení kybernetické bezpečnosti v dané oblasti. Navrhovaná řešení vyhodnotit.

Zásady pro vypracování:

Využijte teoretických východisek oboru logistika. Čerpejte z literatury doporučené vedoucím práce a při zpracování práce postupujte v souladu s pokyny VŠLG a doporučeními vedoucího práce. Části práce využívající neveřejné informace uveďte v samostatné příloze.

Diplomovou práci zpracujte v těchto bodech:

Úvod
1. Teorie bezpečnosti v informačních technologiích
2. Právní rámec kybernetické bezpečnosti
3. Analýza informačních systémů v železniční osobní dopravě
4. Telekomunikace a přenos dat
5. Návrh řešení ICT bezpečnosti a jeho vyhodnocení

Závěr

Rozsah práce: 55 – 70 normostran textu

Seznam odborné literatury:

GÁLA, Libor, POUR, Jan a Zuzana ŠEDIVÁ. Podniková informatika: počítačové aplikace v podnikové a mezipodnikové praxi. 3., aktualizované vydání. Praha: Grada Publishing, 2015. ISBN 978-80-247-5457-4.

GAŠPARÍK, Jozef a Jiří KOLÁŘ. Železniční doprava: technologie, řízení, grafikony a dalších 100 zajímavostí. Praha: Grada Publishing, 2017. ISBN 978-80-271-0058-3.

KOLOUCH, Jan a Pavel BAŠTA. CyberSecurity. Praha: CZ.NIC, z.s.p.o., 2019. ISBN 978-80-88168-31-7.

Vedoucí diplomové práce: prof. Ing. Václav Cempírek, Ph.D., DBA

Datum zadání diplomové práce: 31. 10. 2021
Datum odevzdání diplomové práce: 12. 5. 2022

Přerov 31. 10. 2021

Ing. Blanka Kalupová, Ph.D.
vedoucí katedry

prof. Ing. Václav Cempírek, Ph.D.
rektor

Čestné prohlášení

Prohlašuji, že předložená diplomová práce je původní a že jsem ji vypracoval samostatně. Prohlašuji, že citace použitých pramenů je úplná a že jsem v práci neporušil autorská práva ve smyslu zákona č. 121/2000 Sb. o autorském právu, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon) ve znění pozdějších předpisů.

Prohlašuji, že jsem byl také seznámen s tím, že se na mou diplomovou práci plně vztahuje zákon č. 121/2000Sb., o právu autorském, právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon), ve znění pozdějších předpisů, zejména § 60 – školní dílo. Beru na vědomí, že Vysoká škola logistiky o.p.s. nezasahuje do mých autorských práv užitím mé diplomové práce pro pedagogické, vědecké a prezentační účely školy. Užiji-li svou diplomovou práci nebo poskytnu-li licenci k jejímu využití, jsem si vědom povinnosti informovat předtím o této skutečnosti prorektora pro vzdělávání Vysoké školy logistiky o.p.s.

Prohlašuji, že jsem byl poučen o tom, že diplomová práce je veřejná ve smyslu zákona č. 111/1998 Sb., o vysokých školách a o změně a doplnění dalších zákonů (zákon o vysokých školách), ve znění pozdějších předpisů, zejména § 47b. Taktéž dávám souhlas Vysoké škole logistiky o.p.s. ke zpřístupnění mnou zpracované diplomové práce v její tištěné i elektronické verzi. Souhlasím s případným použitím této práce Vysokou školou logistiky o.p.s. pro pedagogické, vědecké a prezentační účely.

Prohlašuji, že odevzdaná tištěná verze diplomové práce, elektronická verze na odevzdaném optickém médiu a verze nahraná do informačního systému jsou totožné.

V Roztokách, dne 18. 08. 2022

.....
podpis

Poděkování

Rád bych tímto poděkoval vedoucímu diplomové práce panu prof. Ing. Václavovi Cempírkovi, Ph.D., DBA za trpělivý a skvělý přístup.

Rovněž bych rád poděkoval svým kolegům informatikům i dopravákům za cenné rady a možnost se učit i z praxe.

V neposlední řadě bych rád poděkoval své ženě Olze a dceři Viktorce, a to za trpělivost a podporu.

Anotace

Železniční doprava jako průmyslové odvětví ve stále větší míře využívá prvky informačních technologií, digitalizace a automatizace. S jejich rychlejším a širším nástupem nepřichází pouze výhody, ale i hrozby, zejména pak z pohledu kybernetické bezpečnosti. Bezpečnostní aspekty se netýkají pouze dopravce samotného, ale i jeho digitálních, tzn. datových a komunikačních vazeb s dalšími rolemi v železničním systému (např. s manažerem infrastruktury nebo s cestujícími). Informační technologie pronikají i do segmentu železničních vozidel.

Klíčová slova

Informační systém, kybernetická bezpečnost, digitalizace, rozhraní, železniční dopravce, manažer infrastruktury, dopravní telematika, architektura informačního systému, penetrační testy, komunikační jednotka, sítě, průmyslový počítač.

Annotation

Railway transport as part of industry sector uses more elements of information technology, digitalization and automatization. Faster and biger advent of this technology does not bring only benefits, with them come threats especially from point of view cybersecurity. The security aspects does not concern the railway carrier itself, but his digital (its mean data and communications relations) with other roles in ralways system (for example realationship with passangers or infrastructure manager). Information technology come through the segment of railways vehicles.

Keywords

Information system, cyber security, digitalization, interface, railways carrier, infrastructure manager, transport telematics, information system architecture, penetration testing, communication unit, industrial computer.

Obsah

Úvod

Informační technologie se stávají naprosto běžnou součástí každodenního života. Tak běžnou, že ani její uživatelé nevnímají, že se pracují s informatikou, počítači. Informatika se tak nenásilnou, nenápadnou a postupnou formou stala naprostou rutinou. Když ještě v devadesátých letech minulého století probíhala údržba železničních vozidel v depech, málo kdo by tušil, že zanedlouho bude k jejich kolegům patřit informatik. I dnes, když velcí železniční dopravci tvoří zadání na výrobu nebo dodání železničního vozidla, ve spoustě případů opakují jednu a tu samou chybu – na vozidlo se dívají očima konstruktéra, mechanika, ale IT odborník stále chybí. Přitom vozidla (železniční, silniční) jsou dnes v zásadě souborem jezdících sad počítačů. Ještě víc se tento trend projevuje v letecké dopravě.

S příchodem a rozšířením počítačů do vozidel a dopravy obecně ovšem přichází i nutnost bránit informační systémy a jejich komponenty. Každý čip, port, kód softwarového díla, zkrátka každá informatická část, není jen vítaným pomocníkem, který řídí proces, vypočítává potřebné údaje nebo zajišťuje komunikaci, ale zároveň je slabým místem, které se dá napadnout nebo zneužít. Obecně se dá říci, že lidstvo hrozby podceňuje vždy do té doby, než se nějaká naplní. Při masivnějším příchodu informatiky do kancelářského prostředí bylo např. podceňováno nasazování antivirových programů nebo zálohování dat. V té době vznikl jeden z „informatických vtipů“, který bohužel odrážel smutnou realitu, a sice že „uživatelé počítačů se dělí na dvě skupiny: ty, co o data teprve přijdou a ty, co už od data přišli.“ Pochopitelně ta druhá skupina, po bolestivé zkušenosti, poctivě zálohuje a brání se všemi dostupnými prostředky. Zajímavé je, že tento přístup se znovu a znovu opakuje v prostředí, kde dřív informatika nehrála žádnou nebo alespoň ne významnou roli – zkrátka nepoučení z chyb nás provází vždy a všude.

S rozšířením informatiky dochází ještě k jednomu zásadnímu jevu, a to k budování komplexních systémů. Jednotlivé speciální programy jsou dnes provázány mezi sebou, dochází k výměně velkého množství dat. Na tyto systémy jsou navázána různá čidla, snímače a další příslušenství. Takto komplexně vybudovaný systém má z podstaty věci více slabých míst a celkově je tedy zranitelnější. Proto jeho obrana musí být logicky také komplexnější, sofistikovanější. S příchodem těchto informačních systémů přichází i jejich testování z pohledu bezpečnosti – řízeným způsobem simulovaný útok na systém

s cílem otestovat jeho odolnost nebo odkrýt slabá místa, která jsou po takovém testování neprodleně opravena a posílena.

Informační systémy v dopravě představují zvláštní kategorii. Systémy už řadu let obsluhují zázemí dopravy, jako jsou dispečerská pracoviště, prodeje jízdenek, jízdní řády apod., nicméně informatika se dostává i na vozidla – např. ve formě informačních systémů pro cestující, mobilních přenosných pokladen nebo řídících počítačů ovládající trakční motory, brzdy či klimatizace.

Tato diplomová práce má proto za cíl zanalyzovat informační systémy v dopravě, a vypracovat návrhy řešení, které povedou ke zvýšení kybernetické bezpečnosti v této oblasti. Navrhovaná řešení pak na závěr budou vyhodnocena.

Aby byla tato práce co nejvíce konkrétní a výsledky se daly využít i v praxi, byl rozsah práce zúžen na železniční osobní dopravu. Důvod tohoto zúžení je jednoduchý – doprava celkově jako obor je velmi obsáhlá a analýza a následný návrh by byl velmi povrchní. Volba na železniční osobní dopravu padla z důvodu předchozí praxe autora této práce.

Co se týká odborné literatury, bude použita literatura zaměřená na železniční dopravu, logistiku, informační a telekomunikační technologie a kybernetickou bezpečnost. Literatury, která by propojila výše uvedené problematiky, není bohužel v současné době mnoho k dispozici, jedná se spíše o odborné články než o publikace. Kybernetická bezpečnost v dopravě je svým způsobem řešena i rámci problematiky tzv. Smart Cities.

Vlastní diplomová práce bude nejdříve analyzovat jednotlivé pohledy na informační systémy (např. technický, technologický, právní apod.), na základě kterých pak bude zpracován vlastní soubor návrhů pro kybernetickou bezpečnost v železniční osobní dopravě.

1 Základy a teorie bezpečnosti v informačních technologiích

1.1 Definice zásadních pojmů a principů informačních systémů

Pro naplnění cílů této diplomové práce je na začátek nutné stanovit zásadní pojmy a principy informačních technologií (dále „IT“). Nebude se však jednat o základní nebo encyklopedický popis jednotlivých komponent a funkcí, naopak, pro další se předpokládá obecná znalost informatiky a jejího názvosloví.

Nejen v železniční dopravě jsou informační systémy (dále jen „IS“), popř. soubory IS, stavěny klasickým modelem s třemi základními úrovněmi [1]:

1. hardware (dále jen „HW“), popř. platforma pro vlastní provoz IS nebo jeho části,
2. operační systém (dále jen „OS“), popř. prostředí, které je provozováno na HW a slouží pro běh další úrovně, která je (popř. jsou)
3. aplikace, které zabezpečují zpracování, ukládání, interpretaci, odesílání nebo přijímání (komunikaci) dat.

Obecný model IS je znázorněn na schématu č. 1.1.

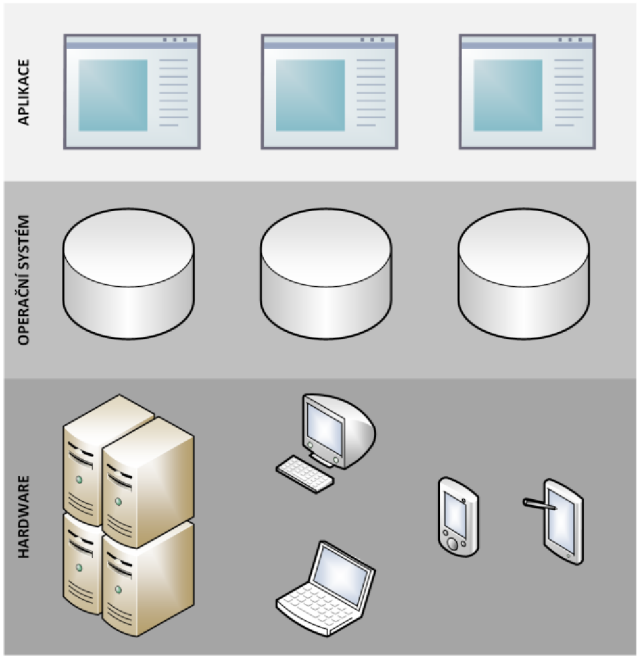


Schéma 1.1 Obecný model IS

Zdroj: vlastní zpracování

Jednotlivé vrstvy základního modelu IS mohou obsahovat nebo naopak mohou být doplněny dalšími komponentami, zejména pak:

1. databází (dále jen „DB“), popř. jiným jednoduchým nebo sofistikovaným úložištěm dat,
2. speciálními aplikacemi, které např. zabezpečují podpůrné funkcionality pro hlavní aplikace (označované též jako middleware, dále jen „MW“),
3. integračními komponentami (např. sběrnicemi nebo řídícími prvky),
4. komunikačními komponentami (např. směrovači, přístupovými body apod.),
5. a dalšími možnými komponentami.

Vlastní řešení, na bázi výše popsaného modelu IS, může být různě modifikováno dle konkrétních řešení, a nemusí se vždy nutně jednat o fyzické řešení. Typickým příkladem je virtualizace, kdy jsou zejména části HW (např. server) nahrazeny speciální aplikací, která emuluje HW (vzniká pak např. virtuální server). V rámci některých řešeních jsou na počítačích spuštěny tzv. virtuální stroje, které emulují jiný počítač, ačkoliv primární počítač i virtuální stroj jsou v provozu na jednom a tom samém HW, přičemž každý z těchto počítačů zpravidla využívá jiný OS.

Obecný popis funkce klasického modelu IS spočívá v tom, že:

1. IS je fyzicky nebo virtuálně umístěn na HW, který poskytuje prostřednictvím OS prostředí pro běh aplikací,
2. do tohoto prostředí jsou nahrány aplikace, které vykonávají požadované funkce; mezi nejzásadnější patří práce s daty (sběr, zpracování, interpretace),
3. aplikace ukládají data do DB nebo po primárním zpracování odesílají do jiného IS či úložiště k dalšímu zpracování či archivaci.

Důležitým aspektem (který je z určitého úhlu pohledu i součástí IS) je personál, tedy lidský činitel, který aplikace obsluhuje a využívá datové výstupy pro další práci. Současným trendem je bezpochyby automatizace, tzn. automatický sběr a zpracování dat bez lidského činitele, nicméně lidský faktor nikdy z tohoto řetězce nevypadne, protože:

1. personál se stará i o nastavení a údržbu IS (nejedná se o klasické uživatele IS, ale např. o administrátory IS),
2. i po automatickém zpracování dat je na konci tohoto řetězce uživatel člověk.

V rámci automatizace IS se začíná využívat umělá inteligence, vč. tzv. strojového učení, kdy vlastní aplikace nemá v sobě popsány (nakódovány) všechny potřebné funkce pro

práce s daty, ale naopak obsahuje kód, kterým se aplikace sama doplňuje, a tak se vlastně učí zpracovávat nová data a nové postupy. Využití umělé inteligence v dopravě je dnes zejména v oblasti vytěžování dat (např. z papírových zdrojů), pro jednoduchou komunikaci (např. chat na webových stránkách se zákazníky) nebo jako „našeptávač“ v rámci různých aplikací (kdy aplikace doporučuje uživateli např. nějaký postup nebo zadání hodnoty pro další práci s daty). Ačkoliv už existují IS s využitím umělé inteligence pro řízení dopravy, které by přinesly skutečnou automatizaci dopravních procesů, není tato oblast v praxi příliš využívána, a to z důvodu:

1. poměrně velké chybovosti (např. autonomní řízení automobilů za pomoci umělé inteligence mají poměrně vysoké procento nehodovosti) a
2. nejasná otázka právní odpovědnosti za skutky, které by byly zapříčiněny umělou inteligencí – jinými slovy, kdo by byl odpovědný za nehodu vozidla, které bylo řízeno za pomoci nebo jen prostřednictvím umělé inteligence.

Právní aspekty odpovědnosti za dopady způsobené umělou inteligencí jsou řešeny – zatím bez aplikovatelného v praxi použitelného výsledku – na úrovni Evropské komise [2].

V případě spojení IT s telekomunikačními technologiemi je řešení komplexnější a pak je označováno jako informační a komunikační technologie (dále jen ICT). Řešení ICT je typickým představitelem dopravních telematických systémů pro dopravu, kdy:

1. první část IS je provozována na serverech (počítačích) s obsluhou „od stolu“ (např. dispečerské pracoviště, pracoviště s kancelářskou agendou apod.), v tomto případě se jedná o tzv. stacionární část IS,
2. druhá část IS systému je provozována na mobilní platformě, ať už se jedná o mobilní telefony či podobné (např. přenosné počítače PDA) platformy, nebo o průmyslové počítače, které jsou součástí vozidel a umožňují sběr dat a provoz aplikací. V tomto případě se jedná o mobilní část IS.
3. Mezi stacionární a mobilní částí IS probíhá datová komunikace, a to pomocí přenosových zařízení a telekomunikační sítí. Tato komunikace se označuje také jako „přenosová cesta“. Propojením obou částí IS za pomoci přenosové cesty vznikne systém kategorie ICT.

Na jednotlivé části ICT systému mohou být napojeny další zařízení a technologie, které nejsou samy o sobě IS, ale jsou jejich velmi funkčním doplňkem:

1. čidla, snímače apod. Jedná se většinou o jednoduchá zařízení, která data pouze sbírají a přeposílají je ke zpracování nebo zobrazení do logické části IS,
2. zobrazovací jednotky, jako např. informační tabule, monitory nebo signalizační zařízení,
3. další pomocné zařízení, jako např. síťové prvky, sběrnice, speciální boxy (např. uzemněné, odolné vůči teplotám nebo magnetické síle).

Model dopravních ICT systémů (řešení) je graficky znázorněn na schématu č. 1.2.

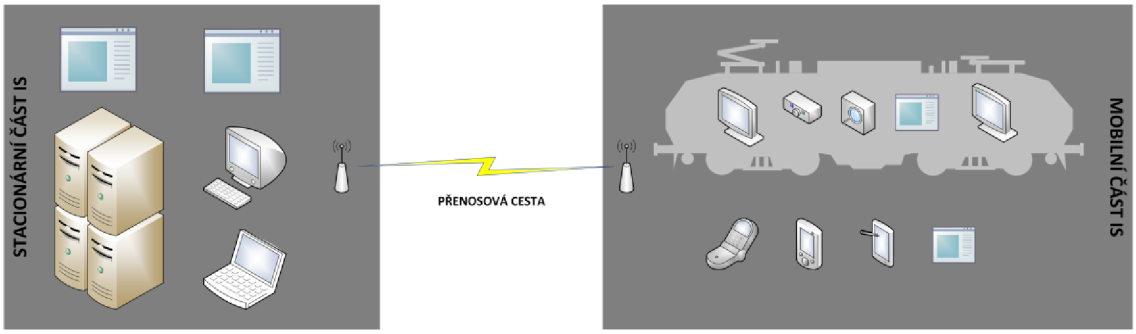


Schéma 1.2 Model dopravních ICT řešení
Zdroj: vlastní zpracování

1.2 Životní cyklus informačního systému a specifika jednotlivých fází

Pro další práci s IS (ICT), zejména pak s ohledem na bezpečnostní aspekty, je nutné rozeznávat, v jakém stádiu životního cyklu se IS nachází.

Obecně odborná literatura rozeznává 3 (tři) etapy životního cyklu IS [1], a sice:

1. vybudování IS,
2. provoz IS,
3. zrušení IS.

Tyto fáze životního cyklu jsou rozepsány v dalších podkapitolách.

1.2.1 Vybudování informačního systému

Na začátku úvahy o IS je záměr o jeho vybudování, většinou ve formě investičního záměru nebo důvodové zprávy, která stanovuje, za jakým účelem se má IS postavit, jaké budou jeho funkcionality a přínosy. Pro detailnější zadání stavby IS je nezbytný procesní model, ze kterého vyplývá:

1. jaké procesy či postupy budou digitalizovány,
2. jaké budou jednotlivé elementy nebo entity IS,
3. jací budou uživatelé IS,
4. jaký bude (odhadovaný) objem dat, a to vč. četnosti datové výměny.

Po procesním modelu přichází první návrh architektury systému – nejdřív se vytvoří tzv. „entrerprise model“, tzn. schématický návrh IS, který je srozumitelný jak pro IT odborníky, tak pro jejich protějšky, většinou zástupce budoucích uživatelů systému (s vynikající znalostí problematiky procesů, které se mají digitalizovat). Při tvorbě tohoto modelu se berou v úvahu další vstupy, zejména pak:

1. legislativní rámec, do kterého bude IS zasazen. V tomto ohledu se může jednat o:
    a. obecně platnou legislativu, jako jsou zákony, vyhlášky apod. – např. při tvorbě účetního systému je zřejmé, že se do tvorby IS musí promítnout zákon o účetnictví,
    b. interní předpisy a nařízení – např. při tvorbě systému pro podporu údržby železničních vozidel bude brán v úvahu interní údržbový předpis a příslušné technické normy, na které se údržbový předpis odvolává.
2. Popis zdrojů dat, jako např. data z jiných IS, data z čidel, snímačů či dalších zařízení, vytěžování dat z nedigitálních zdrojů apod.
3. Základní HW platformy a požadavky na HW, jako jsou servery, počítače či mobilní technologie. Zvláštní kategorie je mobilní část IS zabudovaná do železničních vozidel, protože se jedná de facto o ekosystém IS.
4. Bezpečnostní aspekty a prvky z pohledu:
    a. technického řešení (jako je HW a software – dále jen „SW“ např. firewally, antivirové programy, fyzické oddělení sítí apod.),
    b. procesního (technologické postupy úkonů, manuály a návody, zakázané postupy apod.),

c. legislativního (např. z pohledu zákona o kybernetické bezpečnosti a jeho prováděcích vyhlášek nebo z pohledu interních bezpečnostních předpisů).

Bezpečnostní aspekty nového IS jsou souhrnně uvedeny v tzv. „Bezpečnostním projektu“, který v sobě obsahuje jak analýzu rizik, tak návrh řešení z pohledu technického, ekonomického a projektového (čas realizace, posloupnost kroků apod.).

Takto hrubě navržený informační systém je pak posouzen z ekonomického hlediska (zde mohou být různé, dosti odlišné pohledy, např. jinak se na tvorbu IS bude dívat investor a jinak developer IS). Jednotlivé verze návrhů prochází iteracemi až po finální návrh systému.

Další fáze tvorby informačního systému je detailní analýza. Zde se dříve popsané hrubé modely a popisy precizují až do nejmenšího detailu. Jedním z výstupů analýze je pak cílový koncept, který popisuje velmi detailně budoucí IS, vč. jeho datových vazeb, harmonogram a posloupnosti jednotlivých etap apod. Je to v zásadě mapa k vytvoření vlastního IS (v IT terminologii „roadmap“).

Důležitou součástí cílového konceptu je technický návrh infrastruktury HW, který vychází jak z teoretických výpočtů (zdroje dat jsou např. z entrerprise, relačního nebo datového modelu) nebo se použije odhad za pomoci porovnání s podobným, již funkčním IS. HW je připravován z pozice výkonu (procesory, paměť), datových úložišť a dalších vlastností (např. požadavek na redundanci HW prvků z důvodu vysoké dostupnosti IS). V IT terminologii je tento krok označován jako „sizing“. Ukázka procesního a návazných modelů návrhu konkrétní aplikace jsou uvedeny v příloze A této práce.

V prostředí dopravy, zvláště pak u vozidlových (mobilní části) IS, se využívá speciální HW, který není tak rozšířený a dostupný jako běžně používané počítače a servery. Tento HW (např. vozidlové průmyslové počítače, displeje pro strojvedoucí, vozidlové sítě vč. přenosových prvků apod.) na rozdíl od „normálních“ počítačů musí být speciálně schválen pro použití v dopravě a následně certifikován jako subsystém příslušného vozidla. Certifikace není založena jen na teoretické bázi, kdy výrobce předkládá technickou a provozní dokumentaci, ale naopak prochází fyzickými testy a speciálně se zkoumá, zda příslušný HW nebo subsystém IS negativně neovlivňuje jízdu nebo řízení vozidla. Toto zkoumání a testy může provádět ze zákona [3] jen tzn. notifikovaná osoba

(tzv. „Notified Body“), v České republice se jedná např. o společnost Výzkumný ústav železniční, a.s. Po kladném posouzení HW nebo subsystému IS ze strany notifikované osoby je předložena finální žádost na certifikaci k příslušné státní autoritě, v železničním prostředí se jedná o Drážní úřad.

Jednou ze zásadních fází vytvoření IS je vytvoření prototypu (někdy se mluví např. o pilotním provozu), kdy verze IS, která je de facto připravena k praktickému použití, projde náročnými testy (penetračními = ověření bezpečnosti systému a zátěžovými = ověření zatížení systému při velkém výkonu IS). V rámci pilotního provozu dochází i na testování funkcionalit, tzn., zda systém vyhovuje požadavkům, pro které byl navržen.

V případě, že IS nevyhoví výše popsaným testovacím procedurám, vrací se zpět k opravě a dopracování. Když naopak vyhoví všem požadavkům, nastává fáze (rovněž velmi dobře popsaná v cílovém konceptu) jako implementace IS – někdy se rovněž tato fáze označuje IT termínem „Roll-Out“.

Před nebo v průběhu implementační fáze probíhá školení uživatelů, popř. dalších pracovníků, kteří budou se systémem pracovat (např. administrátoři IS). Teď už nic nebrání tomu, aby byl IS předán do rutinního provozu.

1.2.2 Provoz IS

Při předání IS do (rutinního) provozu dochází k instalaci SW (aplikací) na cílovou HW infrastrukturu (na servery, vozidlové počítače apod.). Důraz je velmi kladen i na předání technické a provozní dokumentace IS – tento krok bývá velkou slabinou IS, a to jak z pohledu běžného provozu IS (tzn. v případě nestandardních jevů lze dohledat příčiny, postup pro jejich odstranění apod.), tak mimořádných událostí, jako je např. kybernetický útok. Slabina spočívá v tom, že dokumentace bývá v praxi nedostatečně zpracovaná (ze strany výrobce IS) a nedostatečně zkontrolovaná (ze strany vlastníka nebo provozovatele IS).

Provoz IS může být realizován přímo vlastníkem IS nebo může být outsourcován k provozovateli systému. Zajištění provozu by mělo být de facto na stejné kvalitativní úrovně, rozdíl je (a proto se k tomuto modelu přiklání spousta vlastníků IS), že profesionální provozovatelé mají kvalitnější a zkušenější provozní personál, lepší a mnohdy levnější HW infrastrukturu (z důvodu množství provozovaných IS) a celkově lepší technické zázemí (např. ochrana IS před výpadkem elektrické energie).

