ŘÍZENÍ RIZIK SYSTÉMŮ PRO ŘÍZENÍ DOPRAVY

Jan Procházka, Dana Procházková,

PRAHA 2022

Recenzenti:
Doc. Ing. Branislav Lacko, CSc.
Doc. Ing. Petr Šrytr, CSc.

RNDr. Jan Procházka, Ph.D., Doc. RNDr. Dana Procházková, CSc., DrSc.

ISBN 978-80-01-06995-0
Doi: https://doi.org/10.14311/BK.9788001069950

OBSAH

ABSTRAKT

Dopravní systémy patří do kritické infrastruktury. Jsou složité a jejich struktura má povahu socio-kyber-fyzickou (technickou). Při jejich řízení se ve značné míře dnes využívají poloautomatické a automatické systémy řízení. Kvalita řízení závisí jak na hardware, tak software systémů řízení. Velkou roli hraje propojení informačních systémů a systémů, které provádí konkrétní úkony, tj. systém označovaný I&C (information and control). Bezpečný provoz dopravních systémů zajistí jen bezpečný provoz I&C systému za předpokladu adekvátního technického stavu dopravních subsystémů, tj. za garance jejich udržitelného stavu a rozvoje. Při automatizaci systémů řízení pro jejich bezpečnost je třeba řešit nejen projevy a ochranu faktorů technických, životního prostředí a souvisejících s lidmi, ale i kybernetických, a případně i dalších.

Práce „Řízení rizik systémů pro řízení dopravy“ se soustřeďuje na poznání a pochopení selhání dopravních systémů kvůli kybernetickým faktorům a jejich kombinaci s ostatními faktory, protože příčinami havárií a selhání jsou v mnoha případech právě kombinace faktorů. Na základě současného poznání určuje nástroj pro posouzení rizik, jejichž zdroje odpovídají reálnému světu (All-Hazard-Approach), tj. propojeným otevřeným systémům.

Jelikož drážní doprava je vysoce důležitou součástí dopravní infrastruktury a její zabezpečení patří dnes mezi priority v Evropě, a také v České republice, jsou uvedeny konkrétní výsledky právě pro ni.

Klíčová slova: Dopravní infrastruktura; automatizace; informační a řídící systémy; zdroje rizik; bezpečnost; zabezpečení provozu vlaků.

ABSTRACT

Transport systems belong to critical infrastructure. They are complex and their structure has the nature of socio-cyber-physical (technical). Semi-automatic and automatic control systems are used to a large extent. The quality of management depends on both, the hardware and the software of management systems. A major role is played by the interconnection of information systems and systems that carry out specific tasks, i.e. the interconnection of information systems and systems that carry out specific tasks, i.e. the system denoted as information and control system (I&C). The safe operation of transport systems will only ensure the safe operation of the I&C system under the assumption of adequate technical condition of transport subsystems, i.e. at a guarantee of their sustainable condition and development. When automating the control systems for their safety, it is necessary to address not only the manifestations and protection of technical, environmental and human factors, but also cybernetic ones, and possibly others.

The work “Risk management of traffic management systems” focuses on cognition and understanding the failures of transport systems due to cyber factors and combining them with other factors, since causes of accidents and failures in many cases are precisely combinations of factors. Based on current knowledge, it determines a risk assessment tools, the sources of which correspond to the real world (All-Hazard-Approach), i.e. interconnected open systems.

Since rail transport is a highly important part of transport infrastructure and its security is now one of the priorities in Europe and also in the Czech Republic, specific results are presented precisely for it.

Key words: Transport infrastructure; automation; information and control systems; sources of risk; safety; security of trains operation.

SEZNAM ZKRATEK

Zkratka	Název
ALARA	As Low As Reasonably Achievable
ALARP	As Low As Reasonably Practicable
ANSI	American National Standards Institute
ARINC	Aeronautical Radio, Inc.
ATO	Automatic Train Operation
ATP	Automatic Train Protection
ATS	Automatic Train Stop
BOZP	Bezpečnost a ochrana zdraví při práci
CBTC	Communications-Based Train Control
CC	Common Criteria
CENELEC	Evropský výbor pro normalizaci v elektrotechnice
CERT	Computer Emergency Response Team
COBIT	Control Objectives for Information and related Technology
CPS	Cyber Physical System
CSIRT	Computer Security Incident Response Team
CSM	Common Safety Methods
CSMS	Communications and System Management Segment
CST	Common Safety Targets
ČSN	České technické normy
DoS attack	Denial-of-Service Attack
DDoS attack	Distributed Denial-of-Service Attack
DSS	Decision Support System / Systém pro podporu rozhodování
EC	European Commission
EN	European Norm
ENISA	European Union Agency for Cybersecurity
ERTMS	European Rail Traffic Management System
ESA 11	Elektronické zabezpečovací zařízení železnice
ETCS	European Train Control System
EU	European Union
FEMA	Federal Emergency Management Agency

GPS	Global Positioning System
GSM-R	Global System for Mobile Communications – Railway
IAEA	International Atomic Energy Agency
IATA	International Air Transport Association
I&C	Information and Control System
ICAO	International Civil Aviation Organization
IEC	International Electrotechnical Commission
IKS	Vnitřní řídící systém
IP	IP adresa
IRIS	International Railway Industry Standard
ISA	International Society of Automation
ISM pásmo	Radiové pásmo přidělené ITU (International Telecommunication Union)
ISMS	Systém řízení bezpečnosti informací
ISO	International Organization for Standardization
IT	Informační technologie
ITIL	Information Technology Infrastructure Library
MCG	Mobile Communication Gate
MQTT	MQ Telemetry Transport
MILS	Multiple Independent Levels of Security
NIST	National Institute of Standards and Technology
OECD	Organisation for Economic Co-operation and Development
RAMS	Reliability, Availability, Maintainability, Safety
Sb.	Sbírka zákonů
SIL	Safety Integrity Level
SeMS	Security Management System
SeSMS	Security and Safety Management System
SIL	Safety Integrity Level
SL	Security Level
SMS	Safety Management System
SoS	System of Systems / systém systémů
SŘV	Systém řízení vlaků
SSŘV	Správa systému řízení vlaků
TAČR	Technologická agentura České republiky

TQM	Total Quality Management
TS	Technical Specification
TSI	Technical Standards for Interoperability
UITP	International Association for Public Transport
UN	United Nations
UTC	Universal Time Coordinated

PŘEDMLUVA

Inženýrství jako nástroj řešení technických problémů se stává dnes, za situace dominance nástrojů politických, ekonomických, ekologických a dalších, prosazovaných prostřednictvím fungování neúměrného množství politiků, úředníků, právníků, ekonomů a dalších jejich pomocníků včetně masmédií, nástrojem zatlačovaným do pozadí s tím, že hrozí častější výskyt disfunkce subsystémů ucelené technické obsluhy lidských sídel typu *stav nouze, stav obecného ohrožení.* Aktuálně pak stát a veřejná správa nedokáží adekvátně reagovat zejména na klíčové problémy a degradační jevy vývoje lidské společnosti. Příčinou toho je formalizmus a ignorace péče o udržitelný stav a rozvoj lidské společnosti. Poznamenejme, že tato situace je zdrojem celé řady dalších příčin, které generují významná rizika jak ve společnosti, tak v dopravě, která je předmětem předložené knihy.

Autoři předložené práce na základě existujících odborných znalostí a zkušeností skutečných odborníků ukazují, jak je třeba řešit komplikované problémy současnosti ve veřejném zájmu. Práce se tudíž zabývá jedním z aktuálních odborných problémů současnosti, kterým je správná činnost propojených otevřených systémů povahy fyzické, kybernetické a sociální. Aby řešení předmětného problému vedlo k udržitelnému stavu, tak jeho koncept musí být správně strategicky orientován, odborně kompetentní a musí mít jasně stanovené relace mezi limity a podmínkami a správně určené odpovědnosti.

Práce vychází z výsledků projektu RIRIZIBE “CZ.02.2.69/0.0/ 0.0/16_018/0002649” a je zpracována v rámci projektu PRKODI “TAČR s identifikačním číslem CK01000095“.

Autoři práce děkují TAČR za podporu, recenzentům panu doc. Ing. Branislavu Lackovi, CSc. a panu doc. Ing. Petru Šrytrovi, CSc., kteří svými připomínkami a doplňky přispěli ke kvalitě knihy, tj. jak k úrovni odborného obsahu, tak ke srozumitelnosti textu pro čtenáře z odborné veřejnosti. Rovněž děkují vedoucí katedry inženýrství rizik VUT v Brně paní Ing. J. Martincové, PhD. za podporu vydání knihy. V neposlední řadě pak děkují ČVUT v Praze za podporu výzkumu rizik a bezpečnosti složitých systémů a za vydání knihy.

1. ÚVOD

Dopravní infrastruktura je otevřený a složitý systém, který se skládá z mnoha dílčích systémů (subsystémů) a mnoha různých prvků. Její model je otevřený systém systémů (označovaný SoS), který má povahu socio-kyber-fyzickou [1]. Dílčí systémy i prvky mohou pracovat samostatně i dohromady. Celek dohromady plní zcela jedinečný úkol, který je vzdálený od úkolů jednotlivých komponent. Podle poznatků shrnutých v práci [2] jsou pro složité systémy důležité dvě systémové vlastnosti, a to:

- interaktivní složitost,
- těsná spojení.

Těsná spojení jsou nutnou podmínkou k eskalaci nežádoucích jevů vedoucích až k selhání či havárii. Charakterizují se jako proces, který je časově závislý, má malé časové rezervy, je invariantní (v procesu je jediné pokračování – B musí následovat po A), a v důsledku předmětných charakteristik je u něho omezený prostor pro improvizaci.

Interaktivní složitost a těsná spojení mezi entitami v socio-kyber-fyzickém systému za jistých podmínek vyvolávají složité interakce, které jsou neplánované, neočekávané a tvoří většinou neznámé sekvence, které nejsou bezprostředně srozumitelné. V systémech systémů předmětné interakce mají za následek nejednoznačná rozhodnutí, nestabilní preference a konfliktní cíle a obvykle vedou ke kritické situaci v důsledku systémového selhání.

Výše uvedená fakta znamenají, že riziko se tak stává systémovou vlastností. Kvůli složitosti a vysoké propojenosti sledovaných objektů je systematická analýza zranitelností a robustností s ohledem na selhání obtížná, a proto se používají výsledky simulací. Bezpečnost je definována jako nefunkční požadavek a je spojena s vynořujícími se podstatnými, tedy nezanedbatelnými vlastnostmi systému, které závisí na limitech a podmínkách. Zvažované nefunkční stavy a vlastnosti nemohou být přiřazeny k jednotlivým komponentám systému. Vynořují se jako integrující výsledek chování systému. Proto požadavky na bezpečnost jsou formulovány na úrovni celého socio-kyber-fyzického systému a poté sestupným procesem na dílčí systémy [2]; tj. postup shora-dolů. Výsledek působení pohromy (tj. libovolného škodlivého jevu pro aktiva systému či celý systém) o jisté velikosti závisí na okamžitém stavu systému.

Prvky i dílčí systémy mají povahu fyzickou, sociální a kybernetickou. Bezpečnost jejich celku [1] proto závisí jak na dílčích položkách různé povahy, tak na jejich propojeních různé povahy. Proto při jejím zajištění je třeba zvažovat jak rizika spojená s prvky, komponentami, soubory komponent i s celkem (jde o aktiva různého stupně), tak i rizika spojená s jejich propojeními, jež jsou realizovány jak vazbami mezi jednotlivými entitami, tak i s toky, které mezi entitami proudí (jde o vertikální i horizontální aktiva). Vazby jsou těsné, volné a složité. Toky jsou energetické, informační, finanční apod. Jelikož svět se dynamicky vyvíjí, tak se mění jak samotná aktiva, tak jejich propojení i prostředí, ve kterém se aktiva nachází.

Charakteristiky složitých socio-kyber-fyzických systémů jsou shrnuty v práci [1]. V předmětné práci jsou rovněž vyhodnoceny havárie a selhání těchto systémů a uvedeny zásady pro řízení jejich rizik ve prospěch bezpečnosti. Vyhodnocení havárií a selhání ukázalo, že vzájemná provázanost systémů působí za jistých podmínek nežádané závislosti (tzv. interdependences). Proto pochopitelně neplatí, že bezpečnost

složitých systémů, jejichž modelem je systém systémů, je agregací bezpečností dílčích systémů. Pro zajištění bezpečnosti celku se musí respektovat i průřezová rizika, která jsou způsobená vazbami a toky napříč SoS a s okolím. Uvedená skutečnost znamená, že dnes používaná integrovaná bezpečnost, která je založená na řízení integrovaného rizika není vždy zcela na místě u sledovaných objektů. Proto musí být postupně nahrazována integrální bezpečností, při jejímž řízení se provádí i řízení průřezových rizik [1].

Z výše uvedených důvodů významný problém nastává v dopravě u řídících systémů [1], a to hlavně ve spojení se zaváděním poloautomatických a automatických systémů řízení do praxe. Se zaváděním pokrokových systémů řízení je spojeno mnoho problémů, které jsou spojené s propojeními mezi technikou, informacemi a lidským faktorem, který vytváří jak hardware, tak software pro zajištění propojení prvků a komponent. Jde o oblast, která je dosud ve stavu zrodu, a proto nemá ustálená pravidla jako technika; kvalitních norem i pravidel dobré inženýrské praxe je málo.

V obecném smyslu rozumíme řízením usměrňování procesů nebo činností, které probíhají v určitém dynamickém systému. Řízení každé entity dělíme také dle rozsahu odpovědnosti, rozhodování a délky plánovacího horizontu. Každá entita plánuje a řídí své aktivity a procesy především na třech úrovních: strategická (vrcholová, dlouhodobá), taktická (střednědobá) a provozní (operativní, krátkodobá), přičemž hranice mezi jednotlivými vrstvami nejsou pevné a ostré. V současné době se používá procesní a projektové řízení. Řízení technických děl proto znamená propojení procesů řízení lidí a řízení technických procesů ve smyslu jejich ovládání. Řízení ve smyslu ovládání techniky lze provádět manuálně (ručně), poloautomaticky a automaticky. V posledních dvou případech jde o propojení reálného prostoru s kyberprostorem pomocí usměrněných informačních toků, a tím se do řízení technických děl přidává další faktor.

V současné době automatizace proniká do života všech technických děl. Na jednu stranu přináší obrovské výhody a úspory práce lidí a na straně druhé přináší také další rizika. V souvislosti s automatizací je řízení definováno jako cílené působení řídicího systému na řízený objekt tak, aby bylo dosaženo určeného cíle. V praxi se dnes odlišují ovládání, regulace a vyšší formy řízení (optimální a adaptivní řízení, učení a umělá inteligence).

2. SYSTÉMY ŘÍZENÍ V DOPRAVĚ Z POHLEDU LEGISLATIVY

Systémy řízení bezpečnosti v dopravě jsou částečně definovány Evropskými směrnicemi a následně příslušnou legislativou členských zemí. Legislativa je rozdělená pro každou oblast dopravy zvlášť a podle hodnocení v práci [3] je velmi stručná, v mnoha případech nejasná a navíc má vnitřní rozpory.

V průmyslu se pro řízení bezpečnosti uplatňují především systémy řízení kvality založené na procesním a projektovém řízení typu TQM [4], s implementovaným procesem analýzy rizik, respektive standardu ISO 9000 s rozšířenými požadavky pro kvalitu i bezpečnost výrobků v dané oblasti. Pro elektronické systémy, tj. elektrické / elektronické / programovatelné (E/E/PE) se v průmyslu zavádí mezinárodní standard funkční bezpečnosti IEC 61508 [5]. Uvedené přístupy a standardy systémů řízení jsou pro každou průmyslovou oblast upraveny a doplněny příslušnými standardy uvedenými v následujících odstavcích.

Pouze velmi úzká skupina subjektů dopravy zahrnutých do kategorie subjekt kritické infrastruktury je podřízena zákonu č. 240/2010 Sb., který zavádí do sledované oblasti základní principy krizového řízení, tj. povinnost předmětným subjektům vypracovat plán krizové připravenosti na základě krizového plánu dotčené oblasti, který je pravidelně přezkoumáván, a odpovědnost za veškerou součinnost s dalšími subjekty uvedenými v zákoně. Rozpory se projevují hlavně při řešení kritických situací [1,2].

2.1. Analýza legislativních podkladů

Do oblasti řízení bezpečnosti dopravy se zahrnují systémy řízení bezpečnosti informací (ISMS) a kybernetické bezpečnosti (cyber security) [3]. Je nutné poznamenat, že u systémů řízení bezpečnosti dopravy nejde o bezpečnost (safety), sledovanou v práci [1], ale o zabezpečení informací a zabezpečení kyberprostoru (od anglického slova security); v českých podmínkách se ujal nepřesný pojem bezpečnost informací.

Účelem systému ISMS je zajistit tzv. důvěrnost, integritu (tj. celistvost) a dostupnost informace v organizaci resp. kybernetickém prostoru jakéhokoliv systému. Povinnost zavádění ISMS mají pouze některé subjekty definované v zákoně o kybernetické bezpečnosti, tj. v zákoně č. 181/2014 Sb.; jedná se o vlastníky či provozovatele kritické informační infrastruktury nebo provozovatele kritické infrastruktury dle zákonem stanovených kritérií.

Standardů ve sledované oblasti již existuje mnoho, základními jsou normy řady ISO/IEC 27000 [6] pro systémy řízení bezpečnosti založené na systému řízení standardů řady ISO 9000. ISO norma řady 27000 [6] je dle [3] uznávaná výše zmíněným kybernetickým zákonem. Další normou je ISA/IEC 62443 [7] pro zabezpečení průmyslové automatizace a řídicích systémů, která obsahuje jak procesně organizační požadavky, tak i technické požadavky na výrobky v průmyslových sítích, které zvyšují jejich kybernetickou bezpečnost. Dále jsou známé standardy pro hodnocení úrovně zabezpečení produktů v informačních technologiích ISO/IEC 15408 [8], z angličtiny Common Criteria (CC).

Dle analýzy v [3] se kromě leteckého průmyslu v průmyslových oblastech v dopravě informační resp. kybernetická bezpečnost nezavádí vůbec nebo pouze v dílčích a úzce

zaměřených oblastech. V leteckém průmyslu se doporučuje integrace systémů řízení, kde vedle systému řízení bezpečnosti (SMS) je integrován i systém řízení zabezpečení (SeMS) plněním požadavků předpisu L17 [9]. V rámci SeMS lze požadavky normy ISO/IEC 27000 [6] uplatnit.

Výše uvedená fakta implikují tvrzení, že jsou současné dopravní systémy zabezpečené z hlediska funkční bezpečnosti, ale nepřipouští, že se mohou vyskytnout i jiné nepředvídatelné události. To však je v rozporu s realitou, protože např. kybernetický útok a další pohromy (živelní i havárie) mohou uvažovaný systém uvést do abnormálních a kritických podmínek, které výrazným způsobem ohrožují systém i jeho okolí [1].

V automobilové, resp. ***silniční dopravě*** nejsou definované žádné legislativní ani normativní požadavky na zavádění uceleného systému řízení bezpečnosti [3]. Automobilový průmysl zavádí systémy řízení kvality ISO/TS 16949 [10], který je buď založený na standardu ISO 9000, anebo uplatňuje německou normu kvality pro automobilový průmysl VDA [11]. Pro elektronické systémy pak požadavky na řízení rozšiřuje o standard funkční bezpečnosti ISO 26262 [12], který je založený na průmyslovém standardu pro elektrické / elektronické / programovatelné systémy E/E/PE, tj. EN 61508 [5].

Dle [3] v železniční dopravě je základním dokumentem pro zajištění bezpečnosti Směrnice Evropského parlamentu a Rady 2004/49/EC (Směrnice o bezpečnosti železnic) [13]. Uvedená směrnice vedle systému řízení bezpečnosti zavádí i společné bezpečnostní cíle (CST – Common Safety Targets) a společné bezpečnostní metody dle Prováděcího nařízení Komise (EU) 402/2013 (CSM – Common Safety Methods) [14]. Při jakékoliv technické, provozní a organizační změně je nutné ji zdokumentovat, posoudit a odůvodnit její vliv na bezpečnost dle metodiky Drážního úřadu, který je drážní autoritou v ČR stanovenou Ministerstvem dopravy; metodika je založená na CSM [14], tj. na hodnocení rizik.

Část výše uvedené směrnice vztahující se k systému řízení bezpečnosti [13] byla v ČR transponována do vyhlášky č. 376/2006 Sb., o systému bezpečnosti provozování dráhy a železniční dopravy a postupech při vzniku mimořádných událostí na dráhách. Systém řízení bezpečnosti má dle této vyhlášky povinnost zavádět pouze provozovatel dráhy. Předmětný systém řízení bezpečnosti však respektuje pouze řízení systému za normálních podmínek a při tzv. mimořádných událostech. Mimořádné události se ohlašují Drážnímu úřadu, který události vyšetřuje a je-li potřeba, navrhuje bezpečnostní opatření. Podle citované vyhlášky systém řízení bezpečnosti, který je provozovatel dráhy povinen zavádět, má následující požadavky:

1. Provozovatel dráhy a dopravce vede průběžně dokumentaci (informační systém Facility management) o všech důležitých částech systému zajišťujícího bezpečné provozování dráhy celostátní a regionální a drážní dopravy na těchto dráhách. Ve vnitřních předpisech provozovatele dráhy nebo dopravce musí být stanoveno rozdělení povinností v rámci organizace ve vztahu k zajišťování bezpečnosti provozování dráhy a drážní dopravy a stanoven způsob řízení v organizaci na různých úrovních, způsob zapojeni zaměstnanců na všech úrovních řízení do systému zajišťováni bezpečného provozování dráhy nebo drážní dopravy a způsob zajištění soustavného zlepšování systému bezpečnosti.
2. Systém zajišťování bezpečnosti provozování dráhy celostátní a regionální a drážní dopravy na těchto dráhách musí stanovovat:
   a) bezpečnostní zásady a způsob jejich sdělováni všem zaměstnancům,

b) kvalitativní a kvantitativní cíle organizace v oblasti zachování a zvyšováni bezpečnosti a plány a postupy pro dosažení těchto cílů,
c) postupy zajišťující dodržování existujících, nových a změněných technických a provozních norem nebo jiných závazných podmínek stanovených:
   - v technických specifikacích pro interoperabilitu,
   - ve vnitrostátních právních předpisech,
   - v jiných vnitřních předpisech provozovatele dráhy nebo dopravce, nebo
   - v rozhodnutích úřadů státní správy,
d) postupy pro zajištění souladu stavu zařízení s požadavky technických nebo provozních norem a jinými závaznými podmínkami po dobu životnosti zařízení a po dobu jeho provozu,
e) postupy a metody posuzování rizika a zavádění opatření pro usměrňování rizika v případě, že změna provozních podmínek nebo materiály představují nová rizika pro dopravní cestu dráhy nebo provozováni drážní dopravy,
f) programy školení zaměstnanců a systémy, které zajišťují udržování kvalifikace zaměstnanců a odpovídající úroveň plnění úkolů,
g) opatřeni zajišťující dostatečnou informovanost v rámci provozovatele dráhy nebo dopravce a podle potřeby mezi dopravci používajícími tutéž dopravní cestu dráhy,
h) postupy a vzory pro dokumentování bezpečnostních informací a stanovení postupu pro kontrolu předávání nejdůležitějších bezpečnostních informaci,
i) postupy zajišťující, že jsou závažné nehody, nehody, ohrožení a jiné události ovlivňující bezpečné provozováni dráhy a drážní dopravy oznamovány, jsou zjišťovány jejich příčiny a jsou analyzovány, a že jsou přijímána nezbytná preventivní opatření,
j) plány zásahu, varováni a předávání informací v případě mimořádné situace, jež jsou dohodnuty s příslušnými orgány veřejné správy,
k) ustanovení o provádění periodických vnitřních kontrol systému zajišťování bezpečnosti.

Drážní průmysl není vždy povinen, ale je konkurenčním prostředím stimulován k zavedení drážního standardu IRIS [15], který je integrován do stávajícího systému řízení. IRIS rozšiřuje požadavky systému řízení jakosti (dle ISO 9001) s důrazem na kvalitu a bezpečnost vyvíjených a instalovaných systémů v jejich celém životním cyklu, tj. mimo jiné implementuje požadavky EN 50126 pro prokázání bezporuchovosti, dostupnosti, udržovatelnosti a bezpečnosti systému (RAMS) [16]. Principy funkční bezpečnosti jsou dále rozšířené normou EN 50129 [17] pro bezpečnostně relevantní systémy (zabezpečovací zařízení) a EN 50128 [18] pro jakýkoliv software aplikovaný na drahách. Uvedené evropské normy jsou založené na funkční bezpečnosti dle IEC 61508 [5]. Bližší informace o požadavcích standardu IRIS a jemu příbuzných norem jsou uvedeny v práci [19].

Dle zákona č. 49/1997 Sb., o civilním letectví rozumíme leteckou dopravou civilní letectví. Předmětný zákon dle [3] subjektům civilního letectví napřímo neukládá povinnost zavádění systému řízení bezpečnosti. Ukládá dílčí technické a organizační povinnosti, které lze do systému řízení bezpečnosti implementovat, ale samostatně netvoří ucelený systém. Vybraným subjektům, tj. provozovatelům letišť a leteckých staveb, osobám pověřeným provozováním leteckých služeb, provozovatelům leteckých činností a ostatním osobám zúčastněným na civilním letectví je udělena povinnost dodržovat letecké předpisy, které jsou v souladu s mezinárodními smlouvami, které jsou součástí právního řádu, vydávány Mezinárodní organizací pro civilní letectví (ICAO, tj.

předpisy řady L), Sdružením leteckých úřadů (JAA) podle předpisů Evropské unie (kodexy JAR, Part) a Evropskou organizací pro bezpečnost leteckého provozu EUROCONTROL.

Systém řízení bezpečnosti je vzhledem k výše uvedenému dán předpisem L19 (v originále ICAO Annex 19) [9]. Předpis udává povinnost zavádět systém řízení bezpečnosti následujícím subjektům: schválené organizace pro výcvik, provozovatele letounů a vrtulníků schválení k provozu mezinárodní obchodní letecké dopravy, údržba předmětných letounů a vrtulníků, organizace odpovědné za typový návrh a výrobci, provozovatelé letových provozních služeb (ATS), provozovatelé certifikovaných letišť; podrobnější kritéria, viz zmíněný předpis. Systém řízení bezpečnosti musí být přiměřený dané organizaci.