Provozovatel IS není zodpovědný jen za chod systému, ale za celkové podmínky pro IS, tzn., musí udržovat HW infrastrukturu, vč. jejího zázemí, pravidelně aktualizovat OS, provádět průběžné testování a dohled všech komponent IS. Zvláštní kapitolou je pak kybernetická ochrana, kdy provozovatel instaluje a aktualizuje nástroje pro ochranu IS, jako jsou antivirové programy, firewally a další prvky. Provozovatel IS rovněž poskytuje součinnost pro nasazování nových verzí IS.

V dnešní době se pro stacionární část IS využívají hodně cloudové technologie, kdy není potřeba budovat svoji vlastní HW infrastrukturu, ale využije se sdílená a předem dedikovaná infrastruktura (vč. OS a základní kybernetické ochrany) u poskytovatele cloudových služeb.

Pro správnou funkci provozu IS je nutné mít průběžná data o stavu IS, komunikačních linek a dalších, předem definovaných parametrů. Tyto parametry se sledují pomocí dohledových a diagnostických systémů, kdy je obsluha těchto systémů upozorňována na nežádoucí stavy pomocí tzv. alertů.

V rámci fáze životního cyklu IS provoz je i nutná uživatelská podpora IS. Nejrozšířenějším modelem je trojúrovňová uživatelská podpora (v IT terminologii „Three Level Support“, nebo též „Multilevel Support“), kdy:

1. první úroveň je dedikovaná pro styk s běžným uživatelem systému; tato úroveň není obsazena IT specialisty, ale spíš univerzálními pracovníky, kteří postupují podle předem daných scénářů (otázek a rad uživatelům). Nejdůležitější povinností pracovníků první úrovně uživatelské podpory je záznam a dokumentace přijetí požadavku. Tento čas je totiž rozhodný pro určení, zda uživatelská podpora nebo provozní pracovníci IS poskytli podporu v předem definovaných parametrech (v IT terminologii SLA, **S**ervice **L**evel **A**greement, což jsou provozní smluvní parametry).
2. Druhou úroveň zabezpečují už specialisté, kteří danému IS rozumí a dokáží kreativně pomoci. Uživatelé IS ovšem (alespoň v první fázi) nekomunikují s druhou uživatelskou úrovní napřímo, ale přes první úroveň. Pracovník druhé uživatelské úrovně je natolik fundovaný, že rozhodne, zda případný problém vyřeší bez nutnosti další komunikace nebo zda se spojí přímo s uživatelem IS, který původně kontaktoval první úroveň. Pracovníci, kteří zabezpečují druhou uživatelskou úroveň podpory, bývají většinou analytici nebo testeři IS.

3. Třetí úroveň zabezpečují programátoři nebo administrátoři IS, kteří v případě potřeby (např. incidentu v rámci IS) provedou úkon k opravě nebo přenastavení IS.

Důležitým aspektem uživatelské podpory je přesná evidence všech hlášených problémů a dotazů (proto zejména u první úrovně uživatelské podpory jsou telefonické hovory zpravidla nahrávány, na což bývá uživatel předem upozorněn). K evidenci problémů a jejich odstraňování slouží speciální aplikace, obecně označovaná jako „Service Desk“. Data ze Service Desku slouží i pro dlouhodobou práci s IS, jsou zde sledovány hodnoty jako procento odstraněných (nebo neodstraněných) závad, popisy řešení problémů (pro další využití) apod.

Systém uživatelské podpory je zobrazen na schématu č. 1.3:

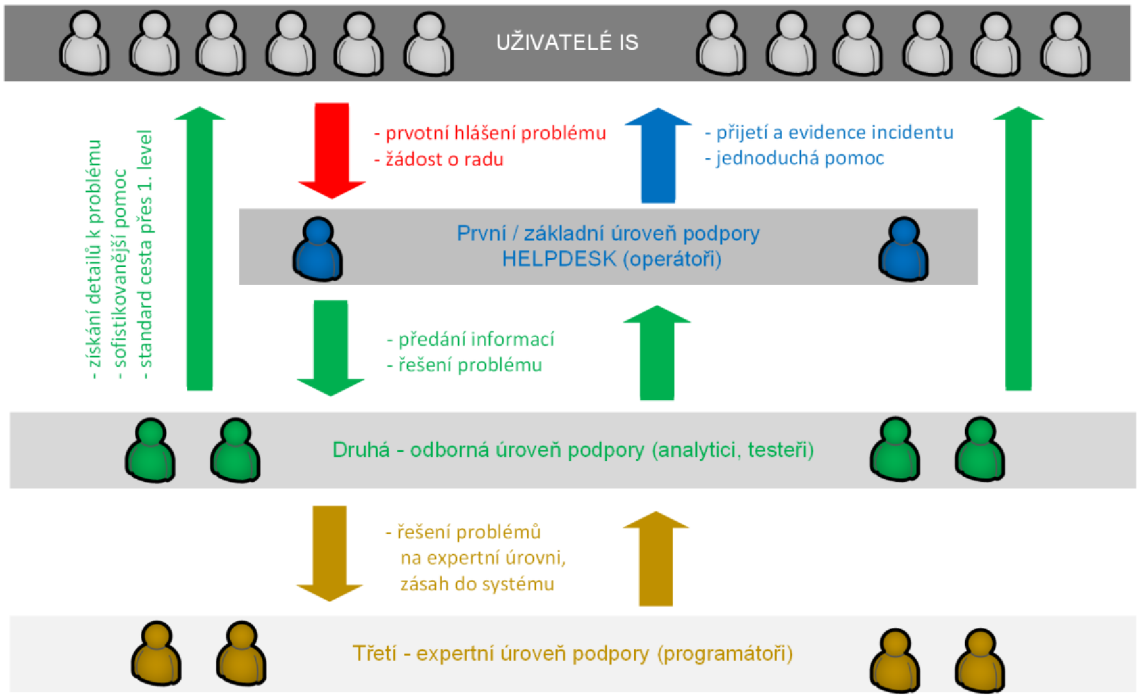


Schéma 1.3 Tříúrovňový systém uživatelské podpory
Zdroj: vlastní zpracování

1.2.3 Zrušení (ukončení) IS

Ukončení či zrušení IS může probíhat různými formami, mezi základní patří:

1. nahrazení IS jinou verzí či jiným IS,
2. ukončení IS bez náhrady.

V obou variantách je nezbytné dbát na ochranu dat, které jsou v IS uloženy a na řádné ukončení veškerých vazeb a komunikací – podcenění této problematiky může vést ke kybernetickému incidentu.

V případě, že je IS nahrazen jinou verzí či jiným IS, nastávají dvě důležité fáze, než se IS vystřídají:

1. migrace dat – aby byla zachována datová integrita a návaznost mezi původním a nástupnickým IS, je nutné provést migraci (transfer) dat. Data do nového IS jsou migrována speciálními postupy, a to buď přímo ze systému do systému nebo přes export do datových skladů či jiného vhodného úložiště.
2. Souběžný provoz původního a nového systému – do ověření, že je nový IS plně připraven ke spuštění a převzetí funkcionalit původního systému, je ponechána vhodná lhůta, kdy jsou oba dva systémy provozovány vedle sebe souběžně. Vůči uživatelům IS se ale tato situace jeví tak, že:
    a. buď pracují ještě v původním systému, nový IS ale už přijímá data, a tak se vlastně zkouší v reálném provozu,
    b. nebo již pracují v novém IS, přičemž původní systém slouží jako jakési záložní řešení pro případ, že by nový systém vykazoval nekorektní stavy.

    Vždy však musí být jasně rozhodnuto, který z těchto IS je po dobu souběžného provozu hlavní a je k dispozici uživatelům a který běží na pozadí z technických důvodů.

Nicméně pro jakoukoliv variantu ukončení či zrušení IS platí, že [1]:

1. data, která budou potřeba v jiném IS musí být odmigrována,
2. data, která je potřeba využívat v budoucnu, nebo musí být (např. z legislativních) důvodů zachována, musí být náležitě zarchivována (mimo původní IS),
3. bezpečností prvky, popř. citlivá data jako např. šifrovací klíče musí být náležitě a bezpečně smazána,
4. IS jako takový je odinstalován, popř. smazán z provozní HW infrastruktury, která se buď použije pro jiné účely nebo se rovněž odstraní.

Nevymazání původního IS nebo části dat (např. z důvodu, že administrátorská obsluha IS tento systém občas využívá např. jako testovací prostředí) může iniciovat závažný kybernetický incident. Systému v neprodukčním módu se nevěnuje tolik pozornosti, není tolik pod kontrolou a je zde pravděpodobnější možnost lidské chyby.

Navíc se v praxi se běžně stává, že dosluhující IS už sice neposkytuje původní funkcionality a není k dispozici uživatelům, nicméně jeho provoz je v určitě míře zachován a slouží jako provozní datový zdroj archivních dat pro nový IS. O to více a důkladněji by měly být ověřeny všechny bezpečnostní aspekty takto smíšeného provozu IS.

1.3 Bezpečnostní východiska informačních systémů

Bezpečnost IS i jejich periferií není jen otázka vlastních bezpečnostních řešení, ale celého bezpečnostního managementu, který se dá charakterizovat:

1. bezpečnostním personálem, do kterého nejsou zahrnuty pouze role kybernetické bezpečnosti, ale i další technický personál, který se podílí na jednotlivých fázích životního cyklu IS,
2. bezpečnostní legislativou, která:
    a. je dána zákony a vyhláškami pro tuto oblast (zejména pak zákon o kybernetické bezpečnosti [4], vč. jeho prováděcích vyhlášek),
    b. navazujícími normativními akty, a sice:
        i. interními předpisy a dokumenty, zejména pak analýzou rizik a bezpečnostní politikou (nebo politikami, pakliže je tato problematika rozsegmentována do jednotlivých oblastí – např. z důvodu lepšího seznamování nebo vyvozování odpovědnosti vyplývající z těchto politik),
        ii. technickými normami a nařízeními (např. rodina ISO 27000 týkající se řízení bezpečnosti informací nebo ISO 15408 pro certifikaci počítačové bezpečnosti),
3. bezpečnostní dokumentací, např. bezpečnostní projekt, který se provádí před vývojem a nasazením systému, a na něj navazující další důležité dokumenty, jako již uvedené bezpečnostní politiky, analýza rizik, krizové plány apod.,
4. podpůrnými technickými nástroji, jako např. aplikace pro správu a zobrazování aktiv, rizik a hrozeb.

V rámci bezpečnostního managementu se pochopitelně neopracuje jen s kybernetickou bezpečností, naopak jsou pokrývány různé oblasti bezpečností problematiky, které

zohledňují pro danou oblast typická specifika. Mezi základní oblasti bezpečnosti z pohledu IS patří:

1. kybernetická (nebo též informatická či počítačová) bezpečnost – zaměřená na technickou stránku IS,
2. fyzická bezpečnost – zaměřená na fyzické aspekty bezpečnosti, jako např. vstupní a kamerové systémy, zabezpečovací zařízení apod.
3. komunikační bezpečnost – oblast bezpečnosti pokrývající nejen technické komunikační zařízení (jako počítače, routery, mobilní telefony), ale i oprávnění a komunikační matice,
4. informační bezpečnost – oblast zaměřená na datový obsah IS vč. příslušné dokumentace a datových úložišť. Tato oblast prošla poměrně rozsáhlou standardizací a v praxi je známá jako ISMS (**I**nformation **S**ecurity **M**anagement **S**ystem neboli systém řízení bezpečnosti informací). Systémem se v tomto ohledu rozumí jak metodika, tak organizace práce a pomocný SW,
5. personální bezpečnost – tato oblast pokrývá vše co souvisí s lidskými zdroji, které přijdou do kontaktu s IS, ať už se jedná o personál vyvíjející či obsluhující IS, tak uživatele a další související role. Jsou zde řešeny takové aspekty, jako práva a povinnosti k IS, oprávnění k přístupu k datům, školení apod.
6. administrativní – bezpečnostní problematika musí být vždy dobře popsaná, zejména pak v řídící a obchodní dokumentaci. Do jisté míry propojuje administrativní bezpečnost všechny ostatní bezpečnostní oblasti a dává jim konkrétní statut. Netýká se jen interních procesů, ale zároveň pokrývá i vztahy navenek, zejména pak vztahy obchodní (např. obchodní smlouvy, na základě kterých jsou řešena práva a povinnosti smluvních stran z pohledu bezpečnosti nebo smlouvy NDA – **N**on-**D**isclosure **A**greement, neboli smlouvy o mlčenlivosti).

Jak bylo popsáno výše, jedním ze základních stavebních kamenů bezpečnostního managementu je příslušná dokumentace. Dá se říci, že na vrcholu pomyslné pyramidy bezpečnostní dokumentace stojí bezpečnostní politiky, které představují strategii a směr. Na ně navazuje další dokumentace, zejména pak analýza rizik, vč. krizových plánů.

1.3.1 Bezpečnostní politiky

Bezpečnostní politiky si určuje každá organizace nebo subjekt podle svých potřeb, nicméně by měly pokrýt všechny oblasti bezpečnosti, které se dané organizace týkají. Nejzásadnější politiky jsou [5]:

1. Politika organizační bezpečnosti – zde se vymezuje v zásadě celá oblast, které se bezpečnost týká, definuje zásadní role, kterým přiřazuje práva a povinnosti.
2. Politika fyzické bezpečnosti – týká se především všech fyzických prvků, které mají souvislosti nebo dopad na bezpečnost, jako např. zabezpečovací a kamerové systémy, oprávnění ke vstupům do zabezpečených místností, systém zámků apod.
3. Politika informační a kybernetické bezpečnosti – tato politika stanovuje rozsah vlastních technických a organizačních opatření vedoucí k předcházení, zabraňování nebo odstraňování následků kybernetických událostí.
4. Politika řízení informací – stanovení práce s daty a dokumentací, jako klasifikace informací (veřejné, důvěrné, tajné), přístup k informacím pro jednotlivé role nebo uživatele, určení nástroje pro ochranu dokumentů nebo jejich zneužití apod.
5. Politika řízení lidských zdrojů – zde se určuje směr zejména pro kvalifikaci a průběžné školení personálu.
6. Politika řízení dodavatelů – netýká se jen veřejných zadavatelů, ale v zásadě všech organizací nebo subjektů, které nakupují elementy nebo řešení či odebírají jakoukoliv oblast bezpečnosti jako službu (outsourcing). Je zde kladen důraz na prověřování dodavatelů, jejich důvěryhodnost, reference a spolehlivost.
7. Politika zvládání kybernetických bezpečnostních incidentů – prvotní a rámcový návod zejména pro vytvoření krizových plánů.

1.3.2 Analýza rizik

Je jedním ze základních kamenů bezpečnosti IS, a to bez ohledu, zda systém nebo daná problematika kompetenčně spadá pod zákon o kybernetické bezpečnosti. Ačkoliv je v názvu slovo „analýza“, nejedná se pouze o analytický dokument – rovněž obsahuje soubor opatření, pravidel a plánů. Analýza rizik musí obsahovat především:

1. Identifikaci aktiv – zde se detailně popisuje, co se vlastně v rámci bezpečnosti IS má chránit. Aktivum je v tomto případě to, co je cenné pro vlastníka nebo další role v rámci IS. Může být jak materiální, tak nehmotné povahy, jedná se zejména o data a informace, ale i o počítače, sítě a další prvky IS.

2. Identifikace hrozeb – jedná se o definici událostí, které mohou mít za následek ztrátu či poškození aktiv. Hrozby jsou definovány většinou ve struktuře [1]:
    a. kdo nebo co může způsobit hrozbu (též jako nositel hrozby),
    b. co konkrétně je v rámci aktiv ohroženo (tzn. objekt hrozby),
    c. jakým způsobem je aktivum ohroženo (tzn. mechanismus ohrožení).
3. Identifikace zranitelnosti (nebo též slabin) – vydefinování slabých míst v IS v návaznosti na aktivech a hrozbách. Výstupy této části analýzy slouží jako jeden ze zásadních vstupů do akčních plánů, tzn., co a jak se má udělat, aby aktiva byla dostatečně chráněna.
4. Analýza dopadů – tato analýza může obsahovat různé kvantifikace a metodiky dopadů hrozeb na IS. Dopady mohou být kvantifikovány např.:
    a. z ekonomického hlediska, tzn. tato hrozba má konkrétní finanční hodnotu (nebo rozsah hodnot); tato hodnota se zpravidla spojuje s odhadem na ztrátu či poškození aktiv a nápravy této situace, externích dopadů (pokuty, sankce apod.),
    b. bodovou nebo procentní stupnicí, která stanoví žebříček dopadů (od nejhorších po zanedbatelné),
    c. kvalifikací dopadu podle dopředu daných kategorií (např. malý/střední/velký dopad).
5. Hodnocení míry rizika – kroky uvedené v předchozích bodech ještě nestanovují riziko jako takové. Aby bylo možné rizika kvantifikovat a řídit, je nutné ke každému jednotlivému aktivu vhodným způsobem přiřadit kombinaci hodnot hrozeb, zranitelnosti a dopadu. Výsledná hodnota bude přiřazena ke předem stanovené stupnici rizik. Pro jednotlivé kategorie rizik (dané stupnicí) se následně stanoví další parametry a podmínky, jako např. krizové plány, komunikační matice apod.
6. Krizové plány – v návaznosti na předchozí části analýzy rizik a v souladu s příslušnou bezpečnostní politikou jsou stanoveny různé postupy a plány, které dávají návody a postupy pro určitou oblast rizik. Krizové plány jsou jednou z nejzásadnějších oblastí, ve které by se měli školit obsluha i uživatelé IS. Mezi nejzásadnější krizové plány patří [6]:
    a. krizová komunikační matice – tzn., kdo komunikuje v případě nastalé hrozby s kým, jsou zde popsány ohlašovací povinnosti, nebo naopak zakázány některé komunikační toky.

b. Plány pro reakci na úspěšný kybernetický útok nebo živelné pohromy – konkrétní plány pro určitý typ události.
c. Plán kontinuity činností (tzv. BCP neboli **B**usiness **C**ontinuity **P**lan) a plán obnovy (tzv. DRP neboli **D**isaster **R**ecovery **P**lan), tzn. vydefinované postupy, díky kterým si organizace v případě mimořádné situace (popsané v identifikaci hrozeb) obnoví zpět svoji činnost – např. spouštění IS po masivním výpadku elektrické energie (tzv. blackoutu).

7. Management bezpečnosti – řídící akty a metodiky, které popisují zejména:
   a. systém řízení rizik,
   b. systém řízení změn
   c. apod.

   Pro management bezpečnosti jsou nutná další relevantní data, proto se doporučuje provádět v pravidelných intervalech (většinou 1x ročně) audit kybernetické bezpečnosti.

Nad rámec výše popsané struktury analýzy rizik je velmi doporučeno se zabývat problematikou:

1. Řízení lidských zdrojů – detailnější analýzy a plány např. rolí v rámci IS, školení, seznamování s bezpečnostními politikami apod.
2. Řízení dodavatelů – jedná se o speciální analýzu a plány zaměřené na dodavatele IS nebo jejich částí či služeb s nimi souvisejícími. Jedná se např. o řešení problematiky tzn. Vendor Lock–In neboli přílišné závislosti na jednom dodavateli. Tato závislost může vést k nedostatečné kontrole bezpečnosti IS a tím naplnění některých rizik.

1.3.3 Technické možnosti bezpečnosti IS

Ochrana IS není tvořena analýzami a plány, ale konkrétními (IT nebo technickými) nástroji nebo pravidly bezpečného chování v rámci práce s IS nebo ICT technologiemi. Díky těmto opatřením nebo souboru nástrojů se výrazně snižují rizika ohrožení IS. Jako nejzásadnější lze uvést:

1. Organizační zásady a pokyny pro práci s technologiemi, např. zákaz používání veřejných Wi-Fi sítí na služebních telefonech/tabletech/počítačích, zákaz užívaní (až na výjimky) sociálních sítí na uvedených zařízeních, zákaz zobrazování

informací na zamčeném mobilním telefonu/tabletu, apod. Příklady takových opatření je možné najít na odborných portálech na internetu [7].

2. Fyzická bezpečnost – zavedení systému vstupních karet, monitoring prostorů, kde je zabezpečen provoz IS, fyzická ostraha příslušných prostor apod.
3. Řízení přístupů – tato oblast bývá nazývaná rovněž Access Management a definuje pravidla pro registrace, autentizace a identifikace uživatelů. Zásadní oblastí Access Managmentu je politika hesel (počet a druh znaků, četnost změny hesla, vícefaktorové ověřování uživatele apod.). V kategorii mobilních přístrojů se řízení přístupů řídí nástroji MDM (**M**obile **D**evice **M**anagement).
4. Ochrana před škodlivým kódem – do této kategorie nepatří jen vlastní ochrana IS jako jsou antivirové programy a firewally, ale další organizační a architektonická opatření, jako např. segmentace vnitřních komunikačních sítí, pravidelná aktualizace OS a MW a další.
5. Nástroje pro dohled nad provozem IS a monitoring událostí a procesů (např. formou tzv. SIEM systémů – **S**ecurity **I**nformation and **E**vent **M**ananagement).
6. Aplikační bezpečnost – jedná se v zásadě o fyzické oddělení HW infrastruktury a instancí SW, včetně dat pro účely vývoje, testování a produkčního provozu IS (proto i jednotlivá, vzájemně nepropojená prostředí: vývojová, testovací a provozní). Žádné z těchto prostředí nesmí automaticky užívat stejná data. Vždy je nutné zachovávat auditní stopu (např. ve formě logů).
7. Šifrování – cílem tohoto opatření je ochrana dat v celém jejich životním cyklu. Do této problematiky patří vlastní šifrování dat v IS nebo datových úložištích (vč. přenosných médií jako např. USB disk), ukládání klíčů a hesel apod. Nešifrují se jen vlastní data, šifrovaná může být i elektronická komunikace. [8]
8. Dostupnost IS a informací – povaha IS určuje jeho dostupnost, přičemž s tímto klíčovým parametrem je IS již projektován. Největší možnost dostupnosti bývá označována jako 24/7, tzn. 24 hodin denně a 7 dní v týdnu. Po odečtení plánovaných odstávek IS dedikovaných na údržbu se pak požadavek na dostupnost IS vyjadřuje v procentech (tzn. nejvyšší dostupnost je 99–100 %). Pro dosažení takto přísných parametrů jsou v rámci architektury IS naprojektovány vlastnosti jako:

a. geocluster (ukládání dat nebo instance IS v různých geografických lokalitách, vzdálených od sebe i stovky až tisíce kilometrů),
b. zavedení pravidla eliminace neboli SPOF (**S**ingle **P**oint **o**f **F**ailure), tzn. výpadek jedné komponenty IS nesmí zapříčinit havárii celého IS,
c. plán zálohování (dat i stavu systému vč. nastavovacích logů a kódů).

9. Ošetření cloudového řešení – výše uvedené řešení opatření je nutné řešit i v případě, že je IS provozován v rámci cloudových služeb. Nad rámec těchto opatření je nutné přihlédnout k vlastnímu zabezpečení cloudu (tzv. bezpečný cloud), vč. jeho certifikace pro bezpečný provoz IS.

Výše uvedený výčet technických možností bezpečnosti IS není konečný a detailní. Další možnosti ochrany příslušného IS budou vyplývat z bezpečnostní dokumentace, zejména pak analýzy rizik a jednotlivých bezpečnostních politik.

2 Právní rámec kybernetické bezpečnosti

Rozsah užívání IS a ICT v rámci běžného života je dnes tak široký, že je nutné tuto oblast regulovat vhodnou legislativou. Na tento právní rámec se dá pohlížet nejen očima zákonů a dalších právních norem, ale i navazujících normativních aktů, jako např. technických norem, vnitřních předpisů apod.

Soubor právních aktů České republiky (dále jen ČR) vztahující se ke kybernetické bezpečnosti, nemá obecnou platnost (tzn. netýká se všech občanů, institucí a právnických osob), ale těch subjektů a rolí, které jsou definovány přímo zákonem. Některé parametry vyplývající ze zákona nelze určit jednoznačně, proto je přezkoumává Národní úřad pro kybernetickou bezpečnost (dále jen „NÚKIB“). Ten následně rozhodne o příslušných kategoriích a povinnostech pro tzv. „povinné osoby“.

Informaticko-bezpečnostní legislativa částečně vychází z konkrétních technických norem a standardů bezpečnosti IS a ICT. Přebírání standardů a inspirace jde však i opačným směrem. Subjekty, které této legislativě nepodléhají, ji často využívají pro své interní potřeby (např. pro tvorbu vnitřních bezpečnostních předpisů a dalších interních normativních aktů).

V rámci standardizace a sladění podmínek v této oblasti vydalo Ministerstvo vnitra ČR ve spolupráci se svou podřízenou organizací agenturou NAKIT (Národní agentura pro komunikační a informační technologie, státní podnik) a s NÚKIB, materiál pro subjekty mimo rámec zmíněné legislativy [9], popisující minimální bezpečnostní standardy IS, přičemž si nelze nevšimnout podobnost struktury a některých doporučení s již zmíněnými právními normami.

2.1 Legislativa

2.1.1 Kybernetický zákon

Zákon č. 181/2014 Sb., o kybernetické bezpečnosti (dále jen „kybernetický zákon“) [4] je základním kamenem právní úpravy zaměřené na bezpečnost IS a ICT. V návaznosti na evropskou legislativu:

1. je do kybernetického zákona transponována Směrnice Evropského parlamentu a Rady (EU) 2016/1148 ze dne 6. července 2016 o opatřeních k zajištění vysoké společné úrovně bezpečnosti sítí a informačních systémů v Unii [10],
2. navazuje kybernetický zákon na Nařízení Evropského parlamentu a Rady (EU) 2019/881 ze dne 17. dubna 2019 o agentuře ENISA („Agentuře Evropské unie pro kybernetickou bezpečnost"), o certifikaci kybernetické bezpečnosti informačních a komunikačních technologií [11].