Minimální požadavky předpisu pro provozovatele všeobecného letectví s velkými nebo proudovými letadly má povinnost zavést:

a) proces identifikace aktuálních a potenciálních nebezpečí a posuzování souvisejících bezpečnostních rizik,
b) proces vývoje a zavádění nápravných opatření nutných k udržení přijatelné úrovně bezpečnosti,
c) ustanovení o průběžném sledování a pravidelném vyhodnocování vhodnosti a účinnosti činností spojených s řízením bezpečnosti.

Pro ostatní výše uvedené subjekty jsou požadavky členěné do čtyř následujících kapitol:

1. Politika a cíle bezpečnosti; závazek a zodpovědnost vedení; odpovědnosti za bezpečnost; jmenování klíčového bezpečnostního personálu; koordinace plánování reakce v případě nouze; dokumentace systému řízení bezpečnosti (SMS).
2. Řízení bezpečnostních rizik; identifikace nebezpečí; hodnocení a zmírňovaní rizik.
3. Zajišťování bezpečnosti: sledování a měření výkonnosti v oblasti bezpečnosti; řízení změn; průběžné zdokonalování SMS.
4. Prosazování bezpečnosti: výcvik a vzdělávání; komunikace o bezpečnosti.

Podrobnější požadavky na implementaci SMS je uveden v dokumentu Doc 9859 Safety Management Manual (tj. manuál řízení bezpečnosti) [20].

Systém řízení bezpečnosti v letecké dopravě je z uvedených tří dopravních oblastí nejrozšířenější, stejně jako v drážní dopravě je založen na principech TQM [4], ale navíc připouští nejen technické problémy, ale i problémy lidského chování (lidský faktor) a také poruchy v organizaci (připouští organizační havárie). Je založen na budování tzv. kultury bezpečnosti. Případnou havárii připisuje několika faktorům: organizaci (manažerské rozhodování a procesy organizace); pracovišti (pracovní podmínky); lidem (lidská chyba a narušení); a ochraně (předpisy, tréning, technologie), s tím, že uvedená posloupnost faktorů je tzv. trajektorií skrytých podmínek pro výskyt havárie.

Předmětná příručka [20] doporučuje SMS integrovat do integrovaného systému řízení, který je flexibilnější pro úpravu směrnic s více systémy, jako jsou například řízení jakosti (QMS), životního prostředí (EMS), ochrana zdraví a bezpečnost práce (OHAS, v češtině BOZP) nebo v kontextu integrální bezpečnosti také důležitý systém řízení zabezpečení (SeMS). SeMS je založen na plnění požadavků předpisu L17 [21] Ochrana mezinárodního civilního letectví před protiprávními činy. Předmětný předpis je cílen především zajištění kvality bezpečnostních opatření (se zaměřením na lidi, místa, dopravní prostředky a kyber prostor) a prevence protiprávních činů, kdežto

ucelený systém SeMS klade více důraz na identifikaci hrozeb a rizik, jejich hodnocení, prevenci a přípravu nouzových a krizových plánů [9].

Letecký průmysl, podobně jako automobilový a drážní, aplikuje pro vývoj elektronických systémů vlastní řadu standardů zajišťující jejich funkční bezpečnost a zabezpečení, prostřednictvím definovaného životního cyklu již od raných fází vývoje [22].

Pro porovnání legislativy v jednotlivých oblastech dopravní infrastruktury, práce [3] člení dopravní systémy vertikálně do kategorií infrastruktury a dopravních prostředků. Infrastrukturální prvky dělí na stavby a konstrukce (zastávky, nádraží, letiště, dopravní cesty, příslušenství), řídicí a zabezpečovací systémy a jiná elektronická zařízení. Dopravní prostředky zahrnují veškeré dopravní prostředky a jiné mobilní části dopravy vyskytující se na příslušné dopravní cestě (se zaměřením na E/E/PE). Do vertikálního rozdělení patří ještě řízený systém, tj. doprava, včetně jeho obsluhy (tj. personál, řidiči, strojvedoucí a piloti), a dále přeprava jakožto produkt dopravy (přeprava lidí a zboží). Horizontálně rozlišuje jednotlivé druhy dopravy.

V tabulce 1, převzaté z práce [3] je pro každou kategorii uvedený legislativní či normativní požadavek ve vztahu k bezpečnosti, tzn. příslušná legislativa nebo norma požaduje přímá technická nebo organizační opatření. Ve sloučených sloupcích je uvedený požadavek společný. Seznam uvedený v tabulce 1 je pouze přehled nejdůležitějších požadavků, nejde o konečný seznam veškerých závazných legislativních a normativních požadavků. Vzhledem k rozsahu Tabulka 1 neobsahuje požadavky Evropských směrnic a nařízení, které jsou do legislativy integrovány. Z důvodu zacílení práce na železniční, silniční a leteckou dopravu nejsou zmíněny vodní doprava, doprava prostřednictvím vedení inženýrských sítí včetně perspektivní dopravy komunálního odpadu

Tabulka 1. Legislativní a normativní požadavky ve vztahu k bezpečnosti silniční, železniční a letecké dopravy; převzato z [3].

	Silniční doprava	**Železniční doprava**	**Letecká doprava**
(Společné pro infrastrukturu a dopravní prostředky):	Zákon č. 13/1997 Sb., o pozemních komunikacích; Vyhláška MDS č. 104/1997 Sb., kterou se provádí zákon o pozemních komunikacích; + závazné a volitelné technické normy ČSN řady 73 xxx.	Zákon č. 266/1994 Sb., o dráhách; Vyhláška MD č. 100/1995 Sb., kterou se stanoví podmínky pro provoz, konstrukci a výrobu určených technických zařízení a jejich konkretizace; Vyhláška Ministerstva dopravy č. 177/1995 Sb., kterou se vydává stavební a technický řád drah; Příslušné normy řady ČSN EN řady 50 xxx;	Zákon č. 49/1997 Sb., o civilním letectví; Vyhláška MDS č. 108/1997 Sb., kterou se provádí zákon č. 49/1997 Sb., o civilním letectví; Příslušné předpisy řady L, JAR a Part.

		Nařízení vlády č. 133/2005 Sb. Nařízení vlády o technických požadavcích na provozní a technickou propojenost evropského železničního systému.	
Infrastruktura – stavby a konstrukce	Zákon č. 183/2006 Sb., o územním plánování a stavebním řádu (stavební zákon); Zákon č. 90/2016 Sb., o posuzování shody stanovených výrobků při jejich dodávání na trh; Prováděcí předpisy k zákonu č. 90/2016 Sb.; Zákon č. 22/1997 Sb., o technických požadavcích na výrobky a o změně a doplnění některých zákonů, ve znění pozdějších předpisů; Vyhláška č. 146/2008 Sb., o rozsahu a obsahu projektové dokumentace dopravních staveb; Vyhláška č. 398/2009 Sb., o obecných technických požadavcích zabezpečujících bezbariérové užívání staveb.		
Infrastruktura – řídicí a zabezpečovací systémy a jiná elektronická zařízení	Zákon č. 90/2016 Sb., o posuzování shody stanovených výrobků při jejich dodávání na trh; Prováděcí předpisy k zákonu č. 90/2016 Sb.; Zákon č. 22/1997 Sb., o technických požadavcích na výrobky a o změně a doplnění některých zákonů, ve znění pozdějších předpisů.		
	ČSN EN 61508 Funkční bezpečnost E/E/PE; ČSN normy třídy 0182 až 0184 pro dopravní telematiku.	ČSN EN 50126 Drážní zařízení - Stanovení a prokázání bezporuchovosti, pohotovosti, udržovatelnosti a bezpečnosti (RAMS).	ČSN EN 61508 Funkční bezpečnost E/E/PE. ČSN normy řady třídy 31 (např. ČSN EN 9100 systémy managementu jakosti pro letectví, ČSN EN 31 9809 – 22 radiolokační zařízení, aj.).
Dopravní prostředky	Zákon č. 56/2001 Sb., o podmínkách provozu vozidel na pozemních komunikacích + Vyhláška č. 341,2,3/2014 Sb.;	ČSN EN 50155 Drážní zařízení - Elektronická zařízení drážních vozidel; výše uvedený standard zahrnuje mimo jiné i: ČSN EN 50126,	ARP4761 Procesy posuzování bezpečnosti; ARP4754/ED-79 Proces vývoje systému;

	ISO 26262 Silniční vozidla - Funkční bezpečnost.	ČSN EN 50129, ČSN EN 50128, ČSN EN 50159.	DO-297/ED-124 integrovaná modulární avionika; DO-187C/ED-12C Proces vývoje SW; DO-254/ED-80 Proces vývoje HW; DO-160D/ED-14D Podmínky prostředí a testovací procedury.
Doprava a její obsluha, přeprava osob a zboží.	Zákon č. 255/2012 Sb., kontrolní řád; Zákon č. 194/2010 Sb., o veřejných službách v přepravě cestujících; Vyhláška MDS č. 175/2000 Sb., o přepravním řádu pro veřejnou drážní a silniční osobní dopravu; Nařízení vlády č. 63/2011 Sb. o stanovení minimálních hodnot a ukazatelů standardů kvality a bezpečnosti a o způsobu jejich prokazování v souvislosti s poskytováním veřejných služeb v přepravě cestujících; Nařízení vlády č. 295/2010 Sb., ze dne 20. října 2010 o stanovení požadavků a postupů pro zajištění propojitelnosti elektronických systémů plateb a odbavení cestujících.		
	Zákon č. 13/1997 Sb., o pozemních komunikacích; Zákon č. 361/2000 Sb., o provozu na pozemních + Vyhláška č. 31/2001 Sb., Vyhláška č. 277/2004 Sb.; Zákon č. 247/2000 Sb., o získávání a zdokonalování odborné způsobilosti k řízení motorových vozidel + Vyhláška č. 167/2002 Sb.,	Zákon č. 266/1994 Sb., o dráhách; Vyhláška č. 175/2000 Sb., o přepravním řádu pro veřejnou drážní a silniční osobní dopravy; Vyhláška č. 101/1995 Sb., kterou se vydává Řád pro zdravotní způsobilost osob při provozování dráhy a drážní dopravy; Vyhláška č. 16/2012 Sb., o odborné způsobilosti osob řídících drážní vozidlo a osob provádějících | revize, prohlídky a	Zákon č. 49/1997 Sb., o civilním letectví; Vyhláška MDS č. 108/1997 Sb., kterou se provádí zákon č. 49/1997 Sb., o civilním letectví; Vyhláška MD č. 410/2006 Sb., o ochraně civilního letectví před protiprávními činy; Vyhláška MD č. 466/2006 Sb., o bezpečnostní letové normě; Příslušné předpisy řady L, JAR a Part.

	Vyhláška č. 156/2008 Sb.; Vyhláška č. 522/2006 Sb., o státním odborném dozoru a kontrolách v silniční dopravě; Vyhláška č. 175/2000 Sb., o přepravním řádu pro veřejnou drážní a silniční osobní dopravy; Zákon č. 194/2010 Sb., o veřejných službách v přepravě cestujících a o změně dalších zákonů.	zkoušky určených technických zařízení; Vyhláška č. 173/1995 Sb. dopravní řád drah, Vyhláška č. 351/2004 Sb., o rozsahu služeb poskytovaných provozovatelem dráhy dopravci; Vyhláška č. 209/2006 Sb., o požadavcích na přípustné emise znečišťujících látek ve výfukových plynech spalovacího hnacího motoru drážního vozidla.; Vyhláška č. 376 /2006 Sb., o systému bezpečnosti provozování dráhy a drážní dopravy a postupech při vzniku mimořádných událostí na dráhách; Nařízení vlády č. 1/2000 Sb., o přepravním řádu pro veřejnou drážní nákladní dopravu.	
Přeprava nebezpečných věcí	Evropská dohoda o mezinárodní silniční přepravě nebezpečných věcí (ADR).	Přeprava nebezpečných věcí (RID); Nařízení vlády č. 208/2011 Sb., o technických požadavcích na přepravitelná tlaková zařízení.	Předpis L18.

Podle výsledků v práci [3] porovnání normativního systému řízení bezpečnosti s dokumenty určenými pro drážní a leteckou dopravu není v dopravě řízena integrální

bezpečnost a jsou zvažována pouze některá vybraná ohrožení, je zde absence řízení aktiv (jejich identifikace, určení kritičností, ochrana atd..). Oblast informačních technologií řízena normami řady ISO 27000 [6] poskytuje proaktivnější přístup, zohlednění tzv. kontextu organizace, zahrnuje řízení aktiv, ukládá povinnost přípravy plánů kontinuity v případě výskytu i neočekávané události. V oblasti IT je také stanovena lepší vertikální úroveň komunikace, např. skupinami CERT (Computer Emergency Response Team) nebo jinými typy CSIRT (Computer Security Incident Response Team), a směrem do nižších úrovní rozdělení vlastníků a správců aktiv. Horizontální úroveň zde však chybí a chybí i návaznost na jiné oblasti. V praxi v oblasti IT dochází také k mnoha nedorozuměním mezi odborníky IT a odborníky působících v různých průmyslových doménách. Přitom je používaná terminologie většinou stejná, ale je jinak chápána koncepce rizika, kritičnosti, v IT také pojem důvěrnosti, integrity a dostupnosti [3].

2.2. Analýza předpisu o zabezpečení průmyslových automatizovaných systémů řízení

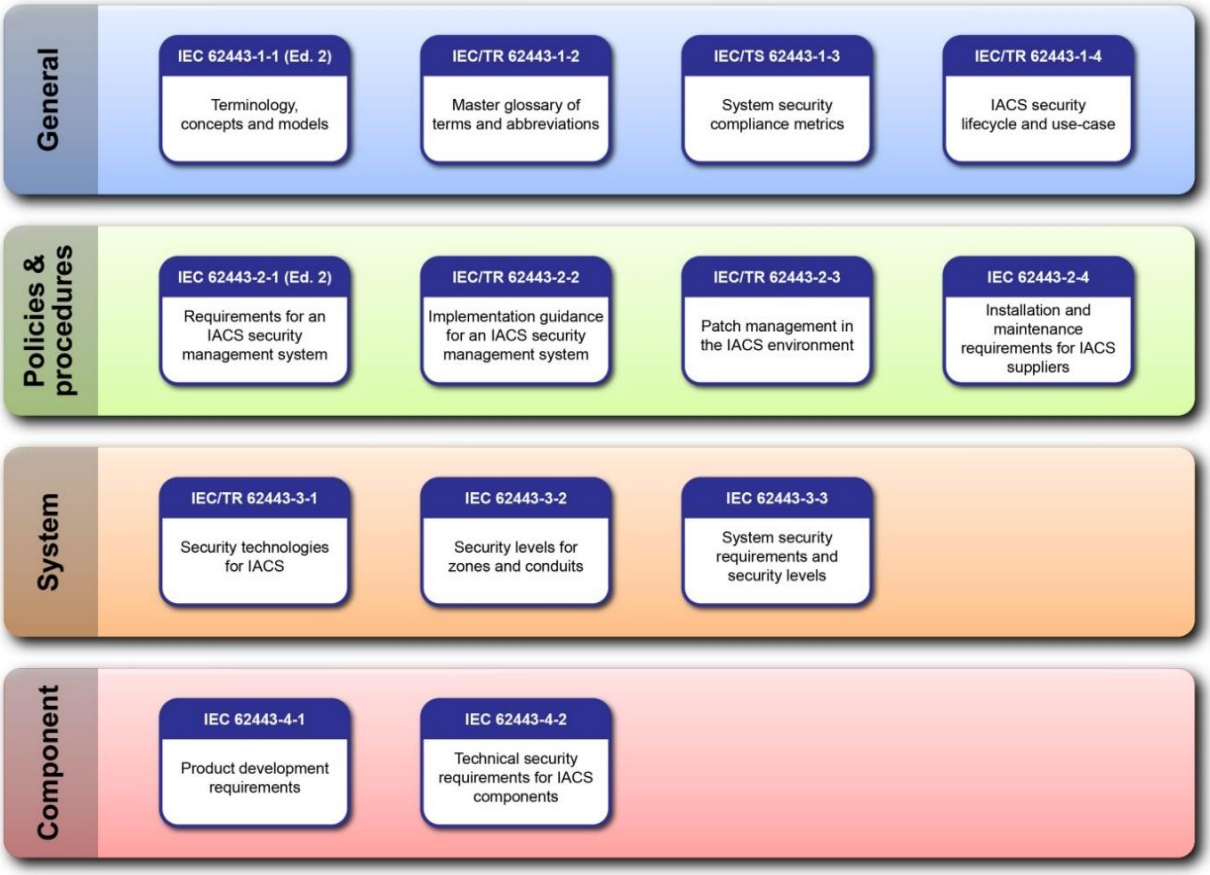
Automatizované systémy řízení v průmyslu, zkráceně I&C systémy stále více pronikají do praxe. Pro jejich zabezpečení byla ISA (International Society for Automation) vytvořena norma ANSI/ISA 62443 [7], která se stala normou IEC (International Electrotechnical Commission). Předmětná norma hraje velkou roli, protože se zabývá kybernetickou bezpečností složitých technologických systémů. Vznikla v návaznosti na problematiku řízení a automatizace v rámci kritické infrastruktury a v průmyslu V4.0. Norma byla vytvořená v USA jako soubor již známých a prověřených postupů a opatření pro zajištění požadovaných cílů bezpečnosti. IEC 62443 upravuje informační a řídící systémy podniků. IEC 62443 je používaná a uznávaná i v Evropě, ačkoliv na jejím základě probíhá diskuse standardizační skupiny o potřebách kybernetické bezpečnosti specifických pro Evropu.

Dnes norma IEC 62443 obsahuje dále uvedené části:

1. IEC 62443-1-1, *Průmyslové komunikační sítě-Zabezpečení sítě a systému-Část 1-1: Terminologie, koncepty a modely*
2. IEC 62443-2-1, *Průmyslové komunikační sítě-Zabezpečení sítě a systému-Část 2-1: Zavádění programu zabezpečení průmyslové automatizace a řídicího systému*
3. IEC 62443-2-3, *Zabezpečení pro průmyslové automatizační a řídicí systémy-Část 2-3: Správa záplat v prostředí IACS*
4. IEC 62443-2-4, *Zabezpečení pro průmyslové automatizační a řídicí systémy-Část 2-4: Požadavky programu zabezpečení pro poskytovatele služeb IACS*
5. IEC 62443-3-1, *Průmyslové komunikační sítě-Zabezpečení sítě a systému-Část 3-1: Bezpečnostní technologie pro průmyslové automatizační a řídicí systémy*
6. IEC 62443-3-2, *Zabezpečení pro průmyslové automatizační a řídicí systémy-Část 3-2: Posouzení bezpečnostních rizik pro návrh systému*
7. IEC 62443-3-3, *Průmyslové komunikační sítě-Zabezpečení sítě a systému-Část 3-3: Požadavky na zabezpečení systému a úrovně zabezpečení*
8. IEC 62443-4-1, *Zabezpečení pro průmyslové automatizační a řídicí systémy-Část 4-1: Požadavky na životní cyklus zabezpečeného vývoje produktu*

9. IEC 62443-4-2, *Zabezpečení pro průmyslové automatizační a řídicí systémy-Část 4-2: Technické bezpečnostní požadavky na komponenty IACS*

Předmětná norma se skládá z několika částí, obrázek 1. Je rozdělena do 4 skupin standardů, které jsou navzájem propojené či se v řadě oblastí překrývají.



Obr. 1. Struktura normy IEC/ISA 62443 [7].

První skupina se zabývá základními ustanoveními terminologie a principů používaných v normě. IEC 62443-1-1 ukazuje, že do informačních systémů, které jsou použity pro výrobu, patří personál, hardware a software, které mohou ovlivnit bezpečnost, zabezpečení či spolehlivost provozních procesů. Z toho vyplývají požadavky na architekturu prvků pro zabezpečení.

Druhá skupina se zabývá provozem kybernetických systémů a slouží pro potřeby operátora technologie (například provozovatele dopravních cest, nebo dopravce). IEC 62443-2-1 zavádí průmyslovou automatizaci a program zabezpečení systému kontroly. Popisuje prvky nutné pro založení CSMS. Patří sem: analýza rizik; určení rizik CSMS; monitoring a vylepšování CSMS.

Třetí skupina se zabývá problematikou kybernetického systému jako celku a slouží pro potřeby integrace jednotlivých technologických podsystémů a komponent v zájmu systémové bezpečnosti. IEC 62443-3-3 definuje úroveň zabezpečení (cílová hodnota SL-T; dosažitelná hodnota SL-A; hodnota vložené (inherentní) schopnosti SL-C. Čtvrtá skupina je pak pro výrobce jednotlivých komponent kybernetického systému a definuje

požadavky na proces vývoje a podpory dané komponenty stejně jako na komponentu samotnou.

Pro použití normy je potřeba vždy určit, v jaké části životnosti a kontextu kybernetického systému se posuzovaná problematika nachází. Následně se musí určit, které části normy se k dané problematice vztahují. V rámci jednotlivých problému se pak neaplikují všechny obsazené požadavky, ale na základě analýzy rizik se vyberou vhodná, dosažitelná a účinná opatření. Na základě výsledku analýzy rizik se určí míra zabezpečení, které je potřeba v daném případě dosáhnout. Tedy, jak velké riziko je potřeba danými opatřeními pokrýt. Bezpečnostní úroveň je rozdělena do pěti úrovní 0-4, které jsou označované jako security level (úroveň zabezpečení) od nezabezpečeného systému (SL0), až po systém zabezpečený proti hrozbám s velkými zdroji pro útok (SL4).

Hlavním přínosem normy IEC 62443 není vytvoření nových postupů, ale utřídění ověřených postupů do uceleného systémů řízení všech zainteresovaných stran. Předmětná změna na systémový přístup se promítla i do oblasti dopravy, která je realizovaná kyber-fyzickými systémy. Kybernetické hrozby tak neohrožují pouze chráněná aktiva (zájmy) informačního charakteru, ale i majetek a životy lidí. Letecká doprava má již dlouhodobě vysoké požadavky na architekturu kybernetických systémů, například ARINC 653 [23]. V oblasti železnice dosud převládají čistě technické normy, které sice dobře definují požadavky na jednotlivé komponenty, chybí však systémové propojení s oblastí informačních technologií, proto poslední kapitola řeší předmětný problém.

3. INFORMAČNÍ TECHNOLOGIE, AUTOMATICKÉ ŘÍZENÍ A SYSTÉMY ŘÍZENÍ BEZPEČNOSTI

Dále soustředíme pozornost jak na základy spojené s informačními technologiemi, tak na základy spojené s automatizovaným řízením. Potom se budeme věnovat principům systémů pro řízení bezpečnosti / zabezpečení u objektů s automatizovaným řízením.

3.1. Informační technologie

Informace, informační systémy a technologie zahrnují velmi širokou oblast, která vytváří vazby mezi systémy. Informace dnes řadíme vedle materiálových, energetických a finančních zdrojů k hlavním faktorům podmiňujícím pokrok nejen v technice, ale ve všech oborech lidské činnosti [24]. Informační toky v systémech vytváří důležitá propojení a spřažení prvků i celých systémů ve složitých objektech. Bez jisté míry informace totiž není možné vytvářet a řídit procesy jakékoliv povahy.

Z pohledu praxe zvyšování informačního výkonu, a to zvláště v případě kritické infrastruktury se nesmí narušit zabezpečení systému a u zvlášť důležitých položek se musí být garantován bezpečný systém [24]. Z tohoto hlediska, je bezpečnost automatizovaných řídících systémů soubor opatření a činností, které zabezpečují všechny informace a informační toky v systému tak, aby mohl řízený systém vykonávat své funkce bezpečně, tj. aby ani při svých kritických stavech způsobených poruchami neohrozil sám sebe ani své okolí. Proces zabezpečení informací spočívá v ochraně důležitých aktiv kybernetického (informačního) systému tak, aby byla pro důležité informace zajištěna požadovaná úroveň dostupnosti, integrity a důvěrnosti [25,26]:

- dostupnost znamená přístupnost a použitelnost informace na žádost oprávněné entity,
- integrita znamená přesnost a úplnost informace,
- důvěrnost znamená, že informace není dostupná nebo není odhalena neoprávněným jednotlivcům, entitám nebo procesům.

Předmětné požadavky jsou často konfliktní, např. zajištěním důvěrnosti snižujeme dostupnost a integritu a také časové nároky na kódování a dekódování, přenos, autentizaci apod. [25,26]. U procesních informačních systémů v dopravě převládají především požadavky na dostupnost a integritu, kdežto důvěrnost nemá tak velkou prioritu [25,26].

Pro zajištění vysoké bezpečnosti, tj. vysokého informačního výkonu a zabezpečení kybernetických systémů se aplikují přístupy procesního a projektového řízení typu TQM (Total Quality Management) [4], ze kterých vychází používané metody i mezinárodní a evropské standardy pro systémy řízení [26]. Účelem výstavby systémů řízení je najít ekonomicky efektivní procesy, které zajišťují jistou míru bezpečnosti a zabezpečení kyber-fyzických systémů, a to je sledováno ve všech fázích, tj. od návrhu, přes analýzu a vývoj, konstrukci, provoz, modernizaci až likvidaci [25].

Informační systémy implementují informační technologie a jsou zaváděny ve všech systémech pro řízení dopravy. Informační technologie interpretují, jsou pomocí nich řízeny, anebo v případě automatizovaných provozů, sami řídí veškeré zmíněné kvalitativní i bezpečnostní parametry. Informační systémy a technologie jsou nedílnou

součástí drážních systémů. Tabulka 2 [27,28] uvádí příklady využití informačních systémů v různých oblastech drážní dopravy.

Správně zvolené parametry uvedených systémů zajišťují velikost jejich informačního výkonu, tj. kvalitu informace umožňující efektivní reakci systému na případné nežádoucí stavy. Tímto zlepšují bezpečnost drah, a to ne jen v normálních podmínkách, ale i v abnormálních a zejména kritických podmínkách [27,28].