Kybernetický zákon upravuje základní pojmy a vztahy v oblasti kybernetické bezpečnosti, zejména:

1. kategorie IC, ICT systémů a služeb, jako
    a. kritickou informační infrastrukturu,
    b. významný informační systém (ten je definovaný vyhláškou ke kybernetickému zákonu),
    c. významnou síť elektronických komunikací,
    d. informační systém základní služby (vysvětlení níže),
    e. digitální služba (on-line řešení jako e-shopy, internetové vyhledávače apod.),
2. definuje odvětví základní služby, které je velmi závislé na elektronických komunikacích a IS, jejichž narušení by mohlo mít zásadní dopad do společenských a ekonomických činností; jedná se se o tato odvětví:
    a. energetika,
    b. doprava,
    c. bankovnictví,
    d. infrastruktura finančních trhů,
    e. zdravotnictví,
    f. vodní hospodářství,
    g. digitální infrastruktura,
    h. chemický průmysl,
3. role (orgány a osoby), kterým jsou v rámci kybernetického zákona ukládány povinnosti:
    a. poskytovatel služby nebo sítě elektronických komunikací,
    b. poskytovatel významné sítě (ne však kritické infrastruktury)

c. správce a provozovatel informačního nebo komunikačního IS kritické infrastruktury,
d. správce a provozovatel významného IS
e. správce a provozovatel IS základní služby (ne však kritické infrastruktury), popř. i provozovatel základní služby,
f. poskytovatel digitální služby.

Z technického pohledu určuje kybernetický zákon bezpečnostní opatření, které dělí na dvě kategorie:

1. organizační opatření a
2. technická opatření.

K organizačním opatřením patří [4, §5, odst. 2]:

1. systém řízení bezpečnosti informací,
2. řízení rizik,
3. bezpečnostní politika,
4. organizační bezpečnost,
5. stanovení bezpečnostních požadavků pro dodavatele,
6. řízení aktiv,
7. bezpečnost lidských zdrojů,
8. řízení provozu a komunikací,
9. řízení přístupu osob,
10. akvizice, vývoj a údržba,
11. zvládání kybernetických bezpečnostních událostí a kybernetických bezpečnostních incidentů,
12. řízení kontinuity činností a
13. kontrola a audit.

Technická opatření jsou [4, §5, odst. 3]:

1. fyzická bezpečnost,
2. nástroj pro ochranu integrity komunikačních sítí,
3. nástroj pro ověřování identity uživatelů,

4. nástroj pro řízení přístupových oprávnění,
5. nástroj pro ochranu před škodlivým kódem,
6. nástroj pro zaznamenávání činnosti informačního nebo komunikačního systému, jeho uživatelů a administrátorů,
7. nástroj pro detekci kybernetických bezpečnostních událostí,
8. nástroj pro sběr a vyhodnocení kybernetických bezpečnostních událostí,
9. aplikační bezpečnost,
10. kryptografické prostředky,
11. nástroj pro zajišťování úrovně dostupnosti informací a
12. bezpečnost průmyslových a řídících systémů.

Kybernetický zákon dále řeší hlášení a evidenci kybernetických incidentů, popisuje kybernetické nebezpečí a postup při varování před ním, a v neposlední řadě stanovuje výkon úřadu NÚKIB jako orgánu státní správy, jeho kompetence, kontrolu apod. O důležitosti poslání NÚKIB svědčí ten fakt, že se prostřednictvím Výboru pro kybernetickou bezpečnost, kde je NÚKIB stálým členem, pravidelně účastní jednání Bezpečnostní rady státu (BRS).

NÚKIB má na základě kybernetického zákona ještě jednu roli, a sice se jedná o tzv. vládní CERT. CERT (zkratka z anglického termínu **C**omputer **E**mergency **R**esponse **T**eam) je místo, které přijímá hlášení a podněty o kybernetických incidentech zejména z oblasti státní správy, kritické informační infrastruktury a významných informačních systémů. O ostatní kybernetické incidenty se stará tzv. národní CERT, se kterým má NÚKIB na základně kybernetického zákona uzavřenu smlouvu. V současné době zastává pozici národního CERT organizace CZ.NIC.

Přehled vztahu kybernetického zákona, jeho prováděcích vyhlášek a dalších normativních aktů je graficky znázorněn na schématu č. 2.1.

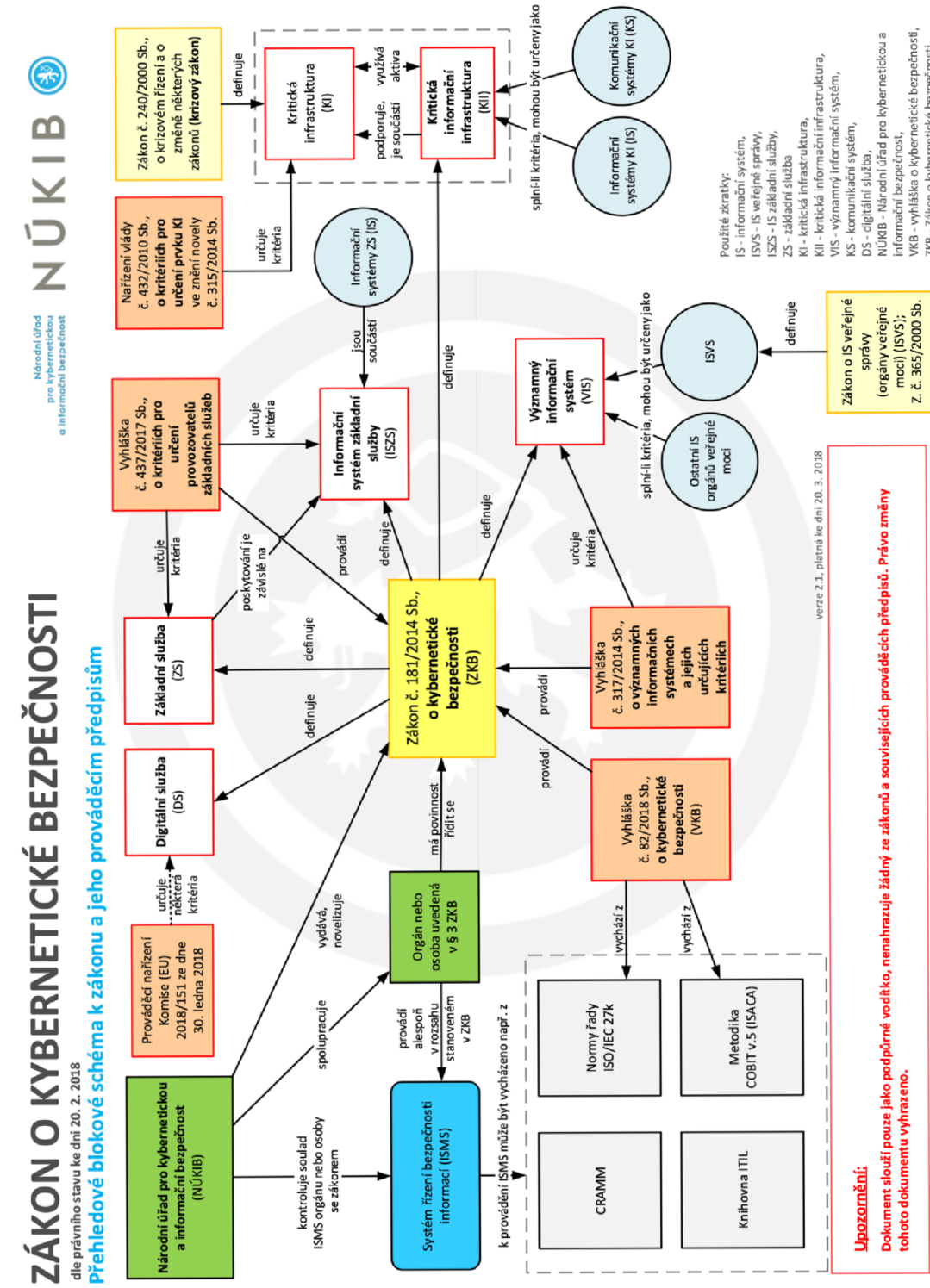


Schéma 2.1 Přehledové blokové schéma ke kybernetickému zákonu a jeho prováděcím předpisům

Zdroj: [12]Národní úřad pro kybernetickou bezpečnost

2.1.2 Prováděcí vyhlášky kybernetického zákona

V současné době má kybernetický zákon 3 (tři) prováděcí vyhlášky:

1. vyhláška č. 317/2014 Sb., o významných informačních systémech a jejich určujících kritériích – velmi krátká vyhláška, která stanovuje definici a kritéria významných informačních systémů [13],
2. vyhláška č. 437/2017 Sb., o kritériích pro určení provozovatele základní služby [14] upravuje odvětvová a dopadová kritéria pro určení provozovatele základní služby a vymezení významnosti dopadu narušení základní služby na zabezpečení společenských nebo ekonomických činností podle § 22a odst. 1 kybernetického zákona,
3. vyhláška č. 82/2018 Sb., vyhláška o kybernetické bezpečnosti [15] upravuje pro informační systém kritické informační infrastruktury, komunikační systém kritické informační infrastruktury, významný informační systém, informační systém základní služby anebo informační systém nebo síť elektronických komunikací, které využívá poskytovatel digitálních služeb:
    a. obsah a strukturu bezpečnostní dokumentace,
    b. obsah a rozsah bezpečnostních opatření,
    c. typy, kategorie a hodnocení významnosti kybernetických bezpečnostních incidentů,
    d. náležitosti a způsob hlášení kybernetického bezpečnostního incidentu,
    e. náležitosti oznámení o provedení reaktivního opatření a jeho výsledku,
    f. vzor oznámení kontaktních údajů a jeho formu a
    g. způsob likvidace dat, provozních údajů, informací a jejich kopií.

2.1.3 Ostatní související legislativa

S problematikou kybernetické bezpečnosti souvisí níže další právní normy. Nejedná se o jejich taxativní výčet, ale výběr těch nejzásadnějších a nejrelevantnějších [16]:

1. zákon č. 240/2000 Sb., o krizovém řízení [17] – zde je řešena problematika ochrany kritické infrastruktury,
2. nařízení vlády č. 432/2010 Sb., o kritériích pro určení prvku kritické infrastruktury [18] – zde je definováno 9 (devět) odvětví pro definici kritické infrastruktury,

3. zákon č. 365/2000 Sb., o informačních systémech veřejné správy [19] – práva a povinnosti pro celý životní cyklus IS veřejné správy, a to včetně nároků na kybernetickou bezpečnost,
4. vyhláška č. 529/2006 Sb., o dlouhodobém řízení informačních systémů veřejné správy [20] – prováděcí vyhláška k zákonu č. 365/2000 Sb., obsahuje požadavky na strukturu a obsah dokumentace IS z pohledu bezpečnosti a požadavky na řízení bezpečnosti IS,
5. zákon č. 412/2005 Sb., o ochraně utajovaných informací a bezpečnostní způsobilosti [21]. Bezpečnost informací je v tomto zákoně upravena jinak než v kybernetickém zákoně, IS pro práci a uchování utajovaných informací musí být speciálně certifikovány; na tento zákon se váže více než 10 (deset) prováděcích vyhlášek, nařízení vlády ČR a dalších právních aktů (vč. právních předpisů Evropské unie),
6. zákon č. 127/2005 Sb., o elektronických komunikacích [22] – kromě úpravy práv, povinností a regulací trhu elektrických komunikací obsahuje zákon ustanovení o ochraně údajů, služeb a sítí elektronických komunikací, podstatnou roli zde hraje Český telekomunikační úřad,
7. zákon č. 297/2016 Sb., o službách vytvářejících důvěru pro elektronické transakce [23], který doplňuje Nařízení Evropského parlamentu a Rady (EU) č. 910/2014 ze dne 23. 7. 2014 o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu [24] a zrušení směrnice 1999/93/ES (tato právní norma známá též jako „eIDAS“). Tyto právní normy řeší problematiku elektronických podpisů, elektronické pečeti a datových razítek.

2.2 Normativní akty

2.2.1 Technické normy a metodiky

Dalšími vstupy, které upravují kybernetickou bezpečnosti, jsou technické a technologické normy. V některý případech se na ně právní předpisy odvolávají konkrétně (citují označení a název normy ve spojitosti s konkrétní povinností) nebo obecně (na skupinu norem zaměřených na konkrétní problematiku).

Nejvíce významnou skupinou norem ve vztahu ke kybernetické bezpečnosti je rodina standardů ISO/IEC řady 27000, která pokrývá celou problematiku bezpečnosti informací

s přihlédnutím k bezpečnosti IS. Nejvíce citovaná norma z této skupiny, ISO 27001, je zaměřená na ISMS. Některé normy z rodiny ISO 27000 byly přijaty jako česká technická norma (ČSN), mezi nejzásadnější je možné jmenovat [16]:

1. ČSN ISO/IEC 27000:2017 Informační technologie – Bezpečnostní techniky – Systémy řízení bezpečnosti informací – Přehled a slovník,
2. ČSN ISO/IEC 27001:2014 Informační technologie – Bezpečnostní techniky – Systémy řízení bezpečnosti informací – Požadavky,
3. ČSN ISO/IEC 27002:2014 Informační technologie – Bezpečnostní techniky – Systémy řízení bezpečnosti informací – Soubor postupů pro opatření bezpečnosti informací,
4. ČSN ISO/IEC 27003:2018 Informační technologie – Bezpečnostní techniky – Systémy řízení bezpečnosti informací – Pokyny,
5. ČSN ISO/IEC 27004:2018 Informační technologie – Bezpečnostní techniky – Systémy řízení bezpečnosti informací – Monitorování, měření, analýza a hodnocení,
6. ČSN ISO/IEC 27005:2019 Informační technologie – Bezpečnostní techniky – Řízení bezpečnosti informací,
7. ČSN ISO/IEC 27006:2016 Informační technologie – Bezpečnostní techniky – Požadavky na orgány provádějící audit a certifikace systémů řízení bezpečnosti informací,
8. ČSN ISO/IEC 27007:2018 Informační technologie – Bezpečnostní techniky – Směrnice pro audit systémů řízení bezpečnosti informací.

Jako další normy pro bezpečnost IS lze uvést:

1. ČSN ISO/IEC 15408:2001 zaměřená na všeobecný model, funkční součásti bezpečnosti a komponenty bezpečnostních záruk,
2. ISO/IEC 20000 obsahuje požadavky na vytvoření a řízení účinného systému managmentu kontinuity podnikání (**B**usiness **C**ontinuity **M**anagement **S**ystem – BCMS),
3. rodina ČSN ISO/IEC 10118 zaměřená na hašovací funkce,

4. ČSN ISO/IEC 4888 Informační technologie – Bezpečnostní techniky – digitální podpisy s dodatkem,
5. rodina ISO/IEC 9000 popisující standard jakosti i pro bezpečnost IS a technologie.

Další skupinou normativních aktů jsou mezinárodně uznávané metodiky zaměřené na IS a ICT, z nichž nejzásadnější jsou [16]:

1. ITIL – aktuální verze ITIL 4 - je soubor postupů, které umožňují lépe plánovat, využívat a zkvalitňovat využití informačních technologií, a to jak ze strany dodavatelů IT služeb, tak i z pohledu zákazníků. Obsahuje 4 (čtyři) základní moduly:
    a. řízení – řízení organizace a report procesů,
    b. praktiky – nastavování služeb s osvědčenou praxí,
    c. hlavní principy – formulace správy služeb,
    d. neustálé zlepšování – zlepšování pomoci iteračních postupů.
2. COBIT – platforma vyvinutá organizací ISACA, zajišťující řízení ICT a informací, vytváří rozhraní mezi obchodními riziky, technickými problémy a požadavky auditu.

Pro železniční osobní dopravu, na kterou je zaměřena tato diplomová práce, připadají v úvahu normy typu TSI – technické specifikace interoperability, které byly vytvořeny za účelem harmonizace podmínek na evropské železniční síti. Některé z těchto norem popisují systémy, které jsou zařazeny z pohledu kybernetického zákona jako kritická informační infrastruktura. Typickým příkladem je systém ERTMS (**E**uropean **R**ail **T**raffic **M**anagement **S**ystem) [25], který se skládá:

1. z evropského vlakového zabezpečovače ETCS (**E**uropean **T**rain **C**ontrol **S**ystem)
2. z bezdrátového systému přenášejícího (nejen) data pro ETCS, tzn. GSM-R (**G**lobal **S**ystem for **M**obile Communication for **R**ailway), obdoba „civilní“ sítě elektronických komunikací určené výhradně pro železniční provoz.

Rodina norem TSI má následující rozsah [26]:

1. strukturální oblasti:
    a. infrastruktura (týká se zejména manažera železniční infrastruktury, dále jen „MI“)
    b. energie (týká se i železničního osobního dopravce, a to z pohledu chytrých digitálních elektroměrů nebo měřáků (zatím) fosilních paliv na hnacích

drážních vozidlech a bezdrátového přenosu dat z vozidel na stacionární část IS)

c. traťové řízení a zabezpečení (část ERTMS na straně MI),
d. palubní řízení a zabezpečení (část ERTMS na straně dopravce)
e. železniční vozidla (včetně ICT prvků a IS umístěných na vozidlech, a to včetně průmyslových počítačů dedikovaných pro obsluhu subsystémů vozidla, jako jsou trakční motory, brzdy, klimatizace apod.).

2. Funkční oblasti:
    a. provoz a řízení dopravy (týká se především MI),
    b. údržba (netýká se jen údržbového zázemí v depech dopravce, ale i senzorů a diagnostických systémů umístěných na železničních vozidlech. Elektronická diagnostika vozidla je v tomto případě opět provozována na průmyslovém počítači na vozidle s využitím různých čidel a senzorů),
    c. využití telematiky v osobní a nákladní dopravě (zde se jedná pouze o IS, které jsou rozděleny do dvou skupin:
        i. TSI TAP – telematické aplikace v osobní dopravě a
        ii. TSI TAF – telematické aplikace v nákladní dopravě.

Dále pro výrobu, provoz a údržbu (opravy) železničních vozidel – jakožto mobilní části IS – jsou nutné technické normy, které upravují podmínky jak samotných vozidel a jejich infrastruktury ICT (např. vozidlové sběrnice), tak jednotlivých komponent ICT (např. pro průmyslový počítač pro řídící vozidlový systém se budou týkat normy elektromagnetické kompatibility). Z typicky technických norem týkajících se železničních vozidel lze uvést konkrétní příklady:

1. rodina norem ČSN EN 62580 – Elektronická drážní zařízení – Palubní multimediální a telematické subsystémy pro dráhy,
2. rodina norem ČSN EN 61375 - Elektronická drážní zařízení – Vlaková komunikační síť (TCN); jednotlivé normy jsou pak zaměřeny na daný typ sítě, jako Ethernet, CAN sběrnice, MVB (multifunkční vozidlová) sběrnice, WTB (vlaková) sběrnice a další,
3. rodina norem ČSN CLC/TS 50459 - Sdělovací, zabezpečovací a systémy zpracování dat – Evropský systém řízení železniční dopravy; jednotlivé normy jsou pak zaměřeny na jednotlivé části systému ERTMS, tzn. ETCS a GSM-R v různých pohledech (jako např. rozhraní strojvedoucí – vlak),

4. rodina ČSN EN 62625 – Elektronická drážní zařízení – Systém palubního záznamu jízdních dat.

Tyto a další zde neuvedené normy, se pak mohou kombinovat s technickými normami, pro daný typ zařízení jako např. uvedená kombinace u kamerových systémů:

1. ČSN EN IEX 63033-2 Vozidlové multimediální systémy – Řidící systém monitorování – Část 2: Kamerové rozhraní a metody záznamu,
2. ČSN EN IEC 62676-5 Dohledové videosystémy pro použití v bezpečnostních aplikacích – Část 5: Specifikace dat a kvalita obrazu pro kamerová zařízení.

Stacionární část železničních IS pokrývají normy běžných IS popsaných výše, doplněných o normy pro datovou elektronickou komunikaci mezi stacionární a mobilní části IS (jako např. pro GSM-R popsané výše).

2.2.2 Vnitřní předpisy

Další možnou dokumentací, která doplňuje právní rámec po stránce interních normativních aktů, jsou vnitřní předpisy. Ty mohou vycházet zejména:

1. ze struktury výše popsaných normativních aktů, doplněné o patřičný detail příslušné organizace, tzn. např. konkrétní bezpečnostní politiky konkrétního subjektu, konkrétní krizové scénáře apod.
2. z povinností, které vyplývají z certifikace zavedení určitých norem a standardů, např. popis procesů nebo stanovení osobní odpovědnosti konkrétních zaměstnanců organizace v rámci certifikace (recertifikace) norem ISO,
3. z certifikace dalších, přísnějších pravidel a opatření v organizaci, např. provedení a certifikace bezpečnostní prověrky Národního bezpečnostního úřadu (NBÚ) u dané právnické osoby,
4. z technických detailů přijatých standardů, např. ze standardu komunikačního protokolu vozidlového modemu je promítnut do interní směrnice provozovatele železničního vozidla.

3 Analýza informačních systémů v železniční osobní dopravě

3.1 Informační systémy železničních osobních dopravců

IS a ICT pro jednotlivé železniční osobní dopravce budou shodně vycházet jako řešení stejných nebo podobných potřeb s pokrytím obdobných procesů, nicméně se budou lišit svým rozsahem a detailem řešení. Pro modelování bezpečnostních aspektů IS a ICT v železniční osobní dopravě bude za účelem naplnění cílů této diplomové práce přihlíženo spíše k řešení velkého dopravce typu Českých drah, a.s. (dále jen „ČD“) a to z důvodu komplexního pohledu na tuto problematiku.

3.1.1 Skupiny IS a ICT

Níže popisované IS a ICT řešení bude zahrnovat různé pohledy na zkoumanou problematiku. V jednotlivých konkrétních případech se nebude jednat o taxativní výčet IS a aplikací, ale o nejzásadnější ukázky daného řešení. Většina ukázek bude demonstrována na prostředí ČD, i když se nejedná o plnohodnotný popis řešení IS a ICT tohoto národního železničního dopravce.

Hlavním pohledem na skupiny IS a ICT řešení je procesní členění, kdy jsou IS rozděleny do skupin podle procesů a potřeb dopravce:

1. Obchodní IS: jedná se o systémy, které pokrývají obchodní činnosti ve smyslu prodeje (nikoliv nákupu) dopravních, popř. doplňkových služeb. Velký železniční osobní dopravce pokrývá trhy:
    i. B2C (**B**usiness to **C**ustomer), tzn. klasický maloobchod, zejména prodej jízdenek a místenek, občerstvení a zboží),
    ii. B2G (**B**usiness to **G**overment), tzn. zabezpečení služeb – v tomto případě dopravní obslužnost ve veřejném zájmu – dojednaných se zástupci státu (Ministerstva dopravy ČR) a samospráv (kraje),
    iii. B2B (**B**usiness to **B**usiness), tzn. obchod vůči jiným právnickým osobám, např. prodej jízd zvláštních nebo speciálních vlaků.

    Obchodní IS musí pochopitelně reagovat na specifické podmínky výše uvedených trhů (např. architektura, funkcionality a v konečném důsledku i bezpečnostní

prvky pro e-shop na prodej jízdenek budou mít zcela jiné parametry než systém pro komunikaci s krajskými objednateli služeb). Mezi důležité obchodní IS patří:

a. cenotvorné IS,
b. vlastní prodejní systémy, tzn. prodejní jádro IS a prodejní kanály, a to ve členění:
    i. pokladní IS, a to stacionární (pro prodej na přepážkách) a také mobilní (na přenosných počítačích nebo mobilních telefonech obsluhy vlaku pro prodej za jízdy),
    ii. e-commerce IS, tzn. e-shop,
    iii. aplikace pro mobilní telefony,
    iv. jízdenkové automaty,
    v. kartové systémy (např. v prostředí ČD je velmi rozšířená IN karta),

    Součástí jádra IS a prodejních kanálů jsou rozhraní na agenturní prodej, v prostředí ČD se jedná zejména o prodej přes portál IDOS nebo prodej prostřednictvím cestovních kanceláří. Další kategoriemi obchodních systémů jsou:

c. CRM (**C**ustomer **R**elationship **M**anagement) – IS pro řízení vztahu se zákazníky,
d. evidence povinností a odpovědností, vyplývajících z obchodních smluv s kraji – tyto smlouvy jsou velmi komplikované a obsáhlé, mají stovky až tisíce stran. Vlastní přenesení povinností vyplývajících ze smluv do vnitřních struktur dopravce není bez IS prakticky možné,
e. informační systémy pro cestující, tzn. hlavně elektronické informační tabule a palubní rozhlas pro hlášení informací o jízdě vlaku. Součástí této rodiny systémů bývá i palubní portál, kde si cestující může ověřit dopravní informace, řízeným a bezpečných způsobem se připojí k internetu, může si elektronicky objednat občerstvení nebo využít vlakový entertainment (sledování filmů, hudby nebo hraní her),
f. systém pro výkaznictví vykonaných služeb vůči objednatelům závazkové dopravy – jedná se o rodinu reportovacích nástrojů, za pomoci kterých jsou vykazovány vlakové výkony, prodané jízdenky, zpoždění nebo odřeknutí vlaků, apod.

2. Provozní IS: tato rodina IS slouží pro informatickou podporu vlastních dopravních výkonů, jedná se především o IS:
    a. pro konstrukci tzv. obchodního jízdního řádu (dále jen „JŘ“) – plnohodnotný JŘ pak sestavuje MI (v ČR to je Správa železnic, dále jen „SŽ“) na základě vstupů obchodních jízdních od jednotlivých železničních dopravců,
    b. plánování oběhů vlakových náležitostí, tzn. vlakového personálu a vozidel – na základě sestaveného JŘ dochází k alokaci vlakových náležitostí na konkrétní trasy vlaku, jedná se o velmi sofistikované systémy, které musí brát (v případě personálu) v úvahu tak složité vstupy, jako je zákoník práce, kolektivní smlouva, plán výluk MI apod.,
    c. IS pro provozní plánování – tyto IS jsou určeny na zpřesňování plánu vlakové dopravy, JŘ tvoří de facto dlouhodobý plán (tzn. na rok), ale je potřeba plánovat v krátkodobých (12 nebo 24 hodin) a střednědobých (měsíce, termíny změny JŘ) cyklech.
    d. Dispečerský IS – systém pro vlastní řízení vlakové dopravy a mimořádností, patří sem zejména sledování jízd vlastních vlaků (vč. vlakových náležitostí). V rámci dispečerských IS může být implementován i energetický dispečink, který v reálném čase sleduje spotřeby hnacích drážních vozidel a s tím spojené mimořádnosti (např. krádeže paliva).
    e. IS pro vyhodnocování provozu – jedná se o analýzu vlakové dopravy, kde se sledují odchylky od výše popsaných plánů a navrhují se opatření k eliminaci těchto odchylek.
    f. IS pro přípravu a interpretaci vlakové dokumentace – tyto systémy konvertují JŘ a další pomůcky a podklady (např. tabulku traťových poměrů nebo přehled pomalých jízd) do formátu čitelného na displejích pro strojvedoucí v hnacích drážních vozidlech, popř. na tabletech nebo mobilních telefonech.
    g. Další podpůrné aplikace jako např. IS sčítání cestujících (sběr dat je založen většinou na bázi kamerového systému nebo infračerveného světla, pak se data odesílají ke zpracování do centrálního IS).

3. IS pro řízení lidských zdrojů:
    a. personální IS obsahující především data o zaměstnancích a pracovních smlouvách,
    b. IS pro management a prokazování (ze zákona) odborné a zdravotní způsobilosti (tato data jsou vázána na licenci dopravce pro provozování drážní dopravy); v rámci této skupiny jsou i IS pro rozvoj lidských zdrojů (školení, zvyšování kvalifikace),
    c. docházkové systémy (v železničním prostředí velmi komplikované s ohledem na nepřetržitý směnný provoz a kolektivní smlouvu).
4. Ekonomické IS mají v souvislosti se specifiky železničního dopravce dvě velké skupiny IS:
    a. ekonomické a finanční IS (ve velkých společnostech často řešeno modulárním systémem SAP), zaměřené na ekonomiku, účetnictví, fakturace, řízení cashflow a dluhové služby (treasury), evidenci majetku apod.,
    b. controllingové IS s vnitropodnikovým pohledem na ekonomiku, manažerskými nadstavbami (dasboardy) a reportovacími nástroji.
5. Technické a údržbové IS jsou dedikovány pro technický management vozidel:
    a. základem těchto IS kartotéka vozidel a jejich náhradních dílů,
    b. dále následují IS pro plánování a řízení realizace vozidlové údržby,
    c. systém prediktivní údržby – v podstatě automatizovaný řetězec údržby železničních vozidel, kde na základě vozidlové a infrastrukturní diagnostiky IS automaticky plánují termíny oprav, rezervaci dílů ze skladů a pracovní čety,
    d. skladové IS (s prvky automatické evidence a vydávání ze skladů),
    e. další podpůrné IS, jako evidence čištění vozidel a běžné údržby.
6. Nákupní IS určené jak:
    a. pro rozsáhlý nákup techniky a náhradních dílů (s velmi obsáhlými číselníky) a s propojením na skladové IS,
    b. tak pro (v případě ČD pro všechny nákupy, nebo u všech dopravců např. při čerpání dotačních prostředků) řízení veřejné obchodní soutěže (zde patří zejména správa profilu zadavatele, zveřejňování zadávacích dokumentací a výsledků tendrů).

7. Bezpečnostní systémy se členěním na:
    c. systémy pro vlastní ochranu IS, dat a ICT infrastruktury (antiviry, antispamy, firewally apod.),
    d. monitorovací, dohledové a alertovací nástroje pro aplikace, IT infrastrukturu a sítě (do této kategorie patří např. SIEM),
    e. detekce a evidence kybernetických událostí,
    f. systémy fyzické bezpečnosti, vstupní (kartové) systémy, kamerové systémy,
    g. řízení práv a přístupů k IS a komunikačním sítím a datovým zdrojům (**A**ccess **M**anagement, dále jen „AM“),
    h. identifikace a autorizace uživatelů IS (**I**dentity **M**anagement, dále jen „IM“),
    i. z určitého úhlu pohledu může být i v této kategorii mobilní část zabezpečovacího systému ETCS (vlakový zabezpečovač), i když se na něj vztahují jiné principy, zákony a normy než na ostatní zde uvedené systémy. Je potřeba si ale uvědomit, že jádro vozidlové infrastruktury ETCS tvoří průmyslový počítač se SW kódem (stejně jako u moderních infrastrukturních zabezpečovacích systémech MI).
8. Kancelářské podpůrné IS jsou určeny na podporu běžné administrativní činnosti společnosti, patří sem elektronická pošta, elektronický oběh spisu, evidence smluv a právních případů, dokumentové knihovny a úložiště pro běžnou kancelářskou práci, aplikace projektové kanceláře, nástroje pro telekonference apod.
9. Podpůrné IS pro vlastní chod informatiky, jako např. HelpDesk nebo Service Desk, znalostní báze, aplikace pro modelování procesů nebo SW modelů apod.

Z pohledu umístnění IS lze IS třídit na:

1. stacionární IS – serverové nebo desktopové aplikace,
2. mobilní IS včetně čipových karet a virtualizace těchto karet na mobilní telefonech – tzn. aplikace na mobilních telefonech nebo PDA počítačích,
3. mobilní vozidlové IS – systémy pevně spojené s vozidlem, většinou se jedná o průmyslový počítač a soustavu čidel,

4. komunikační IS – např. speciální komunikační řešení pro přenos dat mezi stacionárními a mobilními vozidlovými IS, telekonferenční IS apod.
5. IS provozované v cloudu, tzn. bez vlastní fyzické HW infrastruktury,
6. IS s využitím technologií virtuální (VR) nebo rozšířené reality (AR), např. pro simulování podmínek výcviku strojvedoucích nebo pro virtuální pomoc při údržbě (např. systémy BIM – informační systém budov).

Z pohledu obsluhovaných procesů v čase lze mluvit o:

1. IS pro plánování,
2. IS pro řízení a operativu,
3. IS pro vyhodnocování a archivaci.

Z úhlu pohledu kybernetické a informační bezpečnosti připadají v úvahu:

1. IS určené kybernetickým zákonem a/nebo úřadem NÚKIB jako ty, které spadají pod tento zákon,
2. IS nespadající pod kybernetický zákon, ale využívající jiné bezpečnostní a právní normy (např. GDPR neboli **G**eneral **D**ata **P**rotection **R**egulation),
3. vlakové zabezpečovací zařízení (jako např. ETCS),
4. ostatní IS.

3.1.2 IS osobních železničních dopravců z pohledu kybernetického zákona

V průběhu let 2020 a 2021 proběhla jednání NÚKIB se zástupci většiny železničních osobních dopravců, kteří provozují pravidelnou linkovou dopravu v ČR, za účelem zpřesnění základní služby, resp. IS základní služby podle kybernetického zákona.

V zásadě všichni tito dopravci byli po jednáních určeni povinnou osobou ve smyslu kybernetického zákona. Pro rozhodnutí byly relevantní parametry uvedené v příloze vyhlášky č. 437/2017 Sb., o kritériích pro určení provozovatele základní služby následovně [14]:

1. v citované části vyhlášky vyhovuje železničnímu osobnímu dopravci druh subjektu „Provozovatel drážní dopravy nebo zařízení služeb podle zákona o drahách“ (tzn. dopravci jsou zde rozšířeni ještě o zařízení služeb, což jsou např.

místa pro čerpání trakční nafty, které na území ČR zabezpečují např. společnosti ČD nebo Arriva),

2. dále jsou upravena speciální kritéria druhu subjektu v písmenech b) a c) následovně: „b) provozovatel železniční dopravy, jehož hlavní činností je přeprava zboží nebo cestujících na tratích transevropské dopravní sítě (TEN-T), systému mezinárodních železničních magistrál (AGC), systému nejdůležitějších tras mezinárodní kombinované dopravy a souvisejících objektů (AGTC) nebo železničního koridoru pro mezinárodní nákladní dopravu (RFC) nebo c) podnik odpovědný za řízení alespoň jednoho zařízení služeb nebo za poskytování alespoň jedné doplňkové nebo pomocné služby podle zákona o drahách.“
3. Dopadová kritéria jsou definována následovně:
    i. „závažné omezení či narušení druhu služby postihující více než 50000 osob,
    ii. závažné omezení či narušení jiné základní služby nebo omezení či narušení provozu prvku kritické infrastruktury,
    iii. hospodářskou ztrátu vyšší než 0,25 % HDP,
    iv. nedostupnost druhu služby pro více než 1600 osob, která není nahraditelná jiným způsobem bez vynaložení nepřiměřených nákladů,
    v. oběti na životech s mezní hodnotou více než 100 mrtvých nebo 1000 zraněných osob vyžadujících lékařské ošetření nebo
    vi. narušení veřejné bezpečnosti na významné části správního obvodu obce s rozšířenou působností, které by mohlo vyžadovat provedení záchranných a likvidačních prací složkami integrovaného záchranného systému.“

U každého osloveného železničního dopravce byly vybrány konkrétní IS (konkrétní údaje o těchto IS nejsou z pochopitelných důvodů zveřejněny), nicméně se dá obecně říci, že se jedná o některé provozní, technické a údržbové IS ve smyslu předchozí podkapitoly této diplomové práce. K těmto IS musí železniční osobní dopravci implementovat opatření a nástroje podle kybernetického zákona, a to s kontrolním termínem 1 (jeden) rok od vydání rozhodnutí NÚKIB.

3.2 Stručná analýza rizik systémů železničního osobního dopravce

Na základě analýzy (popisu) hlavních skupin IS a ICT v podkapitole 3.1.1 bude v dalších částech této diplomové práce provedena stručná a rámcová analýza rizik. Rozsah běžné analýzy rizik pro železničního osobního dopravce velikosti ČD je řádově ve vyšších stovkách až tisících stran, přičemž tato analýza obsahuje velmi citlivé informace, a tudíž z podstaty věci nemůže být zveřejněna mimo okruh vydefinovaných a prověřených osob. Proto bude dále popsaná analýza rizik spíše principiální než konkrétní, nicméně pro cíle této práce dostačující.

3.2.1 Aktiva

Na úvod definice aktiv obecně: podle doporučených metodik pro zpracování analýzy rizik a v kontextu kybernetického zákona je možné rozlišovat 3 (tři) základní kategorie aktiv [16]:

1. primární aktiva jsou informace nebo služby zpracované nebo poskytnuté jednou z kategorií IS definovaných kybernetickým zákonem,
2. podpůrná aktiva – jsou technická aktiva, zaměstnanci a dodavatelé pro implementaci, provoz a rozvoj IS (opět z kategorií IS definovaných kybernetickým zákonem),
3. technická aktiva – jsou technické vybavení, telekomunikační prostředky a programové vybavení IS kategorií definovaných kybernetickým zákonem. Do této skupiny patří i objekty, kde jsou předmětné IS umístěny.

Jak již bylo popsáno v části 3.1.2 této diplomové práce, byly úřadem NÚKIB pro účely odpovědnosti a opatření ve smyslu kybernetického zákona určeny některé provozní, technické a údržbové IS. Dalo by se očekávat, že budou určeny i obchodní IS, jejich ohrožení ale primárně nesplňuje dopadová kritéria ve smyslu vyhlášky č. 437/2017 Sb., o kritériích pro určení provozovatele základní služby – na tuto problematiku se dá totiž nahlížet i v tom slova smyslu, že obchodní IS a činnost s nimi spojená (za účelem zisku) je primárně starost a riziko železničního osobního dopravce (podnikatelské riziko), kdežto ohrožení provozních IS může mít za následek, že nevyjedou vlaky, tudíž se lidé neodstanou do práce, škol, k lékaři, apod. a tak vzniká primárně škoda státu, a to velkého rozsahu (to je upraveno kritériem ve zmíněné vyhlášce dopadem omezení či narušení služby na nejméně 50000 osob a hospodářskou ztrátou vyšší než 0,25 % HDP). Dalším

použitelným dopadovým kritériem ve smyslu výše zmíněné vyhlášky a spojeným s technickými a údržbovými IS je počet možných mrtvých nebo zraněných osob v důsledku ohrožení IS základní služby.

Obě určené kategorie IS však z IT technického pohledu nepředstavují izolovaná řešení, tzn. že navrhovaná bezpečnostní opatření se poměrnou částí dotknout i dalších skupin IS, které poskytují klíčová data nebo služby primárně určeným IS. Jedná se o bezpečnostní IS, některé IS pro řízení lidských zdrojů a podpůrné IS.

Na obchodní IS by se tedy měl železniční osobní dopravce zaměřit také, ale ve svém vlastním zájmu, přičemž může (v rámci harmonizace a standardizace vnitřních podmínek ve společnosti) využít principy vyplývající z kybernetického zákona (např. formou doporučených minimálních technických standardů popsaných v kapitole 2 této diplomové práce).

K samotným nejdůležitějším aktivům:

1. primární aktiva:
    a. informace (číselníky) všech IS a ICT řešení železničního osobního dopravce, zvláště pak informace týkající se určených IS a IS zajišťující vlastní informatickou a kybernetickou bezpečnost,
    b. informace o systémové architektuře IS, komunikačních IS (dále jen KIS) a ICT řešení se zvláštním přihlédnutím k zabezpečení těchto skupin,
    c. informace o možnosti přístupu k jednotlivým IS, informace o heslech a šifrovacích klíčích,
    d. informace zejména o provozních a technických zaměstnancích vykonávajících činnosti provozování drážní dopravy, servisu a údržby železničních vozidel,
    e. informace o jízdních datech a podkladech pro strojvedoucí (zejména sešitové JŘ, tabulky traťových poměrů a seznam pomalých jízd),
    f. informace zahrnující evidenci a popis železničních vozidel s atributy jako evidence údržby, vykonané zkoušky na vozidlech a UTZ (určených technických zařízeních), apod.,
    g. informace o náhradních dílech a jejich dostupnosti a ceně,
    h. informace o trakčních energiích (silová elektrická energie a nafta), jejich dostupnosti a ceně,

i. informace o klíčových dodavatelích (zejména pak IS a služeb, vozidel, náhradních dílů a energií) v jakémkoliv dodavatelském módu,
j. informace o plánovaných vlakových výkonech, zejména pak trasy vlaků (JŘ), plán nasazení vozidel a plán nasazení personálu,
k. informace o skutečném vlakovém provozu (např. polohy vlaků, připravenost vlaků k výkonu, mimořádnosti v provozu a mimořádné události).

2. Podpůrná aktiva:
    a. vlastní určené a související IS, tzn. aplikace a s nimi související komponenty IS, jako DB, OS, vývojové a obslužné nástroje, technické, uživatelské a bezpečnostní dokumentace atd.
    b. vlastní personál spravující výše uvedené IS, klíčoví uživatelé IS a garanti aktiv,
    c. dodavatelské společnosti a externí osoby podílející se na dodávce, implementaci, servisu, údržbě a podpoře výše zmíněných IS,
    d. technická HW a telekomunikačních infrastruktura nutná pro řádné fungování výše zmíněných systémů (a to včetně prvků ICT umístěných na železničních vozidlech),
    e. objekty, kde je umístěna infrastruktura pro provoz IS a ICT, tzn. serverovny, serverové farmy, cloud a rovněž železniční vozidla.

V rámci definice a popisu aktiv dochází zároveň k jejich klasifikaci. Ta je postavena na přiřazení klasifikační úrovně ke každému aktivu ve stupnici:

1. nízká
2. střední,
3. vysoká,
4. kritická.

Klasifikační stupnice může být doplněná ještě z různých úhlů pohledu jako:

1. hodnocení důvěrnosti (jak jsou aktiva přístupná),
2. hodnocení integrity (jaké aktivum vyžaduje ochranu a jak narušení integrity aktiva má dopad na další, zejména primární aktiva),
3. hodnocení dostupnosti (zda dostupnost či nedostupnost aktiva z pohledu času naruší další části systému nebo procesy), apod.

Aktiva musí být řádně evidována, systém evidence se vztahuje na všechny druhy aktiv. Evidence aktiv by měla obsahovat:

1. ID aktiva a další identifikační údaje (např. datum identifikace),
2. název a popis aktiva,
3. typ aktiva (primární, podpůrné/technické),
4. klasifikace aktiva (z pohledu důvěrnosti, integrity a dostupnosti),
5. role spjaté s aktivy: vlastník, správce, provozovatel, garant aktiva a
6. hodnota aktiva.

3.2.2 Hrozby

Hrozby v prostředí železničního osobního dopravce, s ohledem na definici aktiv (přiřazení hrozeb k aktivům), mohou být definovány následovně:

1. fyzické hrozby:
    a. fyzické zničení HW na železničních vozidlech jako důsledek železničních nehod, vandalismu, extrémního počasí (přehřátí nebo zatopení HW, umístěného zejména poblíž strojovny – např. vozidlový počítač, nebo poblíž oken a dveří – např. displeje informačního systému pro cestující), požáru apod.
    b. zničení nebo selhání HW nebo komunikací napojených na stacionární části IS, v důsledku lidské činnosti (např. překopnutí kabelu), živelné události (povodeň, požár), selhání HW apod.,
    c. výpadek napájení doprovozen selháním nebo absencí záložních energetických zdrojů jako baterie nebo dieselagregát,
    d. důsledky špatné údržby a servisu HW prvků,
    e. úmyslné poškození, jako krádež nebo sabotáž,
    f. odposlechy, neoprávněné pořízení obrazového záznamu, zfalšování dat.
2. Softwarové (elektronické) hrozby:
    a. vnější hrozby, zejména pak kybernetický útok (hacking),
    b. softwarové chyby (špatně nebo nedůsledně naprogramový SW),
    c. zanedbaná SW údržba a servis (např. díky neaktualizovanému OS nebo nenainstalovanou novou verzí SW a bezpečnostních záplat).
3. Hrozby z pohledu, kdo by je mohl a jak způsobit:
    a. hrozby, za kterými stojí lidský element, ať už úmyslně nebo ne,

b. hrozby prostřednictvím šířícího se škodlivého kódu (už bez lidského zásahu),
c. únava materiálu, selhání techniky.

V rámci definice (identifikace) hrozeb se určuje (odhadem, na základě zkušenosti, jinou metodou), s jakou pravděpodobností (v %) se může daná hrozba vyskytnout.

3.2.3 Identifikace zranitelnosti (slabin)

V návaznosti na definovaná aktiva a hrozby přichází na řadu další krok, a tím je identifikace zranitelnosti (slabin) určených aktiv. V zásadě se hledají slabá místa, kde neexistuje nebo není známá ochrana, popř. se ochrana aktiv jeví jako nedostatečná. Zranitelnost v konkrétních případech může vyplynout např. z:

1. auditu kybernetické bezpečnosti,
2. penetračních testů, kdy probíhá řízeným způsobem simulovaný kybernetický útok na IS nebo jeho část,
3. z kontrolní činnosti,
4. informací získaných po skutečném kybernetickém incidentu (útoku) apod.

V prostředí železničního osobního dopravce se může jednat např. o:

1. zastaralost platforem IS – některé speciální drážní IS nemají alternativu na trhu a pakliže dopravce neinvestoval do vývoje nové verze takové aplikace, dostává se do nebezpečného stavu, kdy např. není podporován OS, nejsou vydávány bezpečnostní záplaty, neexistuje vhodný HW (současné počítače mohou být na historické aplikace příliš výkonné a silné, proto se v těchto případech používají různé emulátory nebo virtuální počítače, nebo se výkon počítače softwarově omezuje). Na aplikaci v takovém stavu nejdou použít účinné moderní nástroje kybernetické ochrany (nejsou mezi sebou kompatibilní),
2. zastaralost a různorodost HW infrastruktury (na bázi průmyslových počítačů) na železničních vozidlech. Cena výroby a implementace takových počítačů se nedá srovnat s řešením pro průmysl nebo s běžně dostupnou HW infrastrukturou. Zásadní rozdíly spočívají v:
    a. robustní provedení tohoto HW (vzhledem k tomu, že jsou tyto počítače umístěné např. ve strojovně lokomotivy, musí odolat vibracím, otřesům, vlhkosti a velkému výkyvu teplot – podle technických norem od -40 °C až

po 70 °C). V konstrukci takového počítače nesmí být žádné pohyblivé části, proto je velmi obtížné např. chlazení nebo větrání,

b. malosériovosti – počítačů takové konstrukce a druhu se z podstaty věci moc nevyrobí, existuje jen minimum opakovaných řešení.

Důsledkem zmíněných odlišností je až několik generací průmyslových počítačů na jedné flotile vozidel jednoho železničního dopravce. Proto je příprava kybernetické ochrany technicky i finančně náročná.

3. Konkrétní HW řešení na železničních vozidlech nemá takovou odolnost, která je pro dané řešení třeba. Jak bylo vysvětleno v předchozím bodě, průmyslové počítače pro železniční provoz musí být velmi odolné. Existují ale výjimky, kdy požadovaný HW na vozidlech nahrazuje kancelářské řešení, typickým příkladem je Wi-Fi router. Není-li pořízena odolná varianta, životnost takového zařízení se díky drsnému provoznímu prostředí radikálně snižuje (až na nižší jednotky měsíců), nemluvně o nemožnosti začlenit toto zařízení do systému kybernetické ochrany.
4. Funkcionality a data pro jedno konkrétní odvětví nejsou v jednom logickém IS, ale jsou roztříštěny mezi několik řešení s různou kvalitou kybernetické odolnosti. Důsledkem tohoto stavu je příliš mnoho rozhraní, vložených provizorních pomocných aplikací, přechodových můstků a další komplikované a nestandardní vlastnosti.
5. Redundance některých IS, které vznikly např. absencí cílového konceptu IS, postupnou implementací IS do různých organizačních jednotek apod. Typickým příkladem jsou docházkové IS, jiný systém je používán pro strojvedoucí, jiný pro vlakové čety a jiný pro personál zajišťující opravy železničních vozidel. Opatření kybernetické bezpečnosti bude muset být (v některých konkrétních případech) rovněž redundantní, tzn. zbytečně drahé a komplikované.
6. Vendor Lock-In neboli přílišná závislost na jednom dodavateli IS.

3.2.4 Dopady

Kvantifikace dopadů může probíhat buď odhadem nebo exaktním výpočtem. Odhadová metoda se používá zejména pro kvantifikaci dopadů z ekonomického hlediska – např. vyčíslení finančních dopadů jako je pokuta nebo sankce.

Výpočtová metoda vychází z parametrů konkrétního aktiva (kterému jsou přiřazeny body nebo %) a je založena na vzorci pro výpočet hodnoty dopadu aktiva [27]:

$$D_{A1} = MAX\ (A_{A1};\ I_{A1};\ C_{A1}) \qquad (3.1)$$

Vysvětlení ke vzorci:

- D_{A1} je hodnota dopadu aktiva pro aktivum A1,
- C_{A1} hodnocení důvěrnosti aktiva pro aktivum A1,
- I_{A1} hodnocení integrity aktiva pro aktivum A1,
- A_{A1} hodnocení dostupnosti aktiva pro aktivum A1.

3.2.5 Míra rizika

Jelikož se zde uvedená stručná analýza rizik železničního osobního dopravce pohybuje v oblasti principů a modelových (byť konkrétních) příkladech, a nikoliv číselných hodnot, nelze stanovit konkrétní míru rizika ani na rizika navazující scénáře. Lze ale opět využít možnost principu.

Pro výpočet míry rizika doporučuje NÚKIB metodiku, kdy k hrozbám, zranitelnosti a dopadům (vše pochopitelně provázáno k aktivům) jsou přiřazeny (výpočtem, odhadem nebo jinou metodou) exaktní číselné hodnoty (většinou vyjádřeno v % nebo bodech), které se dosadí do následujícího vzorce [28]:

$$riziko = dopad \times hrozba \times zranitelnost \qquad (3.2)$$

Výsledek výpočtů se porovná se stupnicí kvalifikace rizik. Tato stupnice definuje kategorie (druhy) rizika, přičemž každá kategorie rizika má pak svoje pravidla, postupy a další specifika. Kvalifikaci rizik si určuje každá organizace podle svých vlastních potřeb, nicméně NÚKIB doporučuje kategorie rizik uvedené v následující tabulce:

Tab. 3.1 Stupnice kvalifikace rizik

Kvalifikace rizika	Hodnota v %
Nízké	do 25 %
Střední	26–50 %
Vysoké	51–75 %
Kritické	76–100 %

Zdroj: [28]

3.2.6 Krizové scénáře, řízení rizik

Krizové scénáře jsou manuálem pro personál obsluhující nebo pracující s IS. Krizový scénář nikdy nemůže poskytnout dispozice a pokyny pro všechny eventuality, ale jejich principy, pakliže jsou dobře vydefinované, se dají aplikovat na předem určené situace – ty odpovídají seznamu hrozeb z analýzy rizik. Čím větší má hrozba odhadnutou pravděpodobnost nebo četnost, tím propracovanější by měl být krizový scénář.

Základem každého krizového scénáře (nebo nadstavbou všech krizových scénářů) je:

1. komunikační matice, tzn. ke komu se informace o nastalé situaci musí vždy dostat (podmínkou jsou dobře nadefinované role),
2. popis prvotních nezbytných kroků, které se musí provést ihned po naplnění hrozby (např. jako vypnout IS, odpojit KIS, odpojit zdroj napájení, hasit nebo naopak nehasit HW prostředky, které zachvátil požár apod.),
3. kroky nezbytné k ochraně nebo záchraně aktiv – např. po železniční nehodě, kdy je poškozen průmyslový počítač na lokomotivě, se pokusit stáhnout data, která nebyla z vozidla ještě před vzniklou situací odeslána.

Prostředí železničního dopravce je na krizové plány a mimořádné události zvyklé. To je dáno povahou a organizací železniční dopravy, kdy pro krizové provozní situace (většinou nehody a jejich následky) nebo nestandardní průběh přepravy (např. jízda zvláštních vlaků, přeprava jaderného paliva či jiného velmi bezpečného zboží) byly historicky zpracované krizové scénáře a pokyny, jen s tím rozdílem, že v době před nasazením informačních technologií byly tyto plány součástí provozní a technické dokumentace každého dopravního bodu (železniční stanice, výhybny, jiné dopravny), citlivější z těchto plánů pak byl uloženy v trezoru a zapečetěny a aktivovaly se na základě pokynu nadřízené složky.

Zpracování krizových plánu kybernetické bezpečnosti v prostředí železnice bude muset být jasně strukturované a vzhledem k tomu, že v tomto prostředí je nasazeno obrovské množství IS a aplikací (v řádech stovek), měly být některé scénáře spíše stavěné pro skupiny IS, v definovaných případech (jako u IS podléhající pod kybernetický zákon nebo u větších, komplikovanějších IS) pak scénáře přímo pro konkrétní IS nebo ICT řešení.

Žádný z krizových plánu dopředu nemůže postihnout všechny eventuality, které mohou nastat. Proto je nutné krizové plány pravidelně aktualizovat, podobně jako analýza rizik

(na základně auditu kybernetické bezpečnosti, penetračních testů, informací a zkušeností po kybernetickém útoku, kontrolní činnosti apod.).

Krizové plány, např. vzhledem k velikosti a komplikovanosti IS, množstvím jeho vazeb nebo závěrům vyplývající z analýzy rizik, budou rovněž obsáhlé a komplikované. Aby nebylo při tvorbě krizových plánů nic opomenuto (aktiva, souvislosti, role apod.), existují aplikace (IS) přímo vyvinuté pro tvorbu a generování analýzy rizik vč. krizových plánů. Výhoda takového řešení je pak propojení IS analýzy rizik / krizových plánů s dalšími interními IS v dané společnosti, čímž dochází k přirozené a rychlé implementaci základů bezpečnostní problematiky.