Tabulka 2. Příklady využití informačních systémů na drahách; převzato z [27,28].

Oblast	**Proces**
Řízení a plánování (management)	Vyhodnocování dat z provozu Tvorba jízdních řádů Rozpis služeb zaměstnanců Rozhodovací, ekonomické, účetní činnosti Komunikace se záchrannými složkami a s policií
Řízení provozu	Centrální dohled a řízení, dispečerské činnosti Staniční a traťové technologie Sběr a zpracování dat na trase vlaků Komunikace mezi stacionárními a vlakovými systémy Zabezpečovací zařízení
Provoz vlaku	Řízení vlaku, vlakový počítač Datové přenosy mezi vlakovými zařízeními Sledování a řízení vlakových zařízení (dveře, klimatizace, vlakový rozhlas, energetická zařízení) Rozhraní technika – strojvedoucí
Cestující	Informační tabule Systémy odbavení cestujících Zábavná zařízení ve vlaku, wi-fi Navigační systémy – směrové tabule Navigační systémy pro hendikepované

V rámci řízení drážní dopravy se uplatňují především akční procesní informační systémy [24], tj. informační systémy se zpětnou vazbou. Dle práce [24] pro zajištění bezpečnosti řídicích systémů je důležité provozovat informační systémy, které poskytují co nejrychlejší a správné rozhodnutí, což úzce souvisí s informačním výkonem. Dle současného poznání řídicí systémy, které se opírají o vyšší úroveň znalostí, jsou schopné rychlejšího správného rozhodnutí při menší zátěži, tj. rozhodují rychleji.

Každý automatický systém řízení má povahu kyber-fyzickou a pracuje správně pouze za jistých předpokladů, tj. okolních podmínek. Proto má stanovené jisté limity a podmínky, které podmiňují jeho kvalitativní parametry (tj. bezpečnost, spolehlivost, dostupnost, celistvost, kontinuitu a přesnost). Z tohoto důvodu musí existovat mechanismy zajišťující okolní podmínky systému v takovém stavu, který odpovídá stanoveným limitám a podmínkám. Navíc musí být zajištěné plány pro případ, pokud okolní stav systému stanovené podmínky překročí, tj. nastanou abnormální a kritické podmínky v případě výskytu pohrom. Předmětnou problematikou se zabývají ***procesy zajištění informační bezpečnosti*** (přesněji zabezpečení, tj. security), které jsou založené na ochraně důležitých kybernetických (informačních) aktiv způsobem, který pro důležité informace stanovuje požadovaný stupeň důvěrnosti, integrity a dostupnosti - CIA (Confidentiality, Integrity and Availability) [29].

Cílem systémů používaných v řízení technických děl a lidské společnosti je nalézt ekonomicky efektivní procesy, které zajišťují vysokou úroveň zabezpečení kybernetických (kyber-fyzických) systémů, a to v průběhu celého životního cyklu systému, tj. od koncepce, analýzy, návrhu, výstavby, konstrukce, provozu, modernizace, až k likvidaci [29,30]. Uvedené procesy jsou založené na procesním a projektovém řízení TQM (Total Quality Management) [4].

Pravděpodobnost včasného a správného rozhodnutí k zabránění nebo zmírnění dopadů nepříznivých událostí, a to především za abnormálních a kritických podmínek, lze dle [31] dosáhnout:

- vyšší znalostí problémů a zranitelností (uvedených v předchozím odstavci), tj. znalost struktury systémů jejich vazeb, rozdílů a prostředí,
- a vyšším informačním výkonem.

Znalost systému a informační výkon spolu souvisí a jsou limitované fyzikálními vlastnostmi systémů, proto je nutné hledat vhodnou rovnováhu. Informační výkon zvýšíme buď mírou informace nebo informačním tokem. Míra informace závisí na znalosti systému a jeho schopnosti interpretace syntaktických řetězců v datovém toku [31].

Informační tok v čase zvýšíme přenosovou rychlostí a kapacitou přenosového média (které jsou taktéž limitované). Systémy s vyšší mírou znalosti potřebují nižší informační tok, jelikož ten obsahuje vyšší míru informace (např. jeden bit může znamenat jednu konkrétní událost na kterou musí systém reagovat). Naopak znalost systému je limitována jeho výpočetním výkonem, pamětí, ontologií a/nebo kognitivními schopnostmi. Záleží, zda znalost přiřazujeme přirozeným či umělým systémům (člověk/stroj, fyzika/kybernetika, společnost/technika a technologie) [31].

Zvyšování pravděpodobnosti provedení včasného a správného rozhodnutí znamená zvyšování bezpečnosti, tj. zavádění opatření pro zvýšení bezpečí lidí. Zvýšení bezpečnosti vede ke snížení kritičnosti.

3.2. Řízení rizik poloautomatických a automatizovaných systémů řízení

Automatické (automatizované) řízení se obvykle dělí na logické, spojité, diskrétní a fuzzy řízení. Při jeho aplikaci se dle [32] nejčastěji používají:

- rozdělení pravděpodobnosti: normální, log-normální, Weibullovo a Gamma,
- teorie Markových procesů, Kolmogorovy rovnice a další.

V teorii automatického řízení je zdůrazněn význam systémového přístupu k řešení automatizačních úloh a praxe vyžaduje kvantum znalostí z oblasti informačních technologií [19]. Stále více je automatické řízení realizované pomocí kybernetických sítí propojených přes internet. Jelikož pro internet je charakteristická anonymita uživatelů, globální dostupnost a souběžné používání mnoha různých technologií, je zabezpečení informačních systémů připojených k internetu dosti obtížné.

Na základě současného odborného poznání [33-37], pravidla automatického řízení jsou pro daný socio-kyber-fyzický systém vytvářena na základě modelování založeném na teorii spolehlivosti. Na základě dříve uvedených skutečností spolehlivost zařízení se buduje jen na základě dat o náhodných procesech. Proto není zaručena bezpečnost zařízení za všech podmínek, tj. kritických a extrémních podmínek vyvolaných znalostními nedostatky nebo extrémními vlivy. Na základě předmětné skutečnosti vzniká celá řada dalších zdrojů rizik pro technická díla, a to hlavně těch, která používají dálkové přenosy dat.

Na základě představy o propojení řídicího a řízeného systému v [32], je zřejmé, že základní význam v automatickém řízení mají zpětné vazby, na jejichž základě řídicí systémy upravují činnost celého technického díla podle informací z řízených systémů. Kladné zpětné vazby podporují výsledky řízených procesů a záporné je naopak oslabují. Řídicí systémy mají algoritmy, které udělují příkazy a spouštějí některé operace. Řídicí systém zajišťuje, že určené fyzikální veličiny se udržují na předem určených hodnotách. V procesu regulace mění řídicí systém působením na akční veličiny stav řízeného systému tak, aby bylo dosaženo žádaného stavu.

U řídicího systému se dle recentních pojetí, které klade nejvyšší důraz na bezpečnost se v prioritním pořadí sledují vlastnosti jako:

- bezpečnost (úroveň dodržování stanovených podmínek provozu a nevytváření škodlivých (nepřijatelných) dopadů na samotný systém a na jeho okolí),
- funkčnost (úroveň plnění požadovaných úkonů),
- provozuschopnost (úroveň plnění požadovaných úkonů v závislosti na podmínkách normálních, abnormálních a kritických),
- provozní stálost (úroveň dodržování stanovených podmínek provozu v čase),
- inherentně zabudovaná odolnost vůči možným pohromám.

Řízeným systémem je většinou složitý nelineární systém, který:

- je tvořen konečným počtem prvků,
- každý z prvků je jednoznačně popsán konečným počtem měřitelných veličin,
- vzájemné vazby mezi prvky jsou jednoznačně formulovány.

Dynamické vlastnosti řízeného systému můžeme popsat pomocí diferenciálních rovnic, jejichž řešením je stavový vektor. Stavový vektor umožňuje pomocí minimálního počtu veličin určit stav systému v libovolném časovém okamžiku [32].

Pokud není možné kompletně eliminovat zdroj rizika, což platí např. pro živelní pohromy, je dalším nejlepším výběrem ochrana před dopady spojenými s realizací rizika, a to minimalizováním výskytu velkých očekávaných dopadů rizika způsobem, že se příslušná bezpečnostní ochranná opatření (bezpečnostní systémy – Safety Systems) přímo zabudují jak do projektu zařízení, tak i do podmínek provozu projektovaného zařízení, tj. zajistí se bezpečnost. Dalšími v akceptovatelném pořádku priorit jsou zařízení na zvládnutí nebezpečí a na zmírnění jejich dopadů (systémy spojené s bezpečností – Safety Related Systems), které mají jen ochranné funkce. Jsou to např. pojistné

ventily, které chrání před nedovoleným přetlakem v případech, ve kterých se nedovolenému zvýšenému tlaku v zařízení nedá úplně zabránit [1,2,32].

Bezpečnostní systémy jsou konstruované jako pasivní anebo aktivní [1,2,32]. Nejefektivnějšími bezpečnostními zařízeními jsou zařízení pasivní, která fungují na bázi fyzikálních principů (např. gravitace) a pro uvedení do činnosti nepotřebují žádný přidaný impuls. Příkladem pasivního bezpečnostního systému je železniční semafor, jehož rameno automaticky spadne do polohy „stop“ vždy, když se přeruší ovládací proud v přívodním kabelu.

Aktivní bezpečnostní zařízení / systémy jsou méně vhodné, protože pro jejich aktivaci pro zabránění havárie anebo zmírnění jejich dopadů jsou potřebné zvláštní iniciační impulsy. Jejich vytvoření zahrnuje detekci nebezpečí a rozpoznání odpovídající bezpečnostní procedury. Příkladem aktivního bezpečnostního systému může být detektor kouře propojený se sprchovým systémem.

Současné technické poznání dovoluje používat hybridní bezpečnostní systémy, které se samostatně vypínají, když existující podmínky nejsou v rozsahu podmínek stanovených pro provoz aktivních systémů; příkladem jsou ochrany důležitých objektů před velkými zemětřeseními známé z Japonska, Nového Zélandu a z dalších seismicky aktivních oblastí [1,2,32].

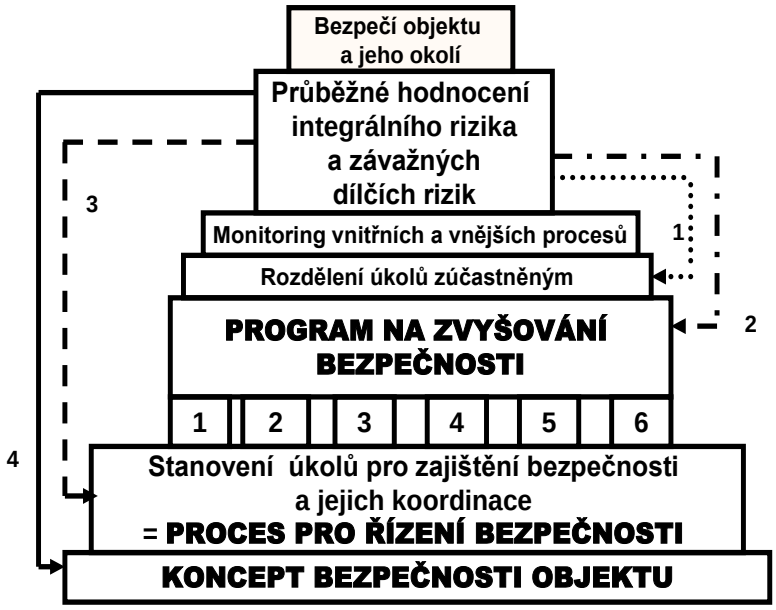
Protože svět se dynamicky vyvíjí, tak mohou nastat podmínky, na které nejsou limity zařízení připraveny, a proto systémy řízení bezpečnosti (i systémy řízení zabezpečení) musí být vždy vybaveny opatřeními pro minimalizování škod v případech, že bezpečnostní opatření a bezpečnostní systémy selžou, anebo se vyskytne neidentifikované nebezpečí. Minimalizování škod může mít podobu varovné a výstražné signalizace, výcviku obsluhy, pokynů a procedur pro chování v nebezpečných situacích, nebo izolace nebezpečných zařízení od osídlených center. Opatření před nehodami včetně nouzového plánování musí být vypracováno ještě před tím, než je zařízení spuštěno do provozu. Při vzniku havárie by už na to nemuselo být dosti času [1,2,32,38,39].

Správné porozumění určité problémové oblasti vyžaduje pochopení její historie, vědeckého základu, kulturního a sociálního prostředí, ve kterém byla vyvinutá a ve kterém se využívá. Systém řízení bezpečnosti má svoje kořeny v inženýrství průmyslové bezpečnosti, která se krok za krokem rozvíjí už od 19. století. Relativně nová disciplína zabývající se systémem řízení bezpečnosti (nebo v českém inženýrském slangu systémovou bezpečností) je odpovědí na podmínky, které vznikly po 2. světové válce, když se vyvinuly její “rodičovské“ disciplíny, a to systémové inženýrství a systémová analýza, které se vyvinuly pro řešení nových a komplexních inženýrských problémů. Vědecká báze všech těchto nových proudů inženýrství spočívá v teorii systémů, jejíž vývoj začal v třicátých letech minulého století [40].