3.2.7 Lidské zdroje

Z pohledu lidských zdrojů se mohou identifikovat čtyři základní skupiny personálu, který pracuje s IS, a tudíž přijde do styku s kybernetickou bezpečností:

1. informatici (technický personál), se všemi v úvahu připadajícími rolemi (např. analytici, programátoři, vývojáři HW, administrátoři IS, architekti včetně architekta kybernetické bezpečnosti atd.),
2. bezpečnostní personál, s rolemi jako bezpečnostní ředitel, analytik, a manažer kybernetické bezpečnosti. Tato speciální role nesmí být pod stejným řízením nebo ve stejné skupině jako architekt kybernetické bezpečnosti (kvůli nezávislé kontrole a auditní stopě),
3. klíčoví uživatelé IS (někdy též označovaní jako superuživatelé), tzn. pokročilí uživatelé IS, kteří jsou schopni se podílet svým specifickým know-how na zadání pro tvorbu nebo změnu IS, jsou velmi dobrými testery (kvůli zpětné vazbě vývojářům),
4. běžní uživatelé IS.

Všechny výše zmíněné role musí být zapojeny do přípravy a procesu kybernetických opatření, některé role pochopitelně pasivně (běžní uživatelé IS), např. formou školení. V praxi se ukazuje, že pouhý teoretický přístup (tzn. tvorba dokumentace, školení, nebo i přijímání zkušeností od třetích osob) nestačí. Proto je potřeba:

1) zaujmout, vtáhnout personál do děje,
2) dát přehlednou strukturu, ve které se budou všechny role vidět,
3) získat praktické zkušenosti.

Bezpečnostní odborníci proto doporučují provádět simulace kybernetických incidentů (tzv. bojové hry), kdy na speciálním prostředí (např. testovacím nebo kopii instance produkčního prostředí) probíhá řízený útok na IS, jedna skupina útočí, druhá brání. Bránící skupina by měla postupovat v souladu s krizovými scénáři. V těchto okamžicích se ukazuje, že reakce nezkušené obsluhy může být pomalá až zmatečná. Navíc bývá dobrým zvykem zapracovat reálné zkušenosti, byť ze simulovaného kybernetického útoku, do krizových plánů.

Součástí bojových her, ale někdy i (poněkud drsného) testování IS, bývá ověření postupů plánu kontinuity činností (BCP) a plánu obnovy (DRP). Ověření spočívá ve vypnutí a následovném zapnutí IS (např. odpojením od zdroje napájení vč. napájení záložního), kdy personál musí zvládnout dostat IS zpět do produkční činnosti, přičemž nejtěžší problematikou je v tomto případě záchrana dat (tedy aktiv).

Některé bojové hry je vhodné z pohledu komplexnosti realizovat i za účasti dodavatelů IS.

3.2.8 Dodavatelé

Dodavatelé jsou z pohledu analýzy rizik zařazeni do podpůrných aktiv a v jistém slova smyslu je na ně pohlíženo jako na vlastní personál. Výběr dodavatele IS předchází pečlivá příprava, v rámci vyhodnocení nabídek se pak posuzuje mj. důvěryhodnost a kompetence, zejména pak prostřednictvím:

1. referencí (realizovaných IT zakázek u jiných zákazníků),
2. certifikací kompetencí nebo oprávnění, např. certifikace IT vendorů o zaškolení dodavatele do příslušných technologií, nebo osvědčení Národního bezpečnostního úřadu (tzv. bezpečnostní prověrka pro práci s utajovanými informacemi), apod.,
3. technického týmu, kdy dodavatel předkládá životopisy, certifikáty a další podklady související s jeho personálem.

Samostatnou kategorií výběru a prověřování IT dodavatelů jsou veřejné zakázky, kde navíc vstupuje do hry příslušná legislativa [29].

Někteří zadavatelé sledují své IT dodavatele i z pohledu opakovaných dodávek, za pomoci tzv.:

1. white listů, kdy uchazeč o dodávku IS se musí nejdřív kvalifikovat nebo certifikovat (tzn. je prověřován), pak teprve může předkládat (i opakovaně) obchodní nabídky,
2. black listů, kdy při opakovaném závažném pochybení ze strany dodavatele není tomuto již povoleno předkládat další nabídky.

Zvláštní problematikou související s dodavateli IS je tzv. Vendor Lock-In neboli přílišná závislost na jednom dodavateli. Tato závislost se může projevit jak v cenách dodávaného řešení (tzn. dodavatel není ničím motivován nabízet běžnou tržní cenu, a tak se cena zvyšuje, nakolik zákazník snese), tak v bezpečnostních otázkách. To se totiž týká vlastního technického řešení IS, kdy může být zadavatel pod diktátem (neochotou) dodavatele a práce spojené s IS jsou pak spíše definovány podle dodavatele než zadavatele. Zvlášť citlivá je tato otázka v případě velkého množství dodávaných ICT komponent. Je znám případ, kdy Německé dráhy (Deutsche Bahn) objednávaly průmyslové počítače do lokomotiv (vč. displejů pro strojvedoucí). Aby se vyhnuly Vendor Lock-In, tak účelově rozdělily flotilu svých vozidel na dvě skupiny, přičemž každá tato skupina měla svého dodavatele. Tím Německé dráhy na jednu stranu diverzifikovaly riziko Vendor Lock-In, na druhou stranu musely důkladněji popsat poptávané řešení a do svých dalších IS integrovat dva dodavatele místo jednoho.

4 Telekomunikace a přenos dat

4.1 Telekomunikací v prostředí železničního dopravce

Velké železniční podniky typu ČD historicky budovaly své vlastní velké datové sítě. Díky transformaci železnic se na bázi evropských legislativních balíčků a následně tzv. transformačního zákona od sebe oddělily ČD a SŽ [30]. Tím se ale oddělil i osud velkých železničních datových sítí. Část, kterou dnes buduje a spravuje SŽ, je primárně určena pro podporu řízení vlakového provozu a její elementy mají status kritické informační infrastruktury (KII) a kritické komunikační infrastruktury (KKI) podle kybernetického zákona.

Sítě v dnešním majetku ČD si prošly konsolidací se sítěmi budované soukromým sektorem, a to prostřednictvím původní organizační složky ČD Správa železničních komunikací na straně jedné a společnostmi ČD – Telekomunikace (původně Tiscali) na straně druhé. Následoval vznik společného podniku ČD – Telematika a.s. (dále jen „ČD-T“), který vybudoval druhou největší optickou síť v ČR (největší síť je v rukou společnosti CETIN, původně Telefonica). V roce 2020 došlo k vykoupení minoritních podílů ČD-T od soukromých vlastníků (PPF) a nyní je ČD-T stoprocentní (100 %) dceřinou společností ČD. Síť ČD-T je využívána spíše pro komerční účely než pro účely železniční dopravy, a jen některé prvky a služby jsou součástí kritické infrastruktury (např. komunikační infrastruktura veřejné správy neboli KIVS).

Pro komunikaci v prostředí železničního osobního dopravce se vlastní infrastruktura využívá hlavně v lokálních pracovištích (depa, opravny, provozní a administrativní pracoviště). Pro datovou a hlasovou komunikaci mezi těmito pracovišti mezi sebou, vnějšími subjekty a dopravními prostředky s personálem (železniční vozidla, strojvedoucí, vlakové čety), jsou využívány komerčně dostupné služby na trhu.

Některé skupiny IS, např. IS pro pak plánování oběhů vlakových náležitostí nebo IS pro řízení lidských zdrojů, komunikují pouze v rámci vnitřní sítě. Naproti tomu obchodní IS jsou vystaveny vnějšímu světu. Fungování IS z pohledu komunikace uvnitř nebo vně interní datové sítě odpovídá i míra zabezpečení těchto IS. U některých IS došlo v průběhu času se změnou dopravního modelu v železniční osobní dopravě i výrazné změně systému komunikace (zde je míněno zapojení objednatelů veřejné služby – dopravní obslužnosti – do aktivní účasti na dopravních procesech). Příkladem je dispečerský IS, který byl dříve

typickou ukázkou IS pouze s interní komunikací. S integrovanými dopravními systémy v jednotlivých krajích vznikly i krajské dopravní dispečinky, jejichž IS jsou úzce propojeny s dispečerskými IS všech dopravců, zapojených do daného dopravního systému (jedná se o všechny druhy dopravy, nejen železniční). Datová výměna a komunikace se v tomto případě týká zejména pohybu a polohy dopravních prostředků, informací o mimořádnostech v dopravě a pokynech s cílem koordinovat dopravce mezi sebou (např. čekání jedné dopravní linky na druhou pro přestup cestujících v případě, že jedna z linek je opožděna).

Pro datovou komunikaci v železničním prostředí se používá referenční model ISO/OSI, který je znázorněn na následujícím schématu:

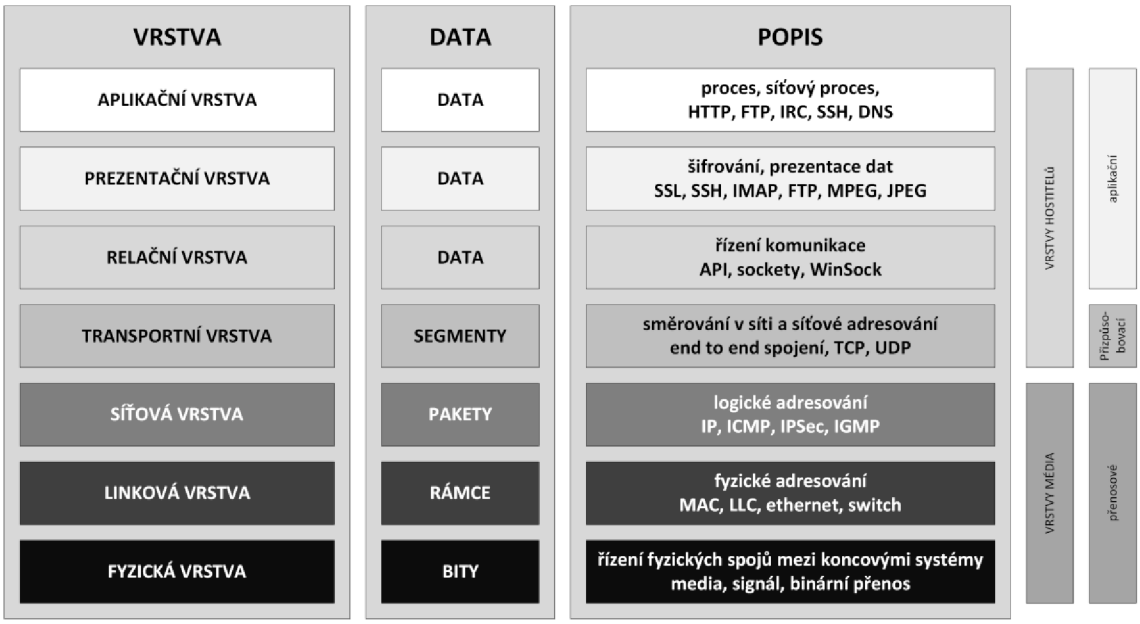


Schéma 4.1 ISO/OSI model
Zdroj: vlastní zpracování

Tento model, bez ohledu na jeho stáří, je výhodný v tom smyslu, že jednotlivé vrstvy jsou nezávislé, a tudíž:

1. v některých případech se dají využít standardizované řešení (např. od dodavatelů IS a ICT), nebo
2. naopak ve specifických případech se využije specializované řešení vhodné pro železniční sektor.

Bezpečnost datové komunikace je zajištěna za pomoci šifrování. Bohužel se daný typ šifrování váže vždy ke konkrétnímu systému nebo skupině IS. Tento stav se dá do budoucna odstranit nasazením jednotných nebo společných kryptografických nástrojů.

V prostředí železničního osobního dopravce se vyskytují následující typy komunikací:

1. datová komunikace IS mezi sebou. Jak bylo popsáno výše, některá komunikace probíhá pouze po interních sítích a některá komunikace s IS nebo uživateli vně systému,
2. datová komunikace v rámci železničního vozidla nebo soupravy – jedná se např. o jednotné ovládání informačního systému pro cestující (informační tabule, vlakový rozhlas), sběr diagnostických údajů z různých částí soupravy nebo vozidla apod. Tato komunikace probíhá na interních vlakových sítích,
3. datová komunikace mezi IS, popř. ICT na železničním vozidle a stacionárními IS, např. odesílání polohy vlaku do dispečerského IS, nebo diagnostické údaje vozidla do údržbového IS,
4. datová komunikace mezi mobilními zařízeními a stacionárními IS, např. nahrání a aktualizace sešitových JŘ do tabletů strojvedoucích nebo dispozice vlakové čety na aplikaci mobilního telefonu ohledně přestupu cestujících či informace o mimořádných situacích,
5. hlasová komunikace s využitím běžných komerčně dostupných prostředků (mobilní telefony s technologií GSM, pevné telefonní linky),
6. hlasová komunikace s využitím datových přenosů (Voice over IP), tzn. volání speciálními, zejména pak instantními nástroji, upravenými pro železniční prostředí. Tyto komunikační nástroje mohou být zaintegrovány přímo do IS, např. pro volání dispečera strojvedoucího je možné využít tuto funkcionalitu v dispečerském IS,
7. služební hlasová komunikace na vyhrazených pásmech – jedná se o řešení komunikace mezi dispečery MI (SŽ) a strojvedoucími jednotlivých dopravců, nebo mezi strojvedoucími a dalším provozním personálem, např. posunovači. Zejména na koridorových tratích je za tímto účelem využívána technologie GSM-R (se speciálními drážními funkcemi), tam, kde tato technologie není, se používá původní duplexní analogový traťový rádiový systém (též „TRS“), který pracuje v pásmu UHF 450 a 460 MHz radiové topologie typu stuha,
8. datová komunikace GSM-R jak pro potřeby zabezpečovacího systému ETCS (v rámci ERMTS), nebo pro speciální drážní aplikace, např. pro přenos dat z elektroměrů elektrických hnacích drážních vozidel do centrálního IS SŽ (jakožto distributora trakční elektrické energie) pro účely řízení odběrů elektrické

energie na celé železniční sítí a pro účely vyúčtování spotřeby jednotlivým železničním dopravcům.

4.2 Specifika železničních telekomunikací

Pro některé druhy dříve popsaných komunikací existují specifické vlastnosti nebo řešení, z nichž nejdůležitější jsou popsány v dalších částech této diplomové práce níže.

4.2.1 Železniční síť GSM-R

Železniční síť GSM-R je služební komunikační síť určená hlavně pro:

1. přenos dat zabezpečovacího zařízení ETCS z míst na trati nebo dispečerského pracoviště MI na stanoviště strojvedoucího (jako jsou např. návěstní znaky povolující nebo zakazující jízdu, nebo znaky které stanovují rychlost vlaku), údaje pro bezpečnou jízdu vlaku (jako např. volný nebo obsazený traťový oddíl před vlakem nebo hlídání vzdálenosti vlaků mezi sebou), povely vlaku pro nouzové situace (zejména adresná funkce „Stop“ nebo tzv. „Generální stop“ kdy může dispečer MI na dálku zastavit konkrétní vlak nebo skupinu vlaků v dané oblasti),
2. hlasovou uzavřenou komunikaci železničního provozního personálu, jak bylo popsáno v předchozí podkapitole této diplomové práce,
3. datovou služební komunikaci, jak bylo popsáno v předchozí podkapitole této diplomové práce.

Tento komunikační systém vznikl jako řešení pro interoperabilitu železniční vlakové dopravy v Evropě, kdy původně každý členský stát používal svůj vlastní analogový rádiový systém, který pracoval na frekvenci přidělené telekomunikační autoritou v dané zemi. Výsledek byl pak takový, že železniční vozidlo jedoucí přes území několika států muselo mít na palubě tolik rádiových zařízení, přes kolik států se uskutečňovala jízda (a tedy kde vozidlo bylo povoleno a certifikováno pro bezpečný provoz). Vyskytly se případy, že takové železniční vozidlo mělo 4 (čtyři) a více rádiových modulů.

GSM-R je proto společným standardem, který v rámci širší technické a obchodní harmonizace vychází ze specifikací GSM a je doplněný o specifické drážní funkce na bázi specifikace EIRENE – MORANE (**E**uropean **I**ntegrated **R**adio **E**nhanced **NE**twork - **Mo**bile **Ra**dio for **Ra**ilways **N**etworks in **E**urope) [31]:

1. bezvýpadková komunikace pro rychlost komunikujícího vozidla do 500 km/h,

2. pracovní kmitočty v trochu jiných pásmech než GSM (876 MHz — 880 MHz pro vysílání dat / uplink a 921 MHz — 925 MHz pro příjem dat / downlink,
3. mezi specifické drážní funkcionality patří:
    a. správa číslování podle funkcí (nevolá se telefonním číslem, ale číslem vlaku nebo jiným přiděleným kódem), a to nejen adresně na jednoho účastníka, ale na okruh účastníků (např. v dané oblasti)
    b. potvrzení ukončení hovoru (tzn. informace, zda účastník hovor ukončil sám, nebo je mimo signál či má slabou baterii apod.)
    c. režim posun – pro komunikaci v rámci posunu, do které nemusí být zapojen MI,
    d. režim přímé komunikace – obdoba analogové vysílačky, kdy nemusí být k dispozici síť GSM-R a zařízení v dosahu komunikují mezi sebou napřímo.
4. Další specifické režimy GSM-R jsou:
    a. PtP Call (Point-to-Point Call): běžné volání jako přes GSM
    b. VGCS (Voice Group Call Systém): skupinový hovor jako u vysílaček,
    c. VBS (Voice Broadcast System): podobné jako VGCS, ale mluví jen iniciátor volání (ostatní pouze poslouchají),
    d. REC (Railways Emergency Call): speciální VGCS s vysokou prioritou (vypíná ostatní komunikace) v případě nouze,
    e. řízení priorit výše uvedených režimů.

Typové vybavení železničního vozidla z pohledu rádiových modulů je zobrazeno na následujícím schématu:

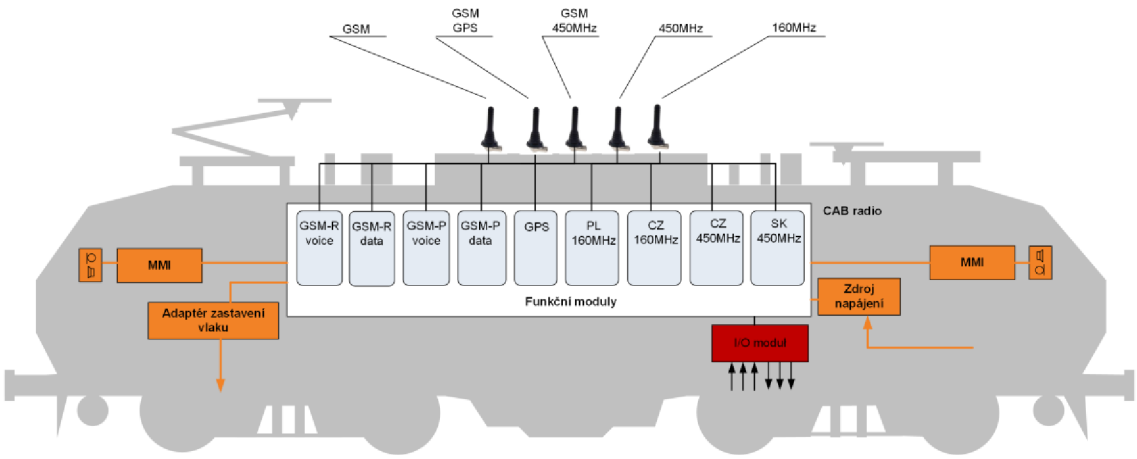


Schéma 4.2 Vybavení železničního vozidla rádiovými moduly

Zdroj: vlastní zpracování podle RPP International

4.2.2 Železniční bezdrátová přenosová síť

S příchodem různých ICT řešení, které se daly využít pro komunikaci mezi stacionární a vozidlovou mobilní částí IS, nastala potřeba řešit univerzálnost datových přenosů. Touto problematikou se začaly zajímat ČD kolem roku 2005 v rámci projektu Železniční bezdrátová přenosová síť (dále jen ŽBPS).

V rámci ŽBPS by tak bylo nutné:

1. vybavit železniční vozidla univerzálním ICT řešením, zahrnující především komunikaci GSM, GSM-R a Wi-Fi (tato sada by mohla být později rozšířena o další technologie, jako např. **I**nternet **o**f **T**hinks – IoT, a dalšími),
2. vybavit komunikační vstupní bod (**A**ccess **P**oint **N**ame – APN) na straně stacionární části IS logikou, která by vybrala příslušný komunikační kanál podle alokace vozidla a rozsahu, popř. druhu přenášených dat.

V praxi by to tak znamenalo, že lokomotiva, stojící v depu (se zapnutou částí mobilního IS) by automaticky začala prostřednictvím Wi-Fi jakožto širopásmového kanálu stahovat velké objemy dat, jako např. sešitové JŘ, předpisy a další objemnou dokumentaci. Naopak při jízdě na trati by docházelo ke komunikaci prostřednictvím GSM / GSM-R (podle dostupnosti), a to jen s malým, nezbytným objemem dat (např. aktualizace, rozkazy apod.).

Zárodek řešení tohoto projektu je implementován v provozu u ČD, ale ne v plně plánovaném rozsahu, a slouží pro řízenou distribuci dat na hnací drážní vozidla (tzn. lokomotivy a příslušné vozy souprav) prostřednictvím sítě GSM. Jedna z nejdůležitějších logických funkcí tohoto řešení do jisté míry nahrazuje funkcionalitu GSM-R, a sice že systém komunikuje ne na bázi telefonních čísel nebo čísel SIM karty, ale za pomoci překladače čísel vlaků (v některých případech čísel vozidel) na IP adresy či obdobné identifikátory přiřazené HW infrastruktuře železničního vozidla.

4.2.3 Telekomunikační vybavení vozidel, vlakové sítě

Pro datovou komunikaci železničního vozidla, a tudíž pro vybavení tohoto vozidla příslušným ICT řešením je důležitá specifikace z pohledu, zda se jedná o:

1. samostatné hnací drážní vozidlo (jako lokomotiva nebo motorový vůz), nebo
2. ucelenou a za běžných provozních podmínek nedělitelnou soupravu (jako jsou např. příměstské elektrické jednotky), nebo

3. hnací drážní vozidlo (lokomotiva), která táhne nebo tlačí železniční osobní vozy klasické stavby spojené do soupravy,
4. kombinaci bodů 2. a 3., kdy nedělitelnou soupravu tvoří osobní vozy a řídící vůz (tzn. vozidlo bez pohonu) a na vlacích s touto soupravou se střídá více lokomotiv.

S ohledem na výše popsané varianty lze konstatovat, že jednotlivá hnací drážní vozidla budou vždy vybavena telekomunikačním HW (tzn. komunikační jednotka / modem s využitím různých technologií). Nedělitelná vlaková souprava obsahuje rovněž hnací drážní vozidlo, tudíž je datová komunikace zajištěna. To platí i pro netrakční soupravy s řídícím vozem, kdy je tento vůz (z pohledu ICT) vybaven jako hnací drážní vozidlo. Co se týká souprav tvořenými železničními osobními vozy klasické stavby, zde mohou nastat varianty, kdy:

1. pro datovou komunikaci pro osobní vozy lze využít HW na lokomotivě, všechny vozidla ale musí mít datovou kabelovou propojku (u starších vozidel toto bývá problém) nebo lze data přenášet bezdrátově (zejména za pomoci vyzařovacích kabelů),
2. osobní vozy mají svůj vlastní komunikační modem (nejdražší, v praxi nepoužitelná varianta), popř. má tento modem jen jeden vůz ze soupravy (označovaný jako „master“) a komunikace do ostatních vozů je zajištěna jako v předchozím bodě. U této varianty je potřeba zvýšená pozornost při řízení oběhů vozidel, aby nedošlo k situaci, že v soupravě nebude žádný master vůz s komunikační jednotkou.

Dále je potřeba vyjít z předpokladu, že by na vozidlech měly být odděleny vlakové sítě určené pro řízení vozidla a jeho subsystémů (trakce, brzdy, klimatizace, dveře apod.), pro služební (informační systémy pro cestující) a komerční účely (Wi-Fi pro cestující). To by ale v extrémním případě znamenalo mít na vozidlech až triplicitní HW infrastrukturu, což není možné z pohledu ani ekonomického, ani technického (kvůli energetické bilanci vozidla) ani prostorového (tolik zařízení by se na vozidlo nevešlo). Proto dochází k řešením, kdy jsou:

1. některé sítě (služební a komerční) virtualizovány na jedné fyzické síti,
2. sdíleny některé prvky infrastruktury pro různé sítě, jako např. modemy, baterie, chlazení apod.

Vlakové sítě, podle svého využití, ale rovněž s ohledem na rozpočet na pořízení vozidla, mohou vycházet z různých standardů, které jsou stručně popsány v další podkapitole. Podle míry zabezpečení vlakových sítí, na ně napojených zařízení a po nich přenášených dat, se rozeznávají stupně integrity bezpečnosti (tzv. SIL, **S**afety **I**ntegrity **L**evel), kdy nejvyšší stupeň (SIL4) odpovídá zabezpečovacímu zařízení, naopak nejnižší stupeň (dříve označován jako SIL0) označuje systém, na který nejsou kladeny žádné bezpečností požadavky.

4.3 Sběrnicová topologie v železniční dopravě

Prostředí železničního osobního dopravce je ideálním prostředí pro nasazení sběrnicových technologií, protože zde komunikuje velké množství objektů mezi sebou. Komunikace jednotlivých prvků mezi sebou napřímo (systémem peer to peer) může celý systém učinit nepřehledný (díky množství vazeb) a nespolehlivý (díky obtížnému nastavení priorit a směrů v komunikaci). [32]

Přístup ke sběrnicovému řešení bude poněkud odlišný pro mobilní a stacionární část IS nebo ICT řešení.

4.3.1 Sběrnice na vozidle

Problematika sběrnic na vozidle úzce souvisí s vlakovými sítěmi. Řídící elektronické systémy vozidla používají sběrnice jako nativní architektonický prvek s vysokou mírou zabezpečení (příslušný stupeň SIL), v železniční dopravě jsou pak nejrozšířenější standardy:

1. RS 485: starší standard, protokoly a rychlosti přenosu dat jsou definovány výrobci vozidel,
2. CAN – obsah protokolů je opět definován výrobcem, do nedávné doby se jednalo o velmi rozšířený standard,
3. Ethernet – nejmodernější standard postavený na IP protokolech (TCP nebo UDP protokoly). Struktura dat v protokolech je definována výrobci na sběrnici napojených zařízení. Jedná se o nejrychlejší druh sběrnice (v porovnání se sběrnicí RS 485 s rychlostí okolo 100 kbit/s, má Ethernet sběrnice rychlost až 100 Mbit/s, v určitých konfiguracích až 1 Gbit/s).

Zajímavostí je, že výrobci železničních vozidel se velmi dlouhou drželi sběrnice CAN, ačkoliv sběrnice na bázi Ethernetu byly již dávno k dispozici. Dá se říci, že výrobce k implementaci Ethernet sběrnic donutil až tlak dopravců, kteří chtěli nebo byli nuceni pořizovat do železničních vozidel větší množství ICT řešení.

Na následujícím schématu je znázorněn návrh řešení nasazení průmyslového počítače pro provoz telematických aplikací pro strojvedoucího s využitím vozidlové sběrnice, konkrétně pro lokomotivu řady 380 ČD.

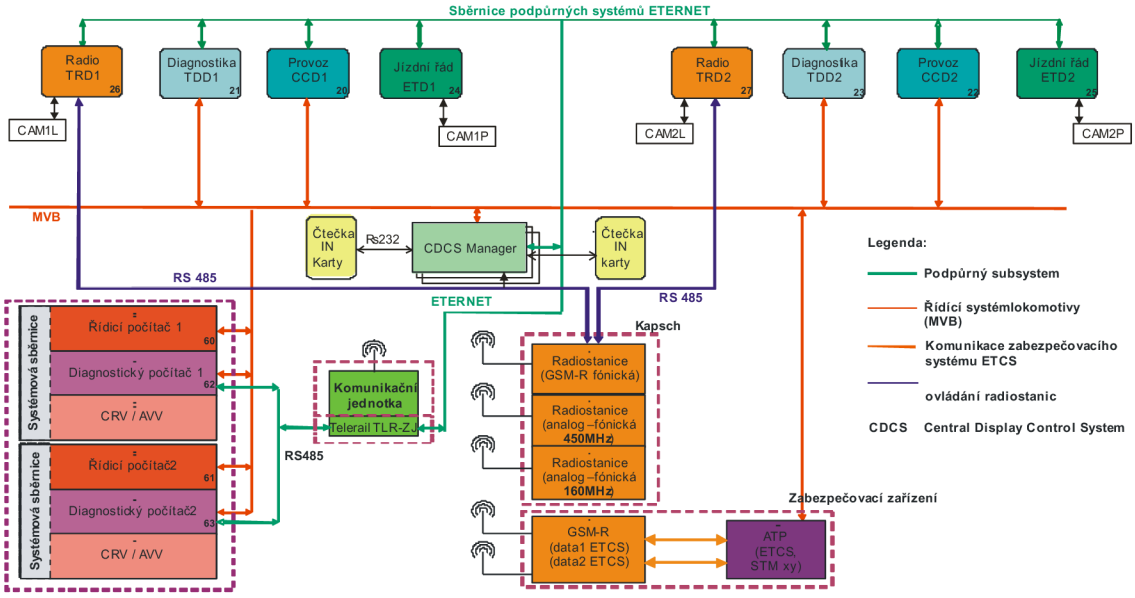


Schéma 4.3 Návrh ICT řešení s využitím sběrnice pro lokomotivu řady 380 ČD
Zdroj: [33]

4.3.2 Sběrnice na stacionární části IS

Sběrnice u stacionárních IS je pokročilá integrační komponenta, založená zpravidla na SW řešení (na rozdíl od vozidel, kde se jedná o HW sběrnice). IS využívající sběrnicovou technologii jsou postaveny na tzv. SOA (**S**ervice **O**riented **A**rchitecture) architektuře, kde mezi sebou prostřednictvím integrační sběrnice komunikují jednotlivé IS propojené takto do většího logického celku.

Řídící úroveň integrační sběrnice obsahuje katalog jednotlivých služeb, komunikace mezi systémy je pak řešena na bázi stanovených priorit. Řešení některých velkých IT vendorů (např. SAP) obsahuje vlastní integrační sběrnice, díky kterým řízeně komunikují jednotlivé moduly IS jak mezi sebou, tak mimo vlastní systém.

Ukázka SOA architektury z prostředí železničního osobního dopravce, konkrétně návrh ICT řešení pro měření trakční elektrické energie, je zobrazena na následujícím schématu:

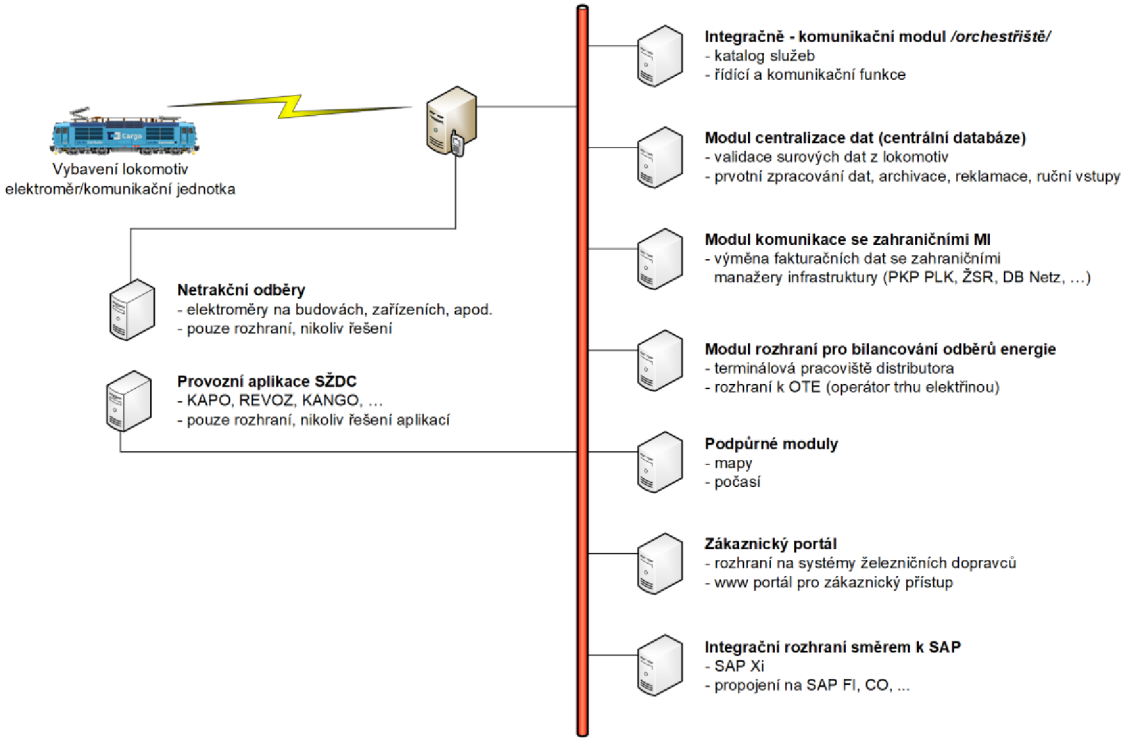


Schéma 4.4 Návrh řešení měření trakční elektrické energie s využitím SOA architektury
Zdroj: vlastní zpracování podle OLTIS Group

Na dalším schématu je návrh komplexního systému železničního osobního dopravce, který využívá sběrnicovou architekturu v mobilní i stacionární části systému. Ačkoliv tento návrh v sobě obsahuje existující IS, nebyl nikdy implementován do provozu.

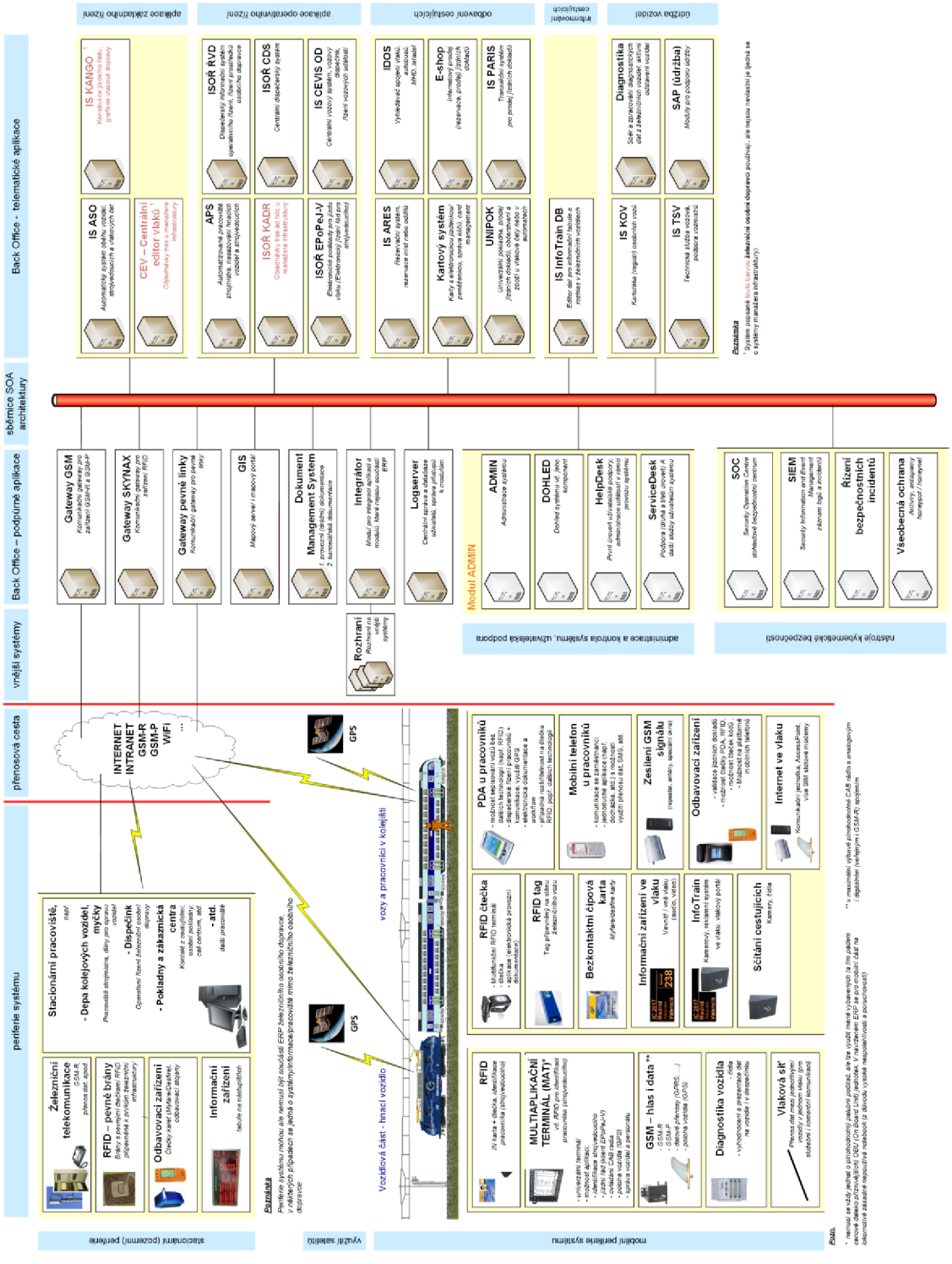


Schéma 4.5 Návrh komplexního systému železničního osobního dopravce s využitím sběrnicové architekturu v mobilní i stacionární části systému

Zdroj: vlastní zpracování podle RPP International

4.3.3 Dohledové a distribuční systémy

Samostatnou kategorií železničních IS jsou řešení pro management mobilní části IS. V podstatě se dá říci, že se jedná o drážní **M**obile **D**evice **M**anagemet (MDM), který na rozdíl od běžných komerčních produktů má specifické funkce pro železniční dopravu (zejména pak v komunikační části jako u ŽBPS). Tento IS slouží zejména pro:

1. dohled nad mobilními komponentami IS (tzn. poloha těchto komponent / vozidla, jejich stav – aktivní / mimo provoz, verze firmwaru a aplikací apod.),
2. zadávaní vstupních dat pro zavedení mobilních komponent a IS do železniční společnosti – na mobilní IS se dá v tomto ohledu dívat jako na:
    a. majetek (s potřebou tento majetek evidovat),
    b. položku technického pasportu, ke které je potřeba mít:
        i. technickou a provozní dokumentaci a
        ii. zasmluvněné nebo uskladněné náhradní díly,
    c. podklad (věcný důvod) pro vyúčtování telekomunikačních služeb,
    d. prvek entrerprise architektury, zejména s ohledem na relační model (datová komunikace související s daným zařízením, zamezení redundantní komunikace na vozidle apod.),
3. vzdálené nahrávání firmwaru (s ohledem na to, aby firmware nebyl aktualizován během jízdy vlaku či jiné nevhodné situaci),
4. vzdálené nahrávání aplikací (se stejnými podmínkami jako u firmwaru)
5. vzdálenou správu dat na železničním vozidle (jak nahrávání, např. data nového JŘ, tak stahování, např. data ze sčítání cestujících nebo kamerového systému)
6. zobrazení a správu alertů na železničním vozidle (např. hlášení výpadku mobilní části IS, větší odběr elektrické energie než přípustná hodnota, pohyb mimo vymezený územní perimetr apod.),
7. integraci (do jisté míry jako APN) na další stacionární IS železničního dopravce.

5 Návrh řešení ICT bezpečnosti a jejího vyhodnocení

V následující části diplomové práce bude pozornost věnována návrhu ICT bezpečnosti s ohledem na v předchozích částech zpracovanou:

1. segmentaci systémů v železniční osobní dopravě a
2. stručnou analýzu rizik systémů železničního osobního dopravce.

Vlastní návrhy budou zahrnovat jak technické řešení, tak organizační či další opatření.

5.1 Všeobecné bezpečnostní návrhy ICT bezpečnosti

Dále budou následovat jednotlivé bezpečnostní návrhy, které se týkají všech částí IS a ICT řešení v prostředí železničního osobního dopravce (tzn. stacionární i mobilní části systému).

5.1.1 Základní ochrana ICT

Mezi základní kameny ochrany ICT patří:

1. ochrana před škodlivým kódem, tzn. nasazení antivirových a anti malwarových řešení. Nasazení by mělo probíhat na všech prvcích ICT, nejen na klasických pracovních stanicích, ale i na serverech (vč. operačních systémů) či mobilních zařízeních. Zvláště mobilní prvky bývají v tomto ohledu opomíjeny, zejména z důvodu, že pro ně vhodné řešení neexistuje (např. pro průmyslové počítače na železničních vozidlech se speciálně upraveným OS založeným na OS LINUX) nebo existuje mylná představa, že díky relativně uzavřenému IT ekosystému je předmětný druh ochrany nepotřebný (např. u zařízení Apple). Praktickou zásadou je instalovat antivirus / antimalware prakticky všude a pravidelně aktualizovat jeho DB. Nevýhodou je, že ve špatně nakonfigurované síti či u komplikovanějšího IS může ochrana typu antiviru mít negativní vliv na výkon IS (zejména s ohledem na rychlost).
2. Pravidelná aktualizace OS a dalšího obslužného SW, zejména s ohledem na bezpečnostní záplaty. Do tohoto opatření se počítá i přechody na novější verze OS, zvláště s ohledem na to, že starší verze přestávají být časem podporovány ze strany vendorů (a tudíž nejsou bezpečnostní aktualizace vydávány).

3. Pravidelné testování z pohledu bezpečnosti ICT a jeho výkonů, tzn. že toto opatření zahrnuje penetrační a zátěžové testy. Na základě výsledů testů by mělo dojít k aktualizaci dalších bezpečnostních opatření. Jako další vhodné opatření se jeví:
    a. zahrnout penetrační a zátěžové testy jako běžnou součást pravidelného kybernetického auditu,
    b. implementovat nástroj pro automatické testování podpůrných aktiv.
4. Kromě ochrany před škodlivým kódem implementovat síťové a aplikační pasti tzv. Honeypot (v případě propojení do sítě Honeynet). Honeypot má za úkol odlákat případného útočníka na jiné (virtuální) místo, na kterém je nasimulované pracoviště (počítač, server apod.). Honeypot pak shromáždí informace o útoku, které se následně použijí pro lepší ochranu IS.

5.1.2 Ochrana dat a elektronická práce s dokumenty

1. Důvěryhodné úložiště je asi základním řešením pro práci s daty, ať už se jedná o ukládání, prezentaci, správu či archivaci. Úložiště může být implementováno jako samostatné řešení nebo součást většího celku (např. Document Management systému nebo jako specializované úložiště pro ekonomické IS). Řešení důvěryhodného úložiště odpovídá zásadám nařízení eIDAS (**e**lectronic **Id**entification **A**uthentication and trust **S**ervice),
2. Na důvěryhodné úložiště ve smyslu související evropské legislativy, navazuje problematika elektronického podpisu, razítka a pečeti. Jejich využití v železniční osobní dopravě nemusí být pouze u administrativních procesů (podpisy smluv či schvalování dokumentů), ale mohou pomoci i v železničním provozu (např. podpis rozkazů či vlakové dokumentace),
3. **D**ata **L**oss **P**rotection (DLP) je speciální SW nástroj, který detekuje a přerušuje neoprávněný přenos či kopírování dat, zejména těch citlivých. Nástroj v sobě obsahuje funkcionality od zamezení jakéhokoliv kopírování dat až po zablokování systémových funkcí jako printscreen.
4. Nasazení kryptografických nástrojů, správa privátních a veřejných klíčů. Pro použití některých šifrovacích nástrojů může být vyžadována certifikace, kterou provádí NÚKIB.

5.1.3 Identifikace uživatelů a řízení práv a přístupů

Identifikace uživatelů a řízení práv a přístupů jsou dvě velmi provázané disciplíny, které se neopírají jen o IT nástroje, ale mají velmi silnou oporu v bezpečnostních politikách a organizačních opatření. Procesy v této oblasti musí být velmi propracované, např. po ukončení pracovního poměru se zaměstnancem se spustí řada opatření a postupů, které vyústí k požadovanému datu k odstranění práv přístupu k příslušným IS a smazání uživatelského účtu. Bezpečnostní politiky rovněž definují zásadní parametry jako délka, složení a platnost hesla, druh identifikace apod. K základním řešením v této oblasti patří:

1. Identity Management, nástroj, který zabezpečuje správu a ověřování identit. Je tak konáno za pomoci vytvoření uživatelských účtů (tzn. zavedení uživatele do systému), kdy každý účet je zároveň reprezentant určité role. Identity management může být realizován i prostřednictvím externí důvěryhodné služby, v praxi se nabízí např. Bank ID [34], kde správa identity v rámci banky (kde proběhne před založením účtu fyzické ověření uživatele) je využita i pro jiné, s bankou nesouvisející systémy. Součástí Identity managementu bývají i sofistikovanější postupy při identifikaci, jako např. více faktorové ověřování (nejen za pomoci jména a hesla, ale ještě např. přístupového kódu zaslaného odlišným komunikačním kanálem, nebo využití tokenu s bezpečnostním klíčem či certifikátem).
2. Access Management, neboli nástroj pro řízení přístupových oprávnění. Ke zřízené identitě, popsané v předchozím bodě, se přiřadí práva přístupů do jednotlivých IS s detailem jednotlivých oprávnění (např. jen prohlížení, nebo čtení i zápis). Důležitou skupinou jsou tzv. privilegované účty – jedná se o účty klíčových uživatelů systému, zejména administrátorů. Přes tyto účty jsou vedeny nejnebezpečnější kybernetické útoky (útočníci se pak dostanou prakticky všude).
3. Password Management je soubor opatření a nástrojů pro práci s hesly. Jak bylo již bylo popsáno, problematika hesel se opírá o bezpečnostní politiku, která definuje parametry a platnosti hesel. Největší problémy nevznikají ve vlastních nástrojích pro hesla, ty jsou stavěny velmi robustně a nekompromisně, ale spíš u vlastních uživatelů. Bezpečnostní incidenty v této oblasti bývají spojeny s poznačením hesla na viditelné místo nebo vyzrazení hesla kolegům kvůli rychlejšímu vyřešení pracovního problému.

5.1.4 Nástroje pro ochranu provozu ICT

Některé nástroje řešící problematiku ochrany provozu ICT definuje přímo kybernetický zákon, popř. jeho vyhlášky. Jedná se zejména o

1. nástroj typu SIEM, který zabezpečuje sběr informací o provozních a bezpečnostních činnostech a jejich ochranu před neoprávněným přístupem nebo změnou [15, §22],
2. nástroj pro řízení bezpečnostních incidentů mající za cíl správu kybernetických událostí a incidentů, nejedná se jen o evidenci, ale i analýzu útoků a souvislostí, elektronické správy aktiv apod. [15, §14, §23, §24]

Výše uvedené nástroje jsou součástí dohledového (de facto dispečerského) ICT pracoviště, které se označuje jako SOC (**S**ecurity **O**perations **C**enter). Některé konkrétní pracoviště SOC jsou zároveň partnery vládnímu nebo národnímu CERT s certifikací CSIRT (**C**omputer **S**ecurity **I**ncident **R**esponse **T**eam).

5.1.5 Ochrana před Vendor-Lock-In

Ochrana před závislostí na jednom dodavateli spočívá v technicko – obchodních opatřeních a důsledné přípravě IS. V rámci této problematiky je možné přistupovat preventivně (tzn. vybírat více dodavatelů nebo se toto pokusit ošetřit v dodavatelských smlouvách) nebo reaktivně, např. za pomoci různých auditů nebo reverzního inženýringu. V každém případě se jedná poměrně drahá řešení, proto základní – byť možná teoretická poučka – je se do situace Vendor Lock-In vůbec nedostat.

5.1.6 Opatření v rámci architektury

Na případné kybernetické hrozby je možné se bránit preventivně v rámci přípravy IS nebo naopak reaktivně odstraněním nežádoucích stavů. Velkou roli v obou případech hraje architektura (tzn. technické řešení) příslušných IS a ICT řešení. V prostředí železničního osobního dopravce se jedná především o:

1. využití sběrnicové topologie u složitějších soustav IS, tzn. zavedením SOA architektury,
2. maximální sjednocení vývojových a provozních platforem IS. Sjednocení vede k menší pracnosti a chybovosti, architektura IS se stává přehlednější a opatření kybernetické ochrany se pak snáze implementují,

3. náhrada starších aplikací, jejich přepracování na nové, podporované technologie. Existují případy historických aplikací, které stále poskytují důležitá data (tedy aktiva) a přitom již nelze oficiální cestou pořídit HW pro jejich provoz (a tak se řeší např. nákupem bazarové techniky). Důvodem náhrady nemusí být jen zastaralost, ale i roztříštěnost funkcionalit (z historických důvodů) do více aplikací – výsledek není jen uživatelsky nepříjemný, ale i kyberneticky nebezpečný.

5.1.7 Školení, tréningy, simulace, bojové hry

Jak již bylo řečeno v předchozích kapitolách, velmi důležitá je osvěta ohledně kybernetické bezpečnosti, a to jak u obslužného technického personálu, který zabezpečuje nasazení, provoz a servis IS, tak u uživatelů IS, zejména těch klíčových (superuživatelů).

Na probíhající kybernetický útok se nedá teoreticky připravit. Školení (zvláště pak ve zrychleném režimu jako např. prostřednictvím e-learningu) je pro tak kritickou situaci velmi málo. Proto je nutné se na eventuální incidenty prakticky připravovat, a to za pomoci simulace nebo bojových her. Tento postup nepředstavuje nic nestandardního, na krizové situace prakticky cvičí v simulovaných situacích i např. hasiči či policie.

5.2 Návrhy řešení ICT v rámci stacionární části IS

Nad rámec opatření uvedených v předchozích podkapitolách je pro stacionární část IS vhodné zavést následující opatření:

5.2.1 Blockchain

Pro některé procesy v osobní dopravě by mohl být blockchain zajímavé řešení z pohledu technického řešení i kybernetické bezpečnosti. Princip blockchainu spočívá na distribuované decentralizované databázi, kterou tvoří jednotlivé uzly. Zápisy do uzlů jsou transparentní a porovnávají se mezi sebou. Proto jsou důvěryhodné a nepodléhají centrálnímu systému. Takto zapisovaná data do databáze „nepustí“ žádný falešný záznam.

Blockchain by proto mohl sloužit jako technologie např. pro Státní jednotný tarif (dále jen „SJT“), což je prodej jízdenek s garancí státu zajišťující stejné podmínky přepravní smlouvy u všech železničních osobních dopravců zapojených do SJT nebo agenturní prodej jízdenek železničního osobního dopravce.

5.2.2 Práce se sítěmi

Na sítě a jejich bezpečnost pamatuje i kybernetický zákon prostřednictví vyhlášky o kybernetické bezpečnosti [15, §15, §28]. Jako jedno z bezpečnostních opatření souvisejících se sítěmi je jejich segmentace. Řešení spočívá v izolaci potenciálního útočníka a zamezení šíření škodlivého kódu mezi segmenty sítě. Takto se mohou oddělit prvky sítě, které jsou součástí systému nebo infrastruktury určené kybernetickým zákonem od ostatních sítí nebo segmentů.

Pro zavedení segmentace sítí je nutné mít i aktuální pasport této infrastruktury, což může být problém u lokalit se starší síťovou výbavou.

5.3 Návrhy řešení ICT v rámci mobilní části IS

Nad rámec opatření uvedených v předchozích podkapitolách je pro mobilní část IS vhodné zavést následující opatření:

5.3.1 Standardy pro stejné typy železničních vozidel

Ačkoliv je architektura ICT na železničním vozidle velmi přísně svázána s technickými normami, provedení bývá velmi různorodé. Jednak každý výrobce železničních vozidel má k problematice ICT jiný přístup (od low cost po high end řešení) a pak dodávky bývají rozloženy do dlouhého časového období (až 10 let), kdy už leckdy není k dispozici původně navrhované ICT řešení.

V prostředí železničního osobního dopravce chybí standard (norma), která by stanovovala:

1. maximální morální životnost vozidlových ICT řešení (např. na 5 let), kdy po uplynutí této lhůty by nastala povinnost ICT vyměnit nebo modernizovat. Pochopitelně by se tato výměna promítla do ceny železničních vozidel nebo dopravní služby, ale při pravidelném cyklu výměn by ekonomický dopad mohl být minimální,
2. typovou ICT architekturu pro logické skupiny vozidel (jako závislá/nezávislá trakce, nové/rekonstruovaná vozidla, lokomotivy/ucelené jednotky apod.),
3. úrovně vybavení výše zmíněných logických skupin železničních vozidel, např.:
    a. povinná úroveň: zabezpečovací zařízení, řídící vozidlový počítač, komunikační jednotka, vlaková síť,

b. rozšířená povinná úroveň: displeje (napevno zabudované počítače) pro strojvedoucí, vozidlová diagnostika,
c. úroveň pro základní komfort cestujících: informační tabule a rozhlas,
d. rozšířená úroveň komfortu pro cestující: palubní Wi-Fi, entertainment portál (filmy, hudba, hry během jízdy vlaku),
e. úroveň vyžadovaná objednatelem dopravní služby: systém pro automatické sčítání cestujících, odbavovací systémy.