Jde o novou oblast. Protože nejvíce problémů v poslední době ve světě i v ČR je v oblasti železniční dopravy (velké havárie spojené se ztrátami na lidských životech, velkými ekonomickými škodami a značnými újmami na životním prostředí), tak jsme se jako autoři publikace soustředili na železniční dopravu; např. Drážní inspekce po každé dopravní nehodě, ve které došlo ke srážce vlaků, ve své zprávě obvykle uvádí, že je třeba zlepšit zabezpečovací systém [41].

Úkolem systému řízení bezpečnosti (SMS) či systému řízení zabezpečení socio-kyberfyzického objektu je zvyšovat bezpečnost objektu, anebo ji alespoň udržovat na stanovené úrovni [2]. Jeho prioritami během provozu jsou: eliminovat zdroje nebezpečí; redukovat (omezit) možné dopady, tj. možná nebezpečí pro chráněná aktiva;

zvládnout realizaci rizik; a lokalizovat a zmírňovat škody. Model je zobrazen na obrázku 2, detailně popsaného [2].



Obr. 2. Model řízení bezpečnosti komplexního kritického objektu v čase [1]. Procesy: 1- koncepce a řízení; 2 - administrativní postupy;3 - technické procesy; 4 - vnější spolupráce; 5 - nouzová připravenost; a 6 - dokumentace a šetření havárií. Zpětné vazby: 1-4 [1].

V případě poloautomatického a automatického řízení je hlavní částí systému řízení bezpečnosti (SMS) či systému řízení zabezpečení socio-kyber-fyzického objektu propojený informační a řídící systém (Information and Control System - I&C) [1]. Jestliže zvážíme fakta:

1. Pro dosažení požadované úrovně bezpečnosti je třeba dobře řídit a správně rozhodovat.
2. Dobré / správné řízení a správné rozhodování je možné jen tehdy, když máme dobrá data a umíme využít nástroje, které máme k dispozici. Data musí být: správná, tj. je známa jejich velikost a přesnost; a musí mít vypovídací schopnost pro řešený problém, tj. musí být validovaná [42]. Datové soubory musí být reprezentativní, tj.: úplné; obsahovat správná data; mít dostatečný počet dat; data musí být rozprostřena homogenně v celém sledovaném intervalu a musí být validovaná. Při aplikaci modelů musí být správně zváženy nejistoty a neurčitosti v datech [42].
3. V reálném světě při zajišťování bezpečnosti složitých socio-kyber-fyzických systémů řešíme netriviální problémy, tj.: je více chráněných aktiv, jejichž cíle jsou v řadě případů konfliktní; aktiva se mění v čase a prostoru; a prostředí, ve kterém jsou aktiva, se dynamický vyvíjí.
4. Koordinace procesů na zajištění bezpečného objektu musí respektovat podmínky normální, abnormální a kritické. Jde o řízený proces, jehož cílem je vytvořit a provozovat technické dílo v potřebné kvalitě; sleduje procesy v prostoru, čase, personálu, materiálu, financích i dokumentech

Tak kvalita systémů I &C závisí na kvalitě chování kritických rozhraní v socio-kyber-fyzickém objektu za různých podmínek; a to zejména těch, které jsou spojeny náhlými velkými dynamickými změnami buď v socio-kyber-fyzickém (technickém) objektu, nebo v jeho okolí. Jde o sběr kvalitních údajů při monitorování (správné rychlé informace) a o kvalitu pravidel pro rozhodování, které jsou zahrnuty v systému I &C.

Způsob řízení bezpečnosti (SMS) socio-kyber-fyzických systémů se opírá o koncepci prevence pohrom či alespoň jejich závažných dopadů, která zahrnuje povinnost zavést a udržovat systém řízení, ve kterém jsou zohledněny dále uvedené problémy:

1. Role a odpovědnosti osob podílejících se na řízení závažných nebezpečí, která jsou spojená s možnými pohromami na všech organizačních úrovních kritického objektu a opatření na zajištění výcviku personálu, která jsou sladěna s identifikovanými potřebami výcviku.
2. Plány pro systematické identifikování závažných nebezpečí spojených s možnými pohromami a z nich plynoucích rizik, která jsou spojena s normálními a abnormálními podmínkami, a pro hodnocení jejich pravděpodobnosti a krutosti (velikosti).
3. Plány a postupy pro zajištění bezpečnosti všech komponent, systémů a funkcí v kritickém objektu a v jeho okolí, a to včetně údržby objektů, zařízení.
4. Plány na implementaci změn v kritickém objektu a v objektech i zařízeních, které jsou v okolí.
5. Plány na identifikaci předvídatelných nouzových situací systematickou analýzou, včetně přípravy, testů a posuzování nouzových plánů pro odezvu na možné nouzové situace.
6. Plány pro průběžné hodnocení souladu s cíli uvedenými v koncepci bezpečnosti a zabudovanými v SMS, a účinné mechanismy pro vyšetřování a provádění korekčních činností v případě selhání s cílem dosáhnout stanovené cíle.
7. Plány na periodické systematické hodnocení koncepce bezpečnosti, účinnosti a vhodnosti SMS a kritéria pro posuzování úrovně bezpečnosti vrcholovým týmem pracovníků kritického objektu.

Z výše uvedeného vyplývá, že u všech systémů řízení hraje velkou roli propojený systém I &C, ve kterém hrají velkou roli kvalita toku informací a kvalita instrukce pro provedení technické operace. Proto se na ně soustřeďuje pozornost u objektů, které jsou řízeny poloautomaticky a automaticky.

4. DATA O SELHÁNÍ SYSTÉMŮ ŘÍZENÍ DOPRAVY

Z důvodu zaměření předmětné práce nejprve uvedeme příklady selhání systémů řízení v dopravě, a pak se budeme věnovat problematice I&C u poloautomatických a automatických systémů řízení.

4.1. Příklady selhání systémů řízení železniční dopravy

Na základě dat [43] byly sledovány v ČR příčiny dopravních nehod vlaků spojené s lidským faktorem a formou zabezpečení. Výsledky jsou uvedeny v tabulce 3.

Tabulka 3. Příčiny dopravních nehod na nádražích v ČR.

Čas	Místo	Událost	Bezprostřední příčina
2013-02-04	Adamov, 2. traťová kolej	neodůvodněná a nezamýšlená jízda vlaku EC 278 na přivolávací návěst na kolej obsazenou vlakem Os 4012.	***Chyba řízení dopravy - nezrušení přivolávací návěsti na vjezdovém návěstidle 2L*** po obsazení kolejového obvodu KO 2Lk vlakem Os 4012, které bylo indikováno na monitoru ZZ.
2011-12-05	Baška, hlavní odjezdové návěstidlo S1	Nedovolená jízda vlaku Os 3127 kolem hlavního (odjezdového) návěstidla S1 do postavené vlakové cesty protijedoucího vlaku Os 3150 v železniční stanici Baška	***Chyba strojvedoucího - nerespektování návěsti „Stůj"*** hlavního (odjezdového) návěstidla S1 žst. Baška vlakem Os 3127.
2018-01-17	Beroun, staniční kolej 2a	nedovolená jízda vlaku Služ 269294 za úroveň cestového návěstidla Lc2a v poloze „Stůj", násilné přestavení výhybky č. 15b a vjetí na 3. staniční kolej obsazenou vlakem Os 7716.	***Chyba strojvedoucího - nerespektování návěsti „Stůj"*** cestového návěstidla Lc2a železniční stanice Beroun strojvedoucím vlaku Služ 269294.
2017-08-31	Bludov, staniční kolej č. 90	nedovolená jízda vlaku Mn 81300 za hlavní (odjezdové) návěstidlo S90P železniční stanice Bludov, které návěstidlo návěst „Stůj", s následným vykolejením hnacího drážního vozidla.	***Chyba strojvedoucího - nerespektování návěsti „Stůj"*** hlavního (odjezdového) návěstidla S90P železniční stanice Bludov osobou řídící hnací drážní vozidlo vlaku Mn 81300.

2017-07-05	Brandýs nad Orlicí, staniční kolej 2a	nedovolená jízda vlaku Nex 60104 za vjezdové návěstidlo 2L s návěstí „Stůj“ a směrem na kolej, ze které ve stejném směru jízdy odjížděl vlak Os 5010.	***Chyba strojvedoucího - nerespektování návěsti „Stůj”*** hlavního (vjezdového) návěstidla 2L do železniční stanice Brandýs nad Orlicí strojvedoucím vlaku Nex 60104.
2016-06-25	Brno hlavní nádraží, staniční kolej č. 4a	nedovolená jízda taženého posunového dílu za seřaďovací návěstidlo Se69 zakazující jízdu, následná srážka s protijedoucím posunujícím samostatným hnacím drážním vozidlem a vykolejení hnacího drážního vozidla taženého posunového dílu po srážce.	***Chyba strojvedoucího - nezastavení taženého posunového dílu před návěstí „Posun zakázán“*** seřaďovacího návěstidla Se69.
2014-03-07	Brno hlavní nádraží, výhybka č. 140	vykolejení řídicího vozu jedoucího v čele vlaku Os 4421 v železniční stanici Brno hlavní nádraží.	***Chyba řízení dopravy - nesprávně postavená cesta*** umožnění jízdy vlaku přes výhybku, ve které ani jeden jazyk nedoléhal k opornici (tzv. „vidlicová jízda“).
2017-12-04	Bylnice, vjezdové návěstidlo BS	nedovolená jízda vlaku Os 23213 za návěstidlo BS s návěstí zakazující jízdu, srážka s posunovým dílem a následným vykolejením vlaku jednou nápravou.	***Chyba strojvedoucího - nerespektování návěsti „Stůj”*** hlavního (vjezdového) návěstidla BS do železniční stanice Bylnice strojvedoucím vlaku Os 23213.
2014-07-08	Česká Třebová Parník, 4. traťová kolej	srážka vlaku Pn 148231 s nákladním vlakem Pn 63710 a následné vykolejení (důsledek projetí návěstidla v poloze „STŮJ“).	***Chyba strojvedoucího - nerespektování návěsti „Stůj”*** hlavního vjezdového návěstidla LV Odb. Parník osobou řídící drážní vozidlo vlaku Pn 148231.
2017-06-10	Český Brod, staniční kolej č. 2	Posunový díl (montážní vůz trakčního vedení) přijížděl po vyloučené 2. staniční koleji od žst. Úvaly k výhybce č. 45 žst. Český Brod, jel odbočným směrem a vjel do provozované 0. staniční koleje, čímž ohrozil postavenou vlakovou	***Chyba řízení dopravy - nesprávně postavená cesta*** - nezamýšlená jízda montážního vozu trakčního vedení přes výhybku č. 45 přestavenou do nesprávného (odbočného) směru.

		cestu protijedoucího vlaku Os 9320.	
2017-06-12	Český Brod, odjezdové návěstidlo L5	nezajištěná jízda vlaku Os 8610 na Přivolávací návěst směrem na traťovou kolej obsazenou vlakem Ex 1359.	***Chyba řízení dopravy - nesprávně postavená cesta*** - odjezd vlaku Os 8610 na Přivolávací návěst po výpravčím nesprávně postavené vlakové cestě směrem na 1. traťovou kolej, kde již stál vlak Ex 1359.
2014-02-13	Děčín, 1. traťová kolej	srážka vlaku Nex 48397 najetím na stojící nákladní vlak Nex 48325.	***Chyba strojvedoucího -nerespektování návěsti „Stůj" -*** nedovolená jízda vlaku Nex 48397 kolem oddílového návěstidla automatického bloku AB 1-26 s návěstí „Stůj".
2017-04-09	Děčín Dolní Žleb, 2. traťová kolej	srážka vlaků Pn 48378 a Lv 43398.	***Chyba strojvedoucího - nerespektování návěsti „Stůj" při nočním řízení podle rozhledových podmínek -*** neřízení hnacího drážního vozidla, vlaku Lv 43398, při jízdě za hlavní (oddílové) návěstidlo automatického bloku 2-81, které návěstidlo návěst „Stůj", za podmínek jízdy podle rozhledových poměrů; překročení nejvyšší dovolené rychlosti o 30 km·h-1.
2014-06-19	Dolní Beřkovice, vjezdové návěstidlo 1S	nezajištěný odjezd vlaku Mn 160780 ze žst. Dolní Beřkovice po posunové cestě bez provedených úkonů k výpravě vlaku a bez uděleného traťového souhlasu na první traťovou R 603. kolej mezistaničního úseku mezi žst. Dolní Beřkovice a žst. Hněvice na dráze železniční, celostátní, na kterou vjel v opačném směru ze žst. Hněvice vlak	***Chyba strojvedoucího - neodsouhlasená jízda vlaku*** - nezajištěná jízda vlaku Mn 160780 ze žst. Dolní Beřkovice na 1. traťovou kolej v mezistaničním úseku žst. Hněvice – žst. Dolní Beřkovice bez traťového souhlasu a bez provedených úkonů k výpravě vlaku.
2015-08-04	Horažďovice předměstí,	srážka vlaku R 668 s vlakem R 667 s následným vykolejením (důsledek nezajištěné jízdy vlaku R 668 – předčasné zrušení	***Chyba řízení dopravy - nesprávně postavená cesta*** - přestavení výhybky č. 28X signalistou St. 2, v době, kdy se na této výhybce nacházela DV vlaku R 668, a následná jízda zadní části vlaku

	pačejovské zhlaví	vlakové cesty pro tento vlak).	R 668 po jiné koleji, než byla pro jízdu tohoto vlaku určena.
2018-02-15	Praha-Horní Počernice, vjezdové návěstidlo S	vjezd vlaku Os 5815 na 2. staniční kolej žst. Praha-Horní Počernice proti odjíždějícímu vlaku Os 5810.	***Chyba řízení dopravy - nesprávně postavená cesta*** - jízda vjíždějícího vlaku Os 5815 na jinou kolej, než pro něj byla určena, proti současně odjíždějícímu vlaku Os 5810.
2012-06-05	Hořovice, 2b. staniční kolej	nedovolená jízda vlaku R 824 kolem hlavního (odjezdového) návěstidla L2b a vjezd na 2. traťovou kolej do obsazeného mezistaničního oddílu vlakem Os 7822.	***Chyba strojvedoucího - neodsouhlasená jízda vlaku*** - nedovolená jízda vlaku R 824 kolem zneplatněného hlavního (odjezdového) návěstidla L2b, o jehož zneplatnění nebyl strojvedoucí písemně zpraven a pro pokračování v jízdě si nevyžádal souhlas osoby organizující a řídící drážní dopravu.
2017-03-01	Hradec Králové hl. n., srdcovce výhybky č. 100XB	nedovolená jízda posunového dílu za úroveň návěstidla L6 zakazujícího jízdu, srážka s protijedoucím vlakem Mn 83044, zpětné odražení a vykolejení posunového dílu.	***Chyba strojvedoucího - nerespektování návěsti „Stůj“*** odjezdového návěstidla L6 žst. Hradec Králové hl. n. strojvedoucím posunového dílu.
2018-11-20	Chotěbuz, km 320,914	nedovolená jízda vlaku Nex 49745 za úroveň hlavního (oddílového) návěstidla automatického bloku 1-3218 bez zastavení, které návěstidlo návěst „Stůj“, a následná srážka s koncem vlaku Nex 49735.	***Chyba strojvedoucího - nerespektování návěsti „Stůj“*** hlavního (oddílového) návěstidla automatického bloku 1-3218 traťové koleje č. 1 odbočka Chotěbuz – Český Těšín osobou řídící hnací drážní vozidlo vlaku Nex 49745.
2018-07-20	Chrást u Plzně, 2. traťová kolej	srážka – najetí vlaku Sv 21920 na konec vlaku Nex 61400.	nezastavení vlaku Sv 21920 před koncem vlaku Nex 61400 při jízdě podle rozhledových poměrů v obsazeném traťovém oddílu automatického bloku. ***Chyba řízení dopravy - noční řízení podle rozhledových poměrů***
2016-08-30	Chválkov, dopravna mezi 1. a 2.	nedovolená jízda vlaku MOs 203 za úroveň předního námezníku v dopravně Chválkov a následná srážka s	nevyčkání příjezdu vlaku MOs 204 a odjezd vlaku MOs 203 z dopravny Chválkov před příjezdem vlaku MOs 204 do této dopravny.

	staniční kolejí	protijedoucím vlakem MOs 204.	***Chyba strojvedoucího - neodsouhlasená jízda vlaku***
2017-03-31	Jihlava město, výhybka č. 34	nezamýšlený vjezd vlaku Pn 62145 na staniční kolej č. 13, obsazenou odstavenými drážními vozidly.	nepřestavení výhybky č. 34 do správné koncové polohy při přípravě vlakové cesty pro jízdu vlaku Pn 62145 na staniční kolej č. 5 vlivem přerušení celistvosti drátovodu k mechanickému přestavníku. ***Chyba řízení dopravy - nesprávně postavená cesta***
2010-12-20	Kamenné Žehrovice, 1. staniční kolej	srážka vlaku Os 19702 se stojícím posunovým dílem	dovolení vjezdu vlaku do dopravny s kolejovým rozvětvením na kolej obsazenou drážními vozidly bez zavedení dalších opatření. ***Chyba řízení dopravy - nesprávně postavená cesta***
2011-08-31	Kařízek, 2. traťová kolej	srážka osobního vlaku Os 7800 s nákladním vlakem Pn 64710 s následným vykolejením posledního vozu nákladního vlaku.	***Chyba strojvedoucího - nerespektování návěsti „Stůj“*** na oddílovém návěstidle AB 2-699 vlakem Os 7800, tj. nezastavení před tímto návěstidlem a nedodržení podmínek pro jízdu podle rozhledu.
2018-12-11	Karlovy Vary dolní nádraží, výhybka č. 23	srážka vlaku Os 7023 se stojícím vlakem Mn 87001 – najetí zezadu.	***Chyba řízení dopravy - nesprávně postavená cesta*** - zrušení vlakové cesty vlaku Mn 87001 výpravčí žst. Karlovy Vary dolní nádraží dříve, než byly uvolněny všechny výhybky a zadní námezník ve vlakové cestě;+ dovolení jízdy vlaku Os 7023 výpravčí žst. Karlovy Vary dolní nádraží, aniž byla jeho vlaková cesta volná
2013-01-22	Kolín, staniční kolej 1a	nedovolená jízda vlaku Os 8663 kolem hlavního (odjezdového) návěstidla S1a.	***Chyba strojvedoucího - nerespektování návěsti stůj*** - nezastavení vlaku Os 8663 před návěstí „Stůj“ hlavního (odjezdového) návěstidla S1a žst. Kolín; nerespektování předvěstěné návěsti „Stůj“ na návěstním opakovači vlakového zabezpečovače HDV vlaku Os 8663.
2014-07-27	Kolín, kolej č. 101b	nedovolená jízda vlaku R 851 kolem hlavního (cestového) návěstidla Sc101c zakazujícího jízdu, rozřez výhybky č.	***Chyba strojvedoucího - nerespektování návěsti „Stůj“*** hlavního (cestového) návěstidla Sc101c žst. Kolín vlakem R 851.

		196 a vjetí do postavené vlakové cesty pro vlak Os 9344 (důsledek selhání lidského faktoru).	
2017-12-15	Kolín, cestové návěstidlo Sc110b	nedovolená jízda posunového dílu za návěstidlo zakazující jízdu a vjetí do postavené vlakové cesty protijedoucího vlaku R 986.	***Chyba strojvedoucího - nezastavení před návěstí Posun zakázán -*** nerespektování návěsti zakazující posun na návěstidle Sc110b strojvedoucím posunového dílu.
2011-10-06	Kostomlaty nad Labem, km 324,779.	nedovolená jízda vlaku Vn 56071 za oddílové návěstidlo automatického bloku 1-3248 s návěstí „Stůj“ a následná srážka s vlakem Pn 66421.	***Chyba strojvedoucího - nerespektování návěsti stůj*** - nedovolená jízda vlaku Vn 56071 za oddílové návěstidlo automatického bloku s návěstí „Stůj“.
2017-11-02	Kostomlaty nad Labem, km 330,570.	srážka vlaku Pn 53973 s koncem vlaku Pn 66021 s následným vykolejením 1 vozu vlaku Pn 66021.	***Chyba řízení dopravy - noční řízení podle rozhledových poměrů -*** nezastavení vlaku Pn 53973 před koncem vlaku Pn 66021 při jízdě dle rozhledových poměrů v obsazeném traťovém oddílu automatického bloku.
2017-04-05	Kralupy nad Vltavou, staničníkolej č. 7	nedovolená jízda vlaku Nex 41363 za úroveň hlavního (cestového) návěstidla Sc7 v poloze „Stůj“ a následné vjetí do jízdní (vlakové) cesty postavené pro vlak Os 9770.	***Chyba strojvedoucího - nerespektování návěsti „Stůj”*** hlavního (cestového) návěstidla Sc7 železniční stanice Kralupy nad Vltavou osobou řídící drážní vozidlo vlaku Nex 41363.
2018-05-03	Křemže, hlavní (odjezdové) návěstidlo L1	nedovolená jízda vlaku Os 8102 za odjezdové návěstidlo L1 v žst. Křemže zakazující jízdu, násilné přestavení výhybky č. 6, vjetí do postavené vlakové cesty pro protijedoucí vlak Os 8103, následná srážka a vykolejení vlaku Os 8103.	***Chyba strojvedoucího - nerespektování návěsti „Stůj“*** hlavního (odjezdového) návěstidla L1 v železniční stanici Křemže osobou řídící drážní vozidlo – vlak Os 8102.
2013-05-02	Kunovice-Loučka, hlavní	nedovolená jízda vlaku Os 3915 kolem hlavního (odjezdového) návěstidla S1, po předchozím nedovoleném	***Chyba strojvedoucího - nerespektování návěsti „Stůj”*** hlavního (odjezdového) návěstidla S1 železniční stanice Kunovice-Loučka osobou řídící drážní vozidlo vlaku Os 3915.

	(odjezdové) návěstidlo S1	rozjezdu vlaku Os 3915 z prostoru pro výstup a nástup cestujících.	
2011-08-23	Praha-Libeň, návěstidlo Lc06	nedovolená jízda vlaku Os 9326 kolem hlavního (cestového) návěstidla Lc06 s návěstí „Stůj“ do postavené posunové cesty po předchozím nedovoleném odjezdu z prostoru pro výstup a nástup cestujících, s následnou srážkou s posunovým dílem v prostoru výhybky 34N, vykolejením dvou HDV, požáru HDV posunového dílu a ekologickou havárii.	***Chyba strojvedoucího - nerespektování návěsti „Stůj“*** hlavního (cestového) návěstidla Lc06 v žst. Praha-Libeň vlakem Os 9326.
2014-02-04	Lípa, 1. staniční kolej	odjezd vlaku Os 15966 z dopravny Lípa bez souhlasu dirigujícího dispečera a následná jízda do oddílu obsazeného vlakem Mn 82552.	***Chyba strojvedoucího - neodsouhlasená jízda vlaku*** - odjezd vlaku Os 15966 z dopravny Lípa bez svolení dirigujícího dispečera do oddílu obsazeného vlakem Mn 82552.
2017-10-11	Lipník nad Bečvou, staniční kolej č. 2	nedovolená jízda vlaku Lv 54204 za hlavní (odjezdové) návěstidlo S2 železniční stanice Lipník nad Bečvou a vjetí do postavené jízdní (vlakové) cesty protijedoucího vlaku Nex 54285.	***Chyba strojvedoucího - nerespektování návěsti „Stůj“*** hlavního (odjezdového) návěstidla S2 železniční stanice Lipník nad Bečvou osobou řídící hnací drážní vozidlo vlaku Lv 54204.
2015-07-14	Praha Masarykovo nádraží, 3. staniční kolej	nedovolená jízda vlaku Os 8616 za návěstidlo Lc3 zakazující jízdu, srážka se záchytným pražcem na 3. SK a vykolejení, srážka se zarážedlem a vjetí do prostoru pro cestující (důsledek selhání lidského faktoru).	***Chyba strojvedoucího - nerespektování návěsti stůj*** - nezastavení vlaku Os 8616 před návěstidlem Lc3 s návěstí „Stůj“.
2013-02-05	Mirošov, 1. staniční kolej	srážka vlaku Vleč 87892 s vlakem Os 27823.	***Chyba řízení dopravy - nesprávně postavená cesta*** - neprovedení zjištění volnosti vlakové cesty pro vlak Vleč 87892 výpravčím a

			následné vypravení vlaku Vleč 87892; + přestavení výměny výhybky č. 10 dozorkyní výhybek pro jízdu vlaku Vleč 87892, ačkoli výhybka byla obsazena vozidly vlaku Os 27823.
2011-10-22	Český Těšín – Polanka nad Odrou, odbočka Odra, hlavní vjezdové návěstidlo 2VL	nedovolená jízda vlaku Os 3428 za hlavní (vjezdové) návěstidlo 2VL odbočky Odra zakazující jízdu, s následnou srážkou předmětného vlaku s technickým zařízením dráhy a vykolejením všech drážních vozidel.	***Chyba strojvedoucího - nerespektování návěsti „Stůj”*** hlavního (vjezdového) návěstidla 2VL odb. Odra osobou řídící drážní vozidlo vlaku Os 3428.
2010-07-03	Olomouc hl. n., grygovské zhlaví, výhybka č. 9	srážka taženého posunového dílu s vlakem Rn 53033 v žst. Olomouc hl. n.	***Chyba strojvedoucího - nezastavení před návěstí Posun zakázán -*** nerespektování seřaďovacího návěstidla Se48 žst. Olomouc hl. n., s návěstí „Posun zakázán”, osobou řídící DV posunového dílu 1. posunové zálohy žst. Olomouc hl. n.
2009-02-16	Paskov, trať 302A, km 13,459	srážka vlaků osobní dopravy – osobních vlaků Os 3101 a Os 3116 mezi železničními stanicemi Vratimov a Paskov s následným vykolejením hnacího drážního vozidla vlaku Os 3101.	***Chyba strojvedoucího - nerespektování návěsti „Stůj”*** odjezdového návěstidla S1 železniční stanice Paskov osobou řídící drážní vozidlo vlaku Os 3101 s následnou nedovolenou jízdou vlaku Os 3101 do prostorového oddílu obsazeného protijedoucím vlakem Os 3116.
2012-03-31	Peruc (trať č. 529C) km 75,628	srážka posunu mezi dopravnami s uvázlým vlakem Os 9756.	***Chyba strojvedoucího - nesprávně postavená cesta*** - dovolení jízdy PMD do kilometru 75,500, který se ve směru jízdy PMD nacházel za uvázlým vlakem; + nedodržení technologických postupů pro bezpečné řízení HDV PMD vzhledem k dopravním a provozním podmínkám.
2014-11-11	Petrovice u Karviné, traťová kolej č. 1	srážka samostatného hnacího drážního vozidla jedoucího jako posun mezi dopravnami s uvázlým nákladním vlakem Pn 47850.	***Chyba strojvedoucího -*** nedovolená jízda posunu mezi dopravnami za kilometr širé trati (místa na trati), do kterého byl posun sjednán a pokynem provozovatele dráhy v písemném rozkaze stanoven a