Každá z takto vydefinovaných úrovní by měla svá technická specifika (vč. bezpečnostních), např. rozměry, napájení, rozhraní, komunikační a bezpečnostní protokoly apod.

Takto připravené standardy by zlevnily výrazným způsobem ICT řešení na železničních vozidlech (narostl by jejich počet a nejednalo by se o proprietární řešení), zvýšila by se úroveň kybernetické bezpečnosti (jednotlivé nástroje by se daly implementovat na celou flotilu vozidel) a zároveň by mohly sloužit jako technická část zadávací dokumentace, a to jak pro nákup samotných železničních vozidel, tak pro zakázky týkající se dopravní obslužnosti.

5.3.2 Rozšíření Mobile Device Management

Ne všechna ICT řešení mobilní části systému jsou zapojena do MDM. Zejména není dořešena problematika distribuce dat (jakožto aktiv), stále se vyskytuje množství železničních vozidel, do jejichž ICT infrastruktury se data nahrávají ještě manuálně.

5.3.3 Sjednocení standardu mobilních komunikací

Železniční vozidla používají pro komunikaci se stacionární částí IS zejména GSM technologií. Bohužel díky velmi postupnému vybavování železničních vozidel je rozsah komunikačních (GSM) jednotek od 2G až po 4G. Navíc v současné době se v rámci běžných telekomunikačních služeb implementuje 5G, proto se dá očekávat i rozšíření této technologie na železniční vozidla.

Z pohledu správné funkce mobilní části IS a zejména pak s ohledem na bezpečnost přenosu dat je nezbytné zmenšit rozsah GSM modemů na železničních vozidlech na max. 2 (po sobě jdoucí a vždy nejnovější) generace.

5.4 Vyhodnocení bezpečnosti ICT v prostředí železničního osobního dopravce

V zásadě lze konstatovat, že bezpečnost ICT v prostředí železničního osobního dopravce je na velmi vysoké úrovni. Je to dáno především:

1. podmínkami železničního prostředí, ze kterého plyne především odpovědnost za životy a zdraví cestujících za podmínek kvality cestování srovnatelné s jinými druhy dopravy,
2. prostředím, které je zvyklé na standardizaci,
3. prostředím, kde ICT řešení mají přirozený způsob využití.

Na druhou stranu i přes vysokou úroveň bezpečnosti železniční sektor nestíhá příliš rychlé tempo informačních technologií. Investice v prostředí železničního dopravce probíhají ve vyšších jednotkách let, návratnost (hlavně u železničních vozidel) je až na 30 (třicet) let. Dalo by se říci, že srdce světa železničních dopravců a světa ICT bijí v odlišném rytmu.

Po určení železničních osobních dopravců jako dodavatelů základní služby (ve smyslu kybernetického zákona) se dá do budoucna očekávat zpřísnění v této oblasti, které přijde po úspěšném kybernetickém útoku. Je možné, že se některé prvky zabezpečovacího zařízení na straně železničních vozidel (zejména pak ETCS) stanou řešením spadajícím pod kybernetický zákon a mohou tak posunout železniční osobní dopravce až do sféry kritické informační infrastruktury.

Závěr

Tato diplomová práce řeší problematiku bezpečnostních aspektů informačních technologií v železniční osobní dopravě. Železniční sektor je obecně zvyklý na vysokou míru bezpečnosti. Vždyť železniční dopravci ručí za životy cestujících, zaměstnanců a za náklad, manažer železniční infrastruktury ručí zase za bezpečnost železniční dopravy a dopravců. Přesto bezpečnost informačních technologií představuje v železničním sektoru jakýsi milník, protože zavádí zcela nové pohledy a řešení.

Informační systémy a technologie jsou na železnici od jejich vzniku, vždyť železniční prostředí je ideálním místem pro jejich využití. Standardy a řešení klasických informačních systémů má na železnici dlouholetou tradici. S okamžikem, kdy se informační technologie začaly dostávat do železničních vozidel, se začala více objevovat specifika železničního prostředí, umocněná relativně malým množstvím vozidel (v porovnání se silniční dopravou). Dalším výrazným milníkem byl začátek platnosti zákona o kybernetické bezpečnosti. Ten nutí železniční osobní dopravce svoji informatickou bezpečnost řešit už ne na dobrovolné bázi, ale na základě zákonné povinnosti. Do budoucna se dá navíc očekávat zpřísnění podmínek, zejména pak směrem k železničním vozidlům.

Analýza v této diplomové proběhla jak z pohledu železničního osobního dopravce, jeho procesů a technických prostředků, tak z pohledu zákona o kybernetické bezpečnosti, na něj navazujících vyhlášek, souvisejících metodik a praxí. Analýza ukázala, že železniční prostředí obsahuje až příliš velké množství nesourodých informačních systémů, a ne vždy se zde používá moderní infrastruktura. Proto musí železniční dopravci s příchodem kybernetických hrozeb tento stav napravit. Rovněž se budou muset víc zaměřit na informační systémy, které se čím dál tím víc stávají nedílnou součástí železničních vozidel. Tuto oblast pokrývají zatím pouze technické normy, které pro mobilní část informačních technologií představují jen jakýsi rámec. Zcela ale chybí standardizace typového řešení, zaměřeného na logické skupiny železničních vozidel. Další navrhovaná oblast zlepšení je praktický výcvik a trénink personálu obsluhující předmětné informační systémy, neboť se ukazuje, že teoretická průprava nestačí.

Přes uvedené výhrady lze ale konstatovat, že bezpečnost informačních a komunikačních technologií v železniční osobní dopravě je na velmi vysoké úrovni.

Seznam zdrojů

[1] BURDA, Karel. *Bezpečnost informačních systémů*. Brno: Vysoké učení technické v Brně, Fakulta elektrotechniky a komunikačních technologií, 2005.

[2] EVROPSKÁ UNIE. *Návrh Nařízení Evropského parlamentu a Rady, kterým se stanoví harmonizovaná pravidla pro umělou inteligenci (Akt o umělé inteligenci) a mění se určité legislativní akty Unie*. In: Brusel: Evropský parlament a Rada, 2021. Dostupné také z: https://eur-lex.europa.eu/legal-content/CS/ALL/?uri=CELEX:52021PC0206

[3] ČESKÁ REPUBLIKA. Zákon č. 266/1994 Sb., o dráhách. In: *Sbírka zákonů*. Praha: Parlament ČR, 1994, částka 79/1994, číslo 266. Dostupné také z: https://www.zakonyprolidi.cz/cs/1994-266

[4] ČESKÁ REPUBLIKA. Zákon č. 181/2014 Sb., o kybernetické bezpečnosti. In: *Sbírka zákonů*. Praha: Parlament ČR, 2014, částka 75/2014, číslo 181. Dostupné také z: https://www.zakonyprolidi.cz/cs/2014-181

[5] KOLOUCH, Jan a kol. *CYBERSECURITY*. Praha: CZ.NIC, 2019. ISBN 978-80-88168-34-8.

[6] SNEDAKER, Susan a Chris RIMA. *Business Continuity and Disaster Recovery Planning for IT Professionals.* Second edition. Boston: Syngress, 2014. ISBN 978-0-12-410526-3.

[7] *10 tipů na zlepšení vaší kybernetické bezpečnosti* [online]. 2. 5. 2019. [cit. 2. 8. 2022]. Dostupné z: https://www.kybez.cz/10-tipu-na-zlepseni-vasi-kyberneticke-bezpecnosti/

[8] BURDA, Karel. *Kryptografie okolo nás*. Praha: CZ.NIC, 2019. ISBN 978-80-88168-49-2.

[9] NÚKIB, NAKIT a Ministerstvo vnitra ČR. *Minimální bezpečnostní standard, podpůrný materiál pro subjekty, které nespadají pod zákon o kybernetické bezpečnosti* [online]. 2020. [cit. 2022-08-15]. Dostupné z: https://nukib.cz/download/publikace/podpurne_materialy/2020-07-17_Minimalni-bezpecnostni-standard_v1.0.pdf

[10] EVROPSKÁ UNIE. Směrnice Evropského parlamentu a Rady (EU) 2016/1148 ze dne 6. července 2016 o opatřeních k zajištění vysoké společné úrovně bezpečnosti sítí a informačních systémů v Unii. In: *Úřední věstník Evropské unie*. Brusel:

Evropský parlament a Rada, 2016, L 194/1, číslo 1148. Dostupné také z: https://eur-lex.europa.eu/legal-content/CS/TXT/PDF/?uri=CELEX:32016L1148&from=CS

[11] EVROPSKÁ UNIE. Nařízení Evropského parlamentu a Rady (EU) 2019/881 ze dne 17. dubna 2019 o agentuře ENISA („Agentuře Evropské unie pro kybernetickou bezpečnost“), o certifikaci kybernetické bezpečnosti informačních a komunikačních technologií a o zrušení nařízení (EU) č. 526/2013 („akt o kybernetické bezpečnosti“). In: *Úřední věstník Evropské unie*. Brusel: Evropský parlament a Rada, 2019, L 151/15, číslo 881. Dostupné také z: https://eur-lex.europa.eu/legal-content/CS/TXT/PDF/?uri=CELEX:32019R0881&from=CS

[12] NÁRODNÍ ÚŘAD PRO KYBERNETICKOU A INFORMAČNÍ BEZPEČNOST. *Systém a rozsah ISMS* [online]. Brno, 31. 5. 2022. [cit. 15. 8. 2022]. Dostupné z: https://www.nukib.cz/download/publikace/podpurne_materialy/ZKB_blokove_schema.pdf

[13] ČESKÁ REPUBLIKA. Vyhláška č. 317/2014 Sb., o významných informačních systémech a jejich určujících kritériích. In: *Sbírka zákonů*. Praha: Národní bezpečnostní úřad a Ministerstvo vnitra, 2014, částka 127/2014, číslo 181. Dostupné také z: https://www.zakonyprolidi.cz/cs/2014-317

[14] ČESKÁ REPUBLIKA. Vyhláška č. 437/2017 Sb., o kritériích pro určení provozovatele základní služby. In: *Sbírka zákonů*. Praha: Národní úřad pro kybernetickou a informační bezpečnost, 2017, částka 157/2017, číslo 437. Dostupné také z: https://www.zakonyprolidi.cz/cs/2017-437

[15] ČESKÁ REPUBLIKA. Vyhláška č. 82/2018 Sb., o kybernetické bezpečnosti. In: *Sbírka zákonů*. Praha: Národní úřad pro kybernetickou a informační bezpečnost, 2018, částka 43/2018, číslo 82. Dostupné také z: https://www.zakonyprolidi.cz/cs/2018-82

[16] SMEJKAL, Vladimír, SOKOL, Tomáš a Jindřich KODL. *Bezpečnost informačních systémů podle zákona o kybernetické bezpečnosti.* Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2019. ISBN 978-80-7380-765-8.

[17] ČESKÁ REPUBLIKA. Zákon č. 240/2000 Sb., o krizovém řízení a o změně některých zákonů (krizový zákon). In: *Sbírka zákonů*. Praha: Parlament ČR, 2000, částka 73/2000, číslo 240. Dostupné také z: https://www.zakonyprolidi.cz/cs/2000-240

[18] ČESKÁ REPUBLIKA. Nařízení vlády č. 432/2010 Sb., o kritériích pro určení prvku kritické infrastruktury. In: *Sbírka zákonů*. Praha: Vláda ČR, 2010, částka 149/2010, číslo 432. Dostupné také z: https://www.zakonyprolidi.cz/cs/2010-432

[19] ČESKÁ REPUBLIKA. Zákon č. 365/2000 Sb., o informačních systémech veřejné správy. In: *Sbírka zákonů*. Praha: Parlament ČR, 2000, částka 99/2000, číslo 365. Dostupné také z: https://www.zakonyprolidi.cz/cs/2000-365

[20] ČESKÁ REPUBLIKA. Vyhláška č. 529/2006 Sb., o dlouhodobém řízení informačních systémů veřejné správy. In: *Sbírka zákonů*. Praha: Ministerstvo informatiky, 2006, částka 172/2006, číslo 529. Dostupné také z: https://www.zakonyprolidi.cz/cs/2006-529

[21] ČESKÁ REPUBLIKA. Zákon č. 412/2005 Sb., o ochraně utajovaných informací a bezpečnostní způsobilosti. In: *Sbírka zákonů*. Praha: Parlament ČR, 2005, částka 143/2005, číslo 412. Dostupné také z: https://www.zakonyprolidi.cz/cs/2005-412

[22] ČESKÁ REPUBLIKA. Zákon č. 127/2005 Sb., o elektronických komunikacích. In: *Sbírka zákonů*. Praha: Parlament ČR, 2005, částka 43/2005, číslo 127. Dostupné také z: https://www.zakonyprolidi.cz/cs/2005-127

[23] ČESKÁ REPUBLIKA. Zákon č. 297/2016 Sb., o službách vytvářejících důvěru pro elektronické transakce. In: *Sbírka zákonů*. Praha: Parlament ČR, 2016, částka 43/2005, číslo 297. Dostupné také z: https://www.zakonyprolidi.cz/cs/2005-127

[24] EVROPSKÁ UNIE. Nařízení Evropského parlamentu a Rady (EU) č. 910/2014 ze dne 23. července 2014 o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu a o zrušení směrnice 1999/93/ES. In: *Úřední věstník Evropské unie*. Brusel: Evropský parlament a Rada, 2014, L 257/110, číslo 910. Dostupné také z: https://eur-lex.europa.eu/legal-content/CS/TXT/PDF/?uri=CELEX:32014R0910&from=cs

[25] EVROPSKÁ UNIE. Nařízení Komise (EU) 2016/919 ze dne 27. května 2016 o technické specifikaci pro interoperabilitu týkající se subsystémů „Řízení a zabezpečení“ železničního systému v Evropské unii. In: *Úřední věstník Evropské unie*. Brusel: Komise EU, 2016, L 158/1, číslo 919. Dostupné také z: https://eur-lex.europa.eu/legal-content/CS/TXT/PDF/?uri=CELEX:32016R0919&from=CS

[26] EVROPSKÁ UNIE. Směrnice Evropského parlamentu a Rady (EU) 2016/797 ze dne 11. května 2016 o interoperabilitě železničního systému v Evropské unii. In: *Úřední věstník Evropské unie*. Brusel: Evropský parlament a Rada, 2016, L 138/44,

číslo 797. Dostupné také z: https://eur-lex.europa.eu/legal-content/CS/TXT/PDF/?uri=CELEX:32016L0797&from=CS

[27] MINISTERSTVO ZDRAVOTNICTVÍ ČR. Metodický pokyn poskytovatelům zdravotních služeb ke kybernetické bezpečnosti [online]. 2017. [cit. 2. 8. 2022]. Dostupné z: https://ncez.mzcr.cz/cs/dokumenty/metodicky-pokyn-poskytovatelum-zdravotnich-sluzeb-k-problematice-kyberneticke-bezpecnosti

[28] KRESA, Dan. *Analýza kybernetické bezpečnosti #4: Hodnocení rizik* [online]. 6. 5. 2019. [cit. 15. 8. 2022]. Dostupné z: https://www.kybez.cz/analyza-kyberneticke-bezpecnosti-4-hodnoceni-rizik/

[29] ČESKÁ REPUBLIKA. Zákon č. 134/2016 Sb., o zadávání veřejných zakázek. In: *Sbírka zákonů*. Praha: Parlament ČR, 2016, částka 51/2016, číslo 134. Dostupné také z: https://www.zakonyprolidi.cz/cs/2016-134

[30] ČESKÁ REPUBLIKA. Zákon č. 77/2002 Sb., o akciové společnosti České dráhy, státní organizaci Správa železnic a o změně zákona č. 266/1994 Sb., o dráhách a změně zákona č. 77/1997 Sb., o státním podniku. In: *Sbírka zákonů*. Praha: Parlament ČR, 2002, částka 34/2002, číslo 77. Dostupné také z: https://www.zakonyprolidi.cz/cs/2002-77

[31] UIC. GSM-R [online]. 2015. [cit. 15. 8. 2022]. Dostupné z: https://uic.org/rail-system/gsm-r/#EIRENE-Specifications

[32] BÁRTA, Petr. 2013. Disertační práce. *Nové koncepty nadřazených řídících systémů kolejových vozidel městské hromadné dopravy*. Fakulta elektrotechnická Západočeské univerzity v Plzni. [online]. [cit. 30. 7. 2022]. Dostupné z: https://dspace5.zcu.cz/bitstream/11025/13689/1/barta_dis_prace.pdf

[33] UniControls. *Návrh ICT řešení s využitím sběrnice pro lokomotivu řady 380 ČD* [online]. Praha: TTC Controls, 2021. [cit. 30. 7. 2022]. Dostupné z: https://www.unicontrols.cz/index_php/cs/

[34] *BankID – vaše digitální občanka* [online]. Praha: BankID, © BankID 2022. [cit. 6. 8. 2022]. Dostupné z: https://www.bankid.cz

[35] GÁLA, Libor, POUR, Jan a Zuzana ŠEDIVÁ. *Podniková informatika: počítačové aplikace v podnikové a mezipodnikové praxi. 3., aktualizované vydání*. Praha: Grada Publishing, 2015. ISBN 978-80-247-5457-4.

[36] GAŠPARÍK, Jozef a Jiří KOLÁŘ. *Železniční doprava: technologie, řízení, grafikony a dalších 100 zajímavostí*. Praha: Grada Publishing, 2017. ISBN 978-80-271-0058-3.

[37] HELLER, Petr a Josef DOSTÁL. *Kolejová vozidla I.* 2. přepracované vydání. Plzeň: Západočeská univerzita, 2010. ISBN 978-80-7043-960-9.

[38] HELLER, Petr a Josef DOSTÁL. *Kolejová vozidla II.* Plzeň: Západočeská univerzita, 2009. ISBN 978-80-7043-641-7

[39] ÚPLNÉ ZNĚNÍ č. 1445. *Svobodný přístup k informacím, Elektronické komunikace, Egoverment, Kybernetická bezpečnost*. Ostrava-Hrabůvka: Sagit, 2021. ISBN 978-80-7488-482-5.

Seznam grafických objektů

Seznam zkratek

APN	Access Point Name
AM	Access Management
BCP	Business Continuity Plan
BRS	Bezpečnostní rada státu
B2B	Business to Business
B2C	Business to Customer
B2G	Business to Goverment
CAN	Controller Area Network
CERT	Computer Emergency Response Team
COBIT	Control Objectives for Information and Related Technology
CRM	Customer Relationship Management
CSIRT	Computer Security Incident Response Team
ČD	České dráhy
ČD-T	ČD – Telematika
ČSN	Česká soustava norem (česká technická norma)
DB	Databáze
DLP	Data Loss Protection
DRP	Disaster Recovery Plan
eIDAS	Electronic Identification Authentication and Trust Service
EIRENE	European Integrated Radio Enhanced NEtwork
EN	European Norm
ENISA	The European Union Agency for Cybersecurity
ERTMS	European Rail Traffic Management Systém
ETCS	European Train Control System

GDPR	General Data Protection Regulation
GSM-R	Global System for Mobile Communication for Railway
HDP	Hrubý domácí produkt
HW	Hardware
ICT	Information and Communications Technology
IoT	Internet of Thinks
IS	Informační systém
ISACA	Information Systems Audit and Control Association
ISO/IEC	International Organization for Standardization / international Electrotechnical Commission
ISO/OSI	International Organization for Standardization / Open Systems Interconnection
ISMS	Information Security Management System
IT	Informační technologie
ITIL	Information Technology Infrastructure Library
JŘ	Jízdní řád
KII	Kritická informační infrastruktura
KKI	Kritická komunikační infrastruktura
MDM	Mobile Device Managemet
MI	Manažer (železniční) infrastruktury
MORANE	Mobile Radio for Railways Networks in Europe
MVB	Multifunction Vehicle Bus
MW	Middleware
NAKIT	Národní agentura pro komunikační a informační technologie
NBÚ	Národní bezpečnostní úřad
NDA	Non-Disclosure Agreement
NÚKIB	Národní úřad pro kybernetickou bezpečnost

OS	Operační systém
PDA	Personal Digital Assistant
PtP Call	Point-to-Point Call
REC	Railways Emergency Call
SIEM	Security Information and Event Mananagement
SIL	Safety Integrity Level
SLA	Service Level Agreement
SOA	Service Oriented Architecture
SOC	Security Operations Center
SPOF	Single Point of Failure
SŽ	Správa železnic
SW	Software
TAF	Telematics Applications for Freight Services
TAP	Telematics Applications for Passenger Services
TCN	Train Communication Network
TRS	Traťový rádiový systém
TSI	Technické specifikace interoperability
UTZ	Uurčené technické zařízení
VBS	Voice Broadcast System
VGCS	Voice Group Call System
WTB	Wire Train Bus
ŽBPS	Železniční bezdrátová přenosová síť

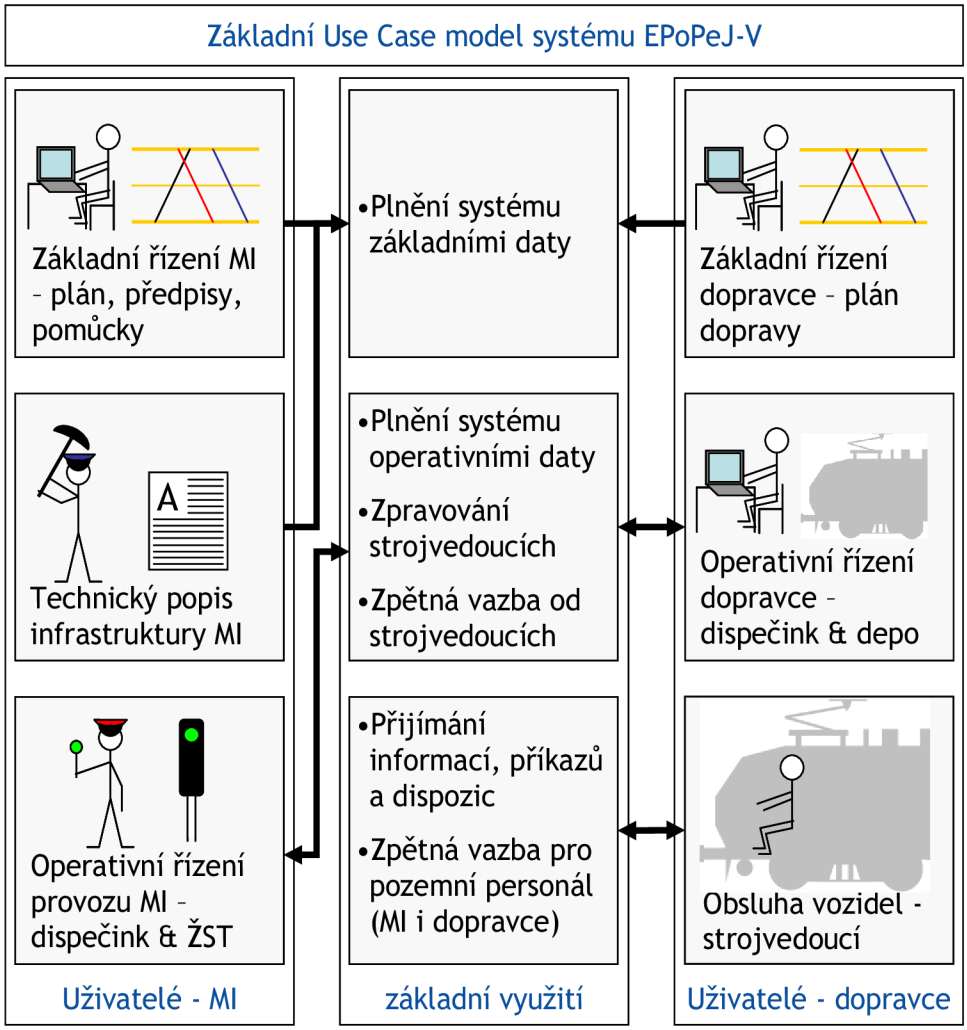
Seznam příloh

Příloha A

Ukázka procesního a návazných modelů konkrétní aplikace

Ukázka procesní modelování a na něj návazných kroků (use case model, zdroje dat, relační model, personální obsluha systému) je zde demonstrována na systému EPoPeJ-V (**el**ektronické **p**odklady **p**ro **j**ízdu **v**laku). Výstupem projektu měla být mobilní aplikace se souhrnnými podklady pro strojvedoucího (JŘ, tabulky traťových poměrů, plánky stanic, obsluhovací řády, interní předpisy, rozkazy, apod.). Projekt zpracovávalo konsorcium společností ČD-T a UniControls pro objednatele ČD. Projekt ve finále nebyl realizován, ČD se rozhodly (v mnohem pozdější době) pro proprietární jednoduché aplikace pro strojvedoucí.

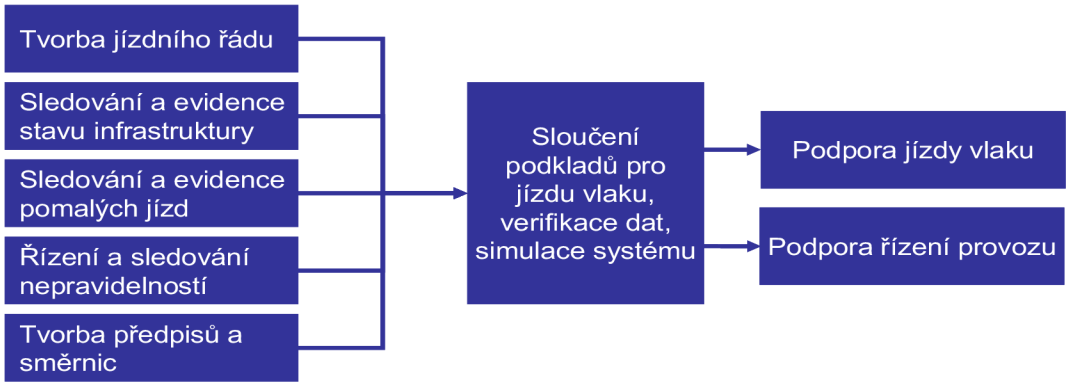
Zdroj: ČD-T (vlastní zpracování)

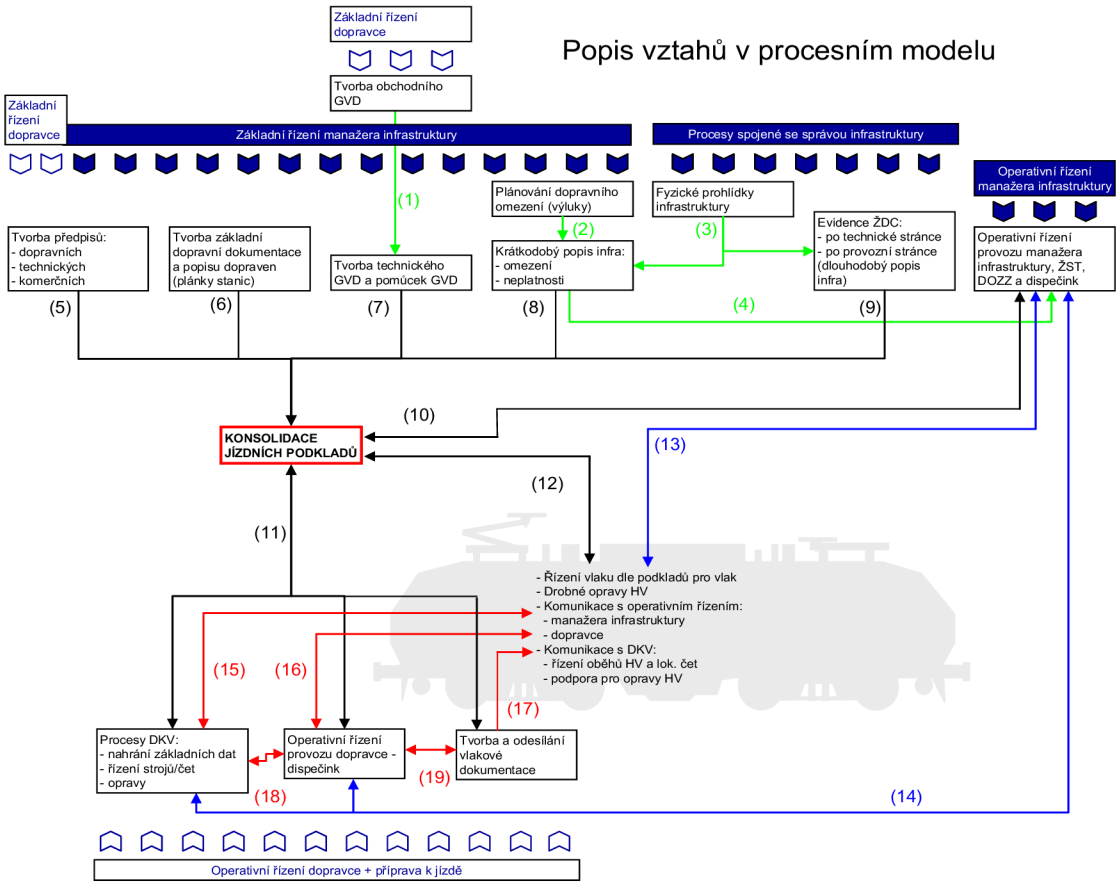


Základní procesní blokový model pro systém EPoPeJ-V

Skupiny procesů	plán základní řízení	distribuce dat operativní řízení	jízda vlaku nebo drážního vozidla
Základní procesy, Které se vztahují k systému EPoPeJ-V	• vyhotovení JŘ • plánování výluk • sledování PJ • sledování dalšího omezení v dopravě • vyhotovení ZDD, TPP a plánků ŽST • vyhotovení předpisů	• nahrání základních dat do MAT • průběžná aktualizace dat v MAT • zpravování písemnými rozkazy • ústní informace přes sdělovací zařízení	• řízení vlaku, vozidla • administrativní úkony spojené s jízdou • potvrzování dopravní příkazy • ústní informace přes sdělovací zařízení
Podklady, které vyplývají ze základních procesů	• podklady pro jízdu vlaku (databáze JŘ) • podklady pro řízení vlaků (dtto) • provozní a technický popis infrastruktury • vnitropodniková legislativa (předpisy, směrnice)	• podklady pro jízdu vlaku (databáze JŘ) • podklady pro řízení vlaků (dtto) • písemné rozkazy • elektronické knihovny	• kvitance/potvrzení rozkazů • aktuální informace o stavu trati a vozidla

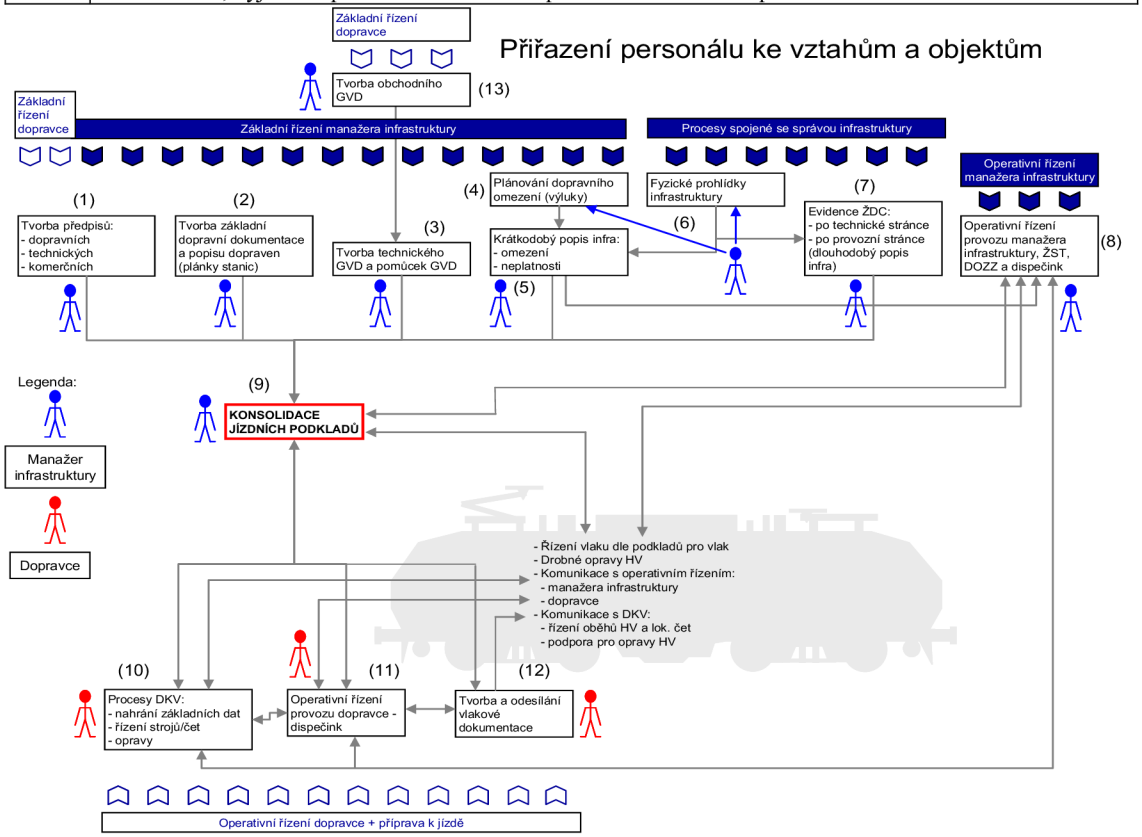
Základní procesy stacionární části EPoPeJ-V





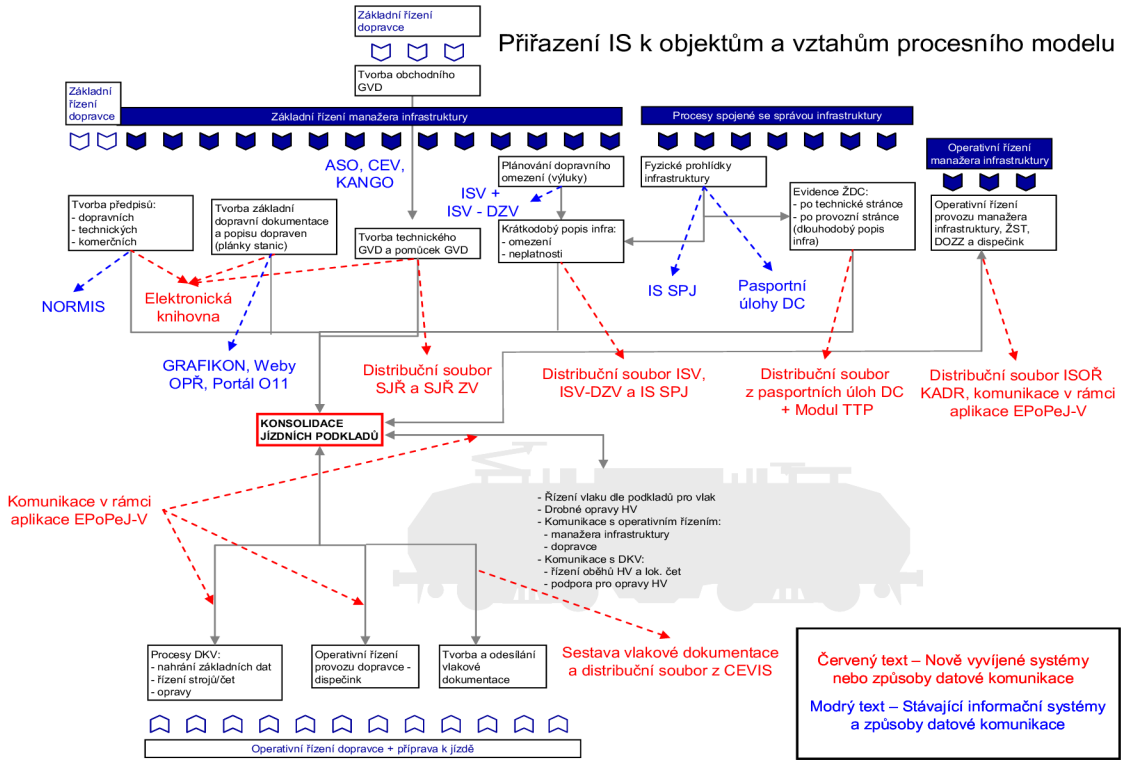
(1)	Předložení požadavku dopravce na zpracování jízdního řádu zástupci provozovatele dráhy
(2)	Zadání plánovaných výluk, obsahujících dopravní omezení (jízdy po nesprávné koleji/proti správnému směru, mimořádnosti na trakčním vedení) do systému ISV-DZV a ISV provozovatelem dráhy. Čerpání těchto informací centrálním serverem EPoPeJ-V.
(3)	Zjištění závad správcem infrastruktury při pravidelných či mimořádných prohlídkách. Jejich zapracování do krátkodobých (pomalé jízdy – systém SPJ) nebo dlouhodobých omezení (oprava TTP).
(4)	Čerpání údajů o krátkodobých omezeních infrastruktury operativním řízením MI z IS SPJ a ISV, příp. ISV-DZV
(5)	Tvorba předpisů, které jsou součástí elektronické knihovny strojvedoucího, manažerem infrastruktury.
(6)	Tvorba ZDD, která je součástí elektronické knihovny strojvedoucího, manažerem infrastruktury.
(7)	Zpracování údajů jízdního řádu (VT SENA), které jsou použity ke sloučení s údaji TTP v centrálním serveru EPoPeJ-V, manažerem infrastruktury.
(8)	Použití údajů o krátkodobých omezeních (IS SPJ a ISV, příp. ISV-DZV) ke tvorbě dokumentu, zobrazujícím jízdní řád, v centrálním serveru EPoPeJ-V
(9)	Zpracování údajů TTP v centrálním serveru EPoPeJ-V manažerem infrastruktury.
(10)	Spojení klientských stanic operativního řízení MI pro získání a příp. tisk podkladů JŘ
(11)	Přenos jízdních podkladů do DKV a operativnímu řízení dopravce za účelem nahrání na vozidlo, přenos vlakové dokumentace na vozidlo
(12)	Automatická aktualizace dat na mobilním terminálu po zadání čísla vlaku
(13)	Předávání a potvrzování písemných rozkazů, hlášení mimořádností strojvedoucím zástupci manažera infrastruktury.
(14)	Předávání podkladů mezi operativním řízením provozu MI a dopravcem + DKV, upozornění MI dopravcem na mimořádnosti v řazení vlaku
(15)	Nahrání základních dat v DKV přes WiFi nebo USB, administrativa DKV, přebírání údajů o traťovém výkonu lok. čet, dat o výkonu HV, evidence poruch.
(16)	Komunikace operativního řízení provozu dopravce s vozidlem ve vztahu nasazení na vlak a mimořádnostem vzniklým při jízdě vlaku.
(17)	Předání vlakové dokumentace, vytvořené dopravcem, na vozidlo.
(18)	Komunikace mezi operativním řízení provozu dopravce a DKV vzhledem k výkonům HV.

(19)	Odeslání vlakové dokumentace operativnímu řízení provozu dopravce s upozorněním na mimořádnosti v řazení vlaku, vyjádření požadavku na řazení operativním řízením dopravce



Legenda ke schématu Přiřazení personálu ke vztahům a objektům, zaměstnanci uvedeni vzhledem k nadefinovaným procesům:

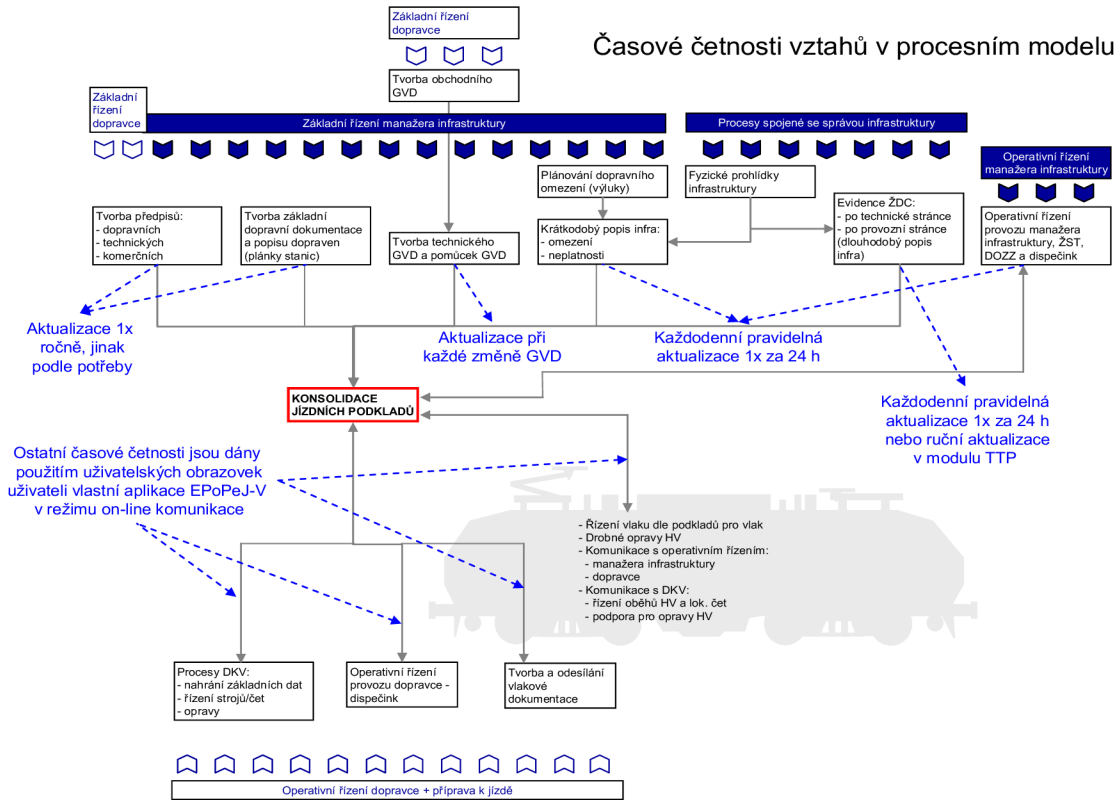
(1) Zaměstnanci provozovatele infrastruktury – bez nárůstu personálu
(2) Zaměstnanci provozovatele infrastruktury – bez nárůstu personálu
(3) Zaměstnanci provozovatele infrastruktury – bez nárůstu personálu
(4) Zaměstnanci provozovatele infrastruktury – bez nárůstu personálu
(5) Zaměstnanci provozovatele infrastruktury – bez nárůstu personálu
(6) Zaměstnanci provozovatele infrastruktury – bez nárůstu personálu
(7) Zaměstnanci provozovatele infrastruktury – bez nárůstu personálu
(8) Zaměstnanci provozovatele infrastruktury – bez nárůstu personálu
(9) Centrální server EPoPeJ-V – nárůst v rámci outsourcingu – 1 správce databáze, 1 analytik – technolog, 1 správce aplikačního serveru, 1 - 2 programátoři, 2 pracovníci HelpDesku
(10) Zaměstnanci dopravce – případný nárůst u správců kmenových dat mimo ČD; Odbor 12 ČD – 1 až 2 zaměstnanci, Odbor 16 ČD – 1 zaměstnanec, Odbor 21 ČD – 1 zaměstnanec; využití stávajících zaměstnanců, bez nárůstu personálu
(11) Zaměstnanci dopravce – bez nárůstu personálu
(12) Zaměstnanci dopravce – bez nárůstu personálu



Legenda ke schématu Přiřazení IS k objektům a vztahům procesního modelu:

- Proces tvorby předpisů dokumentuje databáze NORMIS, vstupuje do EPoPeJ-V ve formě elektronické knihovny viz. bod 3.
- Proces tvorby ZDD a Plánků stanic je zdokumentován jednak v databázi GRAFIKON a na webových stránkách OPŘ a UŽST. Dojde ke sloučení do jednoho datového zdroje v elektronické knihovně.
- Procesy Tvorba předpisů a Tvorba ZDD a Plánků stanic se do systému EPoPeJ-V přenáší ve formě elektronické knihovny strojvedoucího.
- Procesy při sestavě a konstrukci GVD podchycují v současné době tři aplikace: SENA, CEV a ASO. Předávání dat probíhá na základě výměnných souborů. Nově vyvíjená aplikace KANGO má být databázovým zastřešením pro stávající 3 vyjmenované aplikace.
- Proces Tvorba technického GVD a pomůcek GVD má své výstupy do EPoPeJ-V ve formě datového distribučního souboru SJŘ a prezentační soubor SJŘ elektronické knihovny strojvedoucího.
- Proces Krátkodobý popis infrastruktury je ovlivněn vstupy z IS Výluk (ISV + ISV-DZV) a IS SPJ. Tyto informační systémy dokumentují plánovaná a operativní omezení v provozu vzhledem ke stavu dopravní cesty.
- Výstupem z procesu Krátkodobý popis infrastruktury pro potřeby systému EPoPeJ-V budou datové distribuční soubory z ISV a IS SPJ.
- Dlouhodobý popis infrastruktury je popsán Pasportními úlohami dopravní cesty. Pro sestavu JŘ v aplikaci SENA však existují kmenová data, která popisují infrastrukturu z pohledu pro určování časových prvků GVD a tyto aktualizuje správce kmenových dat SENA ručně. Dlouhodobý popis infrastruktury je zdokumentován v databázi GRAFIKON jako TTP.
- Pro systém EPoPeJ-V je výstupem z procesu Dlouhodobý popis infrastruktury datový distribuční soubor z pasportních úloh dopravní cesty s výhledem na modul aktualizace TTP v aplikaci EPoPeJ-V.
- Výstupem pro systém EPoPeJ-V z procesu Operativního řízení provozu… je datový distribuční soubor z aplikace ISOŘ KADR.

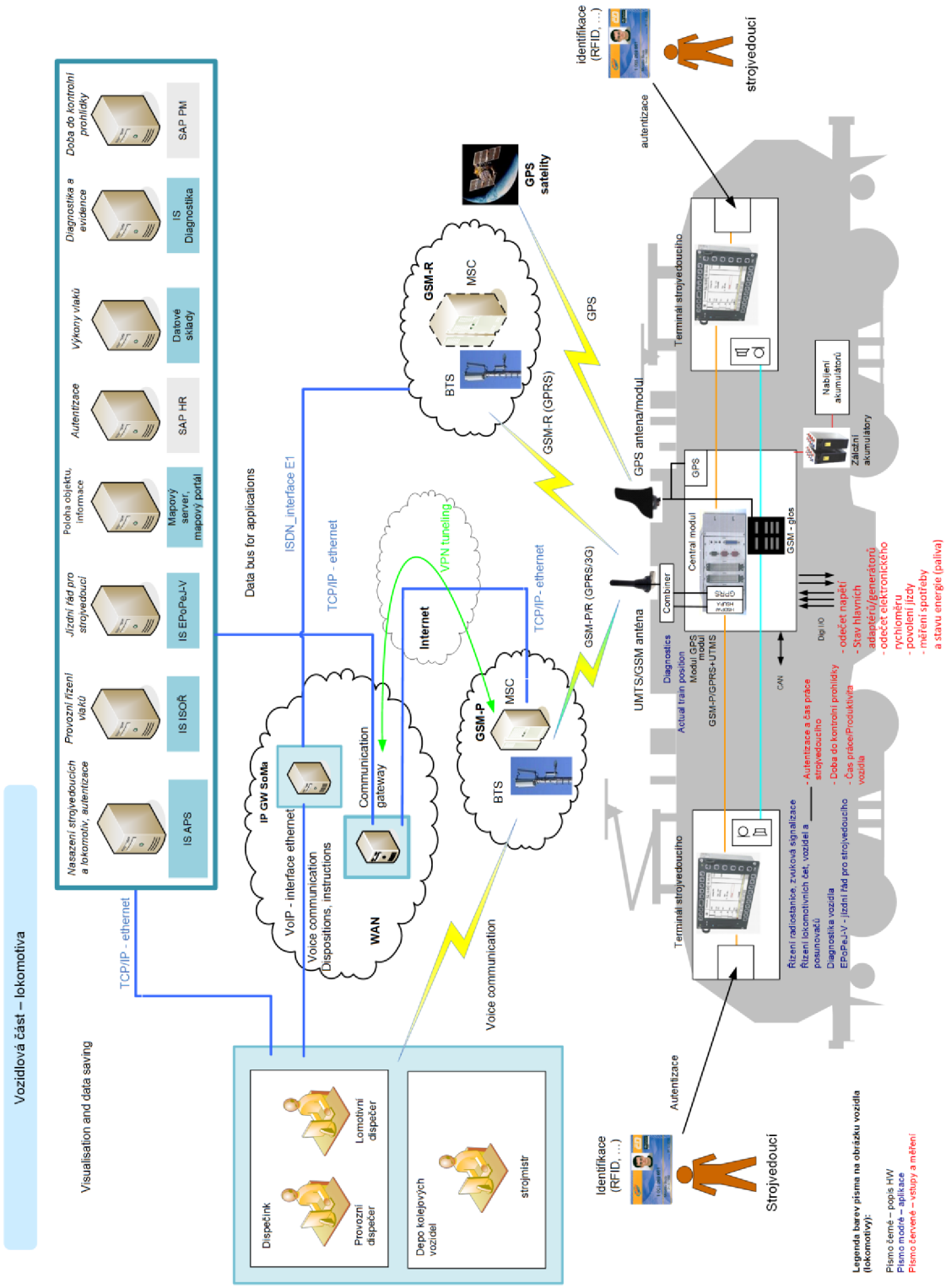
Výstupem pro systém EPoPeJ-V z procesu Tvorba vlakové dokumentace je datový distribuční soubor a výstupní sestava z aplikace CEVIS.



Název procesu	**Informační systém**	**Časová četnost vztahu**
Tvorba předpisů	NORMIS/elektronická knihovna strojvedoucího	Aktualizace pravidelně 1x ročně, další aktualizace podle potřeby změn předpisů
Tvorba ZDD a popis dopraven	Portál O11, weby OPŘ a UŽST/elektronická knihovna strojvedoucího	Aktualizace pravidelně 1x ročně, další aktualizace podle potřeby změn popisu infrastruktury
Tvorba technického GVD a pomůcek GVD	SENA nově KANGO/distribuční soubor SJŘ a SJŘ ZV pro EPoPeJ-V + elektronická knihovna strojvedoucího	Aktualizace při každé změně GVD
Krátkodobý popis infrastruktury (omezení)	ISV, ISV-DZV, IS SPJ/ distribuční soubor ISV, ISV-DZV a IS SPJ pro EPoPeJ-V	Každodenní pravidelná aktualizace 1x za 24 h
Evidence ŽDC (dlouhodobý popis infrastruktury)	Pasportní úlohy dopravní cesty/distribuční soubor z pasportních úloh dopravní cesty pro EPoPeJ-V	Každodenní pravidelná aktualizace 1x za 24 h nebo ruční aktualizace v modulu Aktualizace TTP
Operativní řízení provozu manažera infrastruktury	ISOŘ KADR/distribuční soubor dat z ISOŘ KADR pro EPoPeJ-V	Každodenní pravidelná aktualizace 1x za 24 h
Ostatní procesy s přímým vztahem k EPoPeJ-V	Vlastní aplikace EPoPeJ-V	Časové četnosti jsou dány použitím pořizovacích obrazovek uživateli vlast-ní aplikace EPoPeJ-V v režimu on-line komunikace

Příloha B

Schéma návrhu mobilní části IS (lokomotiva)



Autor DP	**Bc. Václav Nebeský, LL.M.**
Název DP	**Bezpečnostní aspekty informačních technologií v železniční osobní dopravě**
Studijní obor	**Logistika**
Rok obhajoby DP	**2022**
Počet stran	69
Počet příloh	2
Vedoucí DP	Prof. Ing. Václav Cempírek, Ph.D., DBA
Anotace	Železniční doprava jako průmyslové odvětví ve stále větší míře využívá prvky informačních technologií, digitalizace a automatizace. S jejich rychlejším a širším nástupem nepřichází pouze výhody, ale i hrozby, zejména pak z pohledu kybernetické bezpečnosti. Bezpečnostní aspekty se netýkají pouze dopravce samotného, ale i jeho digitálních, tzn. datových a komunikačních vazeb s dalšími rolemi v železničním systému (např. s manažerem infrastruktury nebo s cestujícími). Informační technologie pronikají i do segmentu železničních vozidel.
Klíčová slova	Informační systém, kybernetická bezpečnost, digitalizace, rozhraní, železniční dopravce, manažer infrastruktury, dopravní telematika, architektura informačního systému, penetrační testy, komunikační jednotka, sítě, průmyslový počítač.
Místo uložení	ITC (knihovna) Vysoké školy logistiky v Přerově
Signatura	