			do něhož směl být dopravcem uskutečněn.
2014-12-30	Poříčany, 1. staniční kolej, odjezdové návěstidlo S1	nedovolená jízda vlaku Os 9329 kolem návěstidla S1 zakazujícího jízdu, vjetí do postavené vlakové cesty pro vlak R 983 s následnou srážkou drážních vozidel a vykolejením (důsledek selhání lidskéhočinitele).	***Chyba strojvedoucího - nerespektování návěsti stůj*** - absence technických prostředků zabezpečení v žst. Poříčany, které by při pochybení (omylu nebo selhání) strojvedoucího aktivním zásahem do řízení vlaku zabránily nedovolené jízdě vlaku za hlavní návěstidlo s návěstí zakazující jízdu vlaku; + nerespektování pokynů výpravčího daných při svolení k posunustrojvedoucím vlaku Os 9329.
2013-08-31	Postřelmov, hlavní (odjezdové) návěstidlo S1	nedovolená jízda vlaku R 1234 za hlavní (odjezdové) návěstidlo S1 zakazující jízdu vlaku v železniční stanici Postřelmov s jeho následnou jízdou do řádně postavené jízdní (vlakové) cesty protijedoucího vlaku Os 3714. Touto nedovolenou jízdou vlaku R 1234 byla násilně přestavena výhybka č. 1 a uskutečněna jízda přes železniční přejezd P 6655, který činností světelného přejezdového zabezpečovacího zařízení včas nevaroval uživatele pozemní komunikace, že se k železničnímu přejezdu blíží vlak.	***Chyba strojvedoucího - nerespektování návěsti „Stůj"*** hlavního (odjezdového) návěstidla S1 železniční stanice Postřelmov osobou řídící drážní vozidlo vlaku R 1234.
2012-03-29	Praha hlavní nádraží, kolej č. 26b, hlavní návěstidlo Lc26b	nedovolená jízda vlaku R 791 kolem hlavního návěstidla Lc26b s následným rozříznutím výhybky číslo 84 a jízdou proti stojícímu vlaku R 783.	***Chyba strojvedoucího - nerespektování návěsti „Stůj"*** hlavního (cestového) návěstidla Lc26b žst. Praha hl. nádraží strojvedoucím vlaku R 791.

2014-03-28	Praha hlavní nádraží, 11a staniční kolej, odjezdové návěstidlo S11a	nedovolená jízda vlaku Os 8830 za úroveň odjezdového návěstidla S11a zakazující jízdu vlaku v železniční stanici Praha hl. n. (důsledek selhání lidského faktoru).	***Chyba strojvedoucího - nerespektování návěsti „Stůj“*** hlavního odjezdového návěstidla S11a železniční stanice Praha hlavní nádraží osobou řídící drážní vozidlo vlaku Os 8830.
2017-12-15	Praha hl. n., kolej č. 13a, návěstidlo s návěstí „Konec vlakové cesty“	nedovolená jízda vlaku Os 25907 za návěstidlo s návěstí „Konec vlakové cesty“, srážka se zarážedlem a zpětný odraz soupravy.	***Chyba strojvedoucího - nerespektování návěsti „Stůj“*** návěstěné hlavním (cestovým) návěstidlem Lc13a železniční stanice Praha hl. n. strojvedoucím vlaku Os 25907 a nedovolená jízda za návěstidlo s návěstí „Konec vlakové cesty“.
2017-08-02	Praha hlavní nádraží, seřaďovací návěstidlo Se20	nedovolená jízda posunového dílu kolem návěstidla Se20 v poloze zakazující jízdu a následné vjetí do postavené vlakové cesty vlaku Os 25921.	***Chyba strojvedoucího - nerespektování návěsti Posun zakázán***
2018-05-27	Praha-Vršovice seřaďovací nádraží, odjezdové návěstidlo L1	nedovolená jízda sunutého posunového dílu za odjezdové návěstidlo L1 zakazující další jízdu v železniční stanici Praha-Vršovice seřaďovací nádraží a vjetí do postavené vlakové cesty vlaku Sv 29977.	***Chyba strojvedoucího - nerespektování návěsti „Stůj”*** hlavního (odjezdového) návěstidla L1 v železniční stanici Praha-Vršovice seřaďovací nádraží, stavědlo Odjezd, posunovačem v čele sunutého posunového dílu.
2017-06-05	Přerov – obvod osobní nádraží, staniční kolej č. 5, hlavní (cestové) návěstidlo Sc5	nedovolená jízda vlaku Ex 1342 za úroveň hlavního (cestového) návěstidla Sc5 žst. Přerov, které návěstilo návěst „Stůj“ a následná srážka s betonovým zarážedlem na konci staniční koleje č. 5.	***Chyba strojvedoucího - nerespektování návěsti „Stůj“*** návěstěné hlavním (cestovým) návěstidlem Sc5 železniční stanice Přerov osobou řídící drážní vozidlo vlaku Ex 1342.

2018-02-28	Praha Radotín, návěstidlo Se42	nedovolená jízda sunutého posunového dílu dopravce Českomoravský cement, a.s., za návěstidlo Se42 s návěstí zakazující jízdu, srážka se zádržným pražcem a zarážedlem kusé odvratné koleje, následné vykolejení 2 nákladních vozů a jejich pád do prostoru podchodu pro pěší.	***Chyba strojvedoucího - nerespektování návěsti Posun zakázán*** seřaďovacího návěstidla Se42 vedoucím posunu předmětného sunutého posunového dílu.
2015-10-30	Řehlovice, 2. staniční kolej, odjezdové návěstidlo L2	nedovolená jízda vlaku Nex 163602 kolem odjezdového návěstidla L2 žst. Řehlovice v poloze zakazující jízdu a následná srážka s vlakem Pn 59040 a vykolejení 4 vozů tohoto vlaku.	***Chyba strojvedoucího - nerespektování návěsti stůj*** - nedovolená jízda vlaku Nex 163602 za odjezdové návěstidlo L2 s návěstí „Stůj“ v žst. Řehlovice.
2016-07-10	Rotava, návěst „Místo zastavení“	nedovolená jízda vlaku Os 17016 za úroveň návěsti „Místo zastavení“ a následná srážka s protijedoucím vlakem Os 17007.	***Chyba strojvedoucího - neodsouhlasená jízda vlaku*** - nevyčkání příjezdu vlaku Os 17007 a odjezd vlaku Os 17016 z dopravny Rotava bez souhlasu osoby řídící drážní dopravu (dirigujícího dispečera).
2013-03-27	Roztoky u Prahy, staniční kolej č. 3a, hlavní odjezdové návěstidlo S3a	nedovolená jízda vlaku Os 12149 kolem hlavního odjezdového návěstidla S3a s následným rozříznutím výhybky číslo 6 a jízdou do postavené vlakové cesty pro vlak EC 379.	***Chyba strojvedoucího - nerespektování návěsti stůj*** - nezastavení vlaku Os 12149 před návěstí „Stůj“ hlavního odjezdového návěstidla S3a žst. Roztoky u Prahy; + nerespektování předvěstné návěsti „Stůj“ na návěstním opakovači vlakového zabezpečovače HDV vlaku Os 12149.
2018-08-17	dopravna D3 Rýmařov, výhybka č. 8	nezajištěná jízda vlaku Mn 81013 při odjezdu z dopravny D3 Rýmařov a následné vykolejení taženého drážního vozidla, řazeného na konci vlaku.	***Chyba řízení dopravy - nesprávně postavená cesta*** jízda vlaku Mn 81013 přes výhybku č. 8 v dopravně D3 Rýmařov, která nebyla v době odjezdu vlaku správně přestavena.
2018-03-22	Šlapanice, staniční kolej č. 2	nedovolená jízda vlaku Pn 62171 kolem návěstidla S2 zakazujícího jízdu, následný rozřez výhybky č. 3 a jízda po 2.	***Chyba strojvedoucího - nerespektování návěsti „Stůj”*** hlavního (odjezdového) návěstidla S2 v železniční stanici Šlapanice strojvedoucím vlaku Pn 62171.

		traťové koleji ve směru do žst. Blažovice proti vlaku Os 4140.	
2011-09-12	Slatiňany, manipulační kolej č. 7, výkolejka Vk3	při jízdě sunutého posunového dílu došlo k vykolejení prvních dvou DV přes výkolejku v poloze na kolejnici, pojížděnou proti směru určenému k její funkci, a k následnému pádu člena ONV, jedoucího na zadní stupačce prvního sunutého DV, pod druhé vykolejené DV.	***Chyba řízení dopravy - nesprávně postavená cesta*** - udělení souhlasu k posunu bez předchozího správného postavení posunové cesty.
2018-09-21	Štěpánov, traťové koleje č. 1, hlavní vjezdové návěstidlo 1S,	nedovolená jízda vlaku R 883 za úroveň hlavního (vjezdového)návěstidla 1S železniční stanice Štěpánov, které návěstilo návěst „Stůj“, s následným vjetím na staniční kolej obsazenou vlakem Pn 57039.	***Chyba strojvedoucího - nerespektování návěsti stůj*** - nezjištění návěsti „Stůj” hlavního (vjezdového) návěstidla 1S železniční stanice Štěpánov osobou řídící drážní vozidlo vlaku R 883.
2013-01-30	Strančice, kolej č. 1, hlavní odjezdové návěstidlo L1	nedovolená jízda vlaku Os 9104 kolem hlavního odjezdového návěstidla L1 s následnou jízdou na 1. traťovou kolej proti jedoucímu vlaku Os 2509.	***Chyba strojvedoucího - nerespektování návěsti stůj*** - nezastavení vlaku Os 9104 před návěstí „Stůj“ hlavního odjezdového návěstidla L1 žst. Strančice;
2018-10-23	Studenec, vjezdové návěstidlo „S“	nedovolená jízda vlaku Os 4807 kolem návěstidla „S“ zakazujícího jízdu, následné projetí železničního přejezdu P3849 v km 36,096 v otevřené poloze a vjetí na 1. staniční kolej obsazenou vlakem Os 4806.	***Chyba strojvedoucího - nerespektování návěsti „Stůj“*** hlavního (vjezdového) návěstidla „S“ železniční stanice Studenec strojvedoucím vlaku Os 4807.
2018-07-18	Svor, vjezdové návěstidlo S	nezajištěná jízda vlaku R 1101 na 1. staniční kolej obsazenou vlakem Os 6000.	***Chyba řízení dopravy -*** dovolení vjezdu vlaku R 1101 po vlakové cestě nezamýšleně postavené na 1. staniční kolej obsazenou vlakem Os 6000.

2017-04-04	Ústí nad Labem hlavní nádraží, seřaďovací návěstidlo Se224	nedovolená jízda sunutého posunového dílu za seřaďovací návěstidlo Se224 s návěstí „Posun zakázán“, násilné přestavení výhybky č. 239, vjetí do postavené posunové cesty taženému posunovému dílu, následná srážka a vykolejení.	***Chyba strojvedoucího - nezastavení před návěstí Posun zakázán -*** nedovolená jízda sunutého posunového dílu dopravce METRANS, a. s., za seřaďovací návěstidlo Se224 s návěstí „Posun zakázán“ a vjetí do postavené posunové cesty taženému posunovému dílu dopravce IDS CARGO a. s.
2018-05-28	Ústí nad Labem hlavní nádraží, staniční kolej č. 1, hlavní (cestové) návěstidlo Sc1	nedovolená jízda vlaku Nex 43333 za úroveň hlavního (cestového) návěstidla Sc1 v poloze „Stůj“ a následné vjetí do jízdní (vlakové) cesty postavené pro vlak Os 6905.	***Chyba strojvedoucího - nerespektování návěsti „Stůj”*** hlavního (cestového) návěstidla Sc1 železniční stanice Ústí nad Labem hlavní nádraží osobou řídící drážní vozidlo vlaku Nex 43333.
2015-03-28	Velké Žernoseky, 1. traťová kolej, km 411,153.	nedovolená jízda vlaku Nex 148359 za úroveň návěstidla zakazujícího jízdu, následná srážka s protijedoucím vlakem Pn 53668 a vykolejení.	***Chyba strojvedoucího - nerespektování návěsti stůj -*** nedovolená jízda vlaku Nex 148359 do mezistaničního úseku mezi žst. Velké Žernoseky a žst. Litoměřice dolní nádraží, který byl obsazen protijedoucím vlakem Pn 53668.
2018-07-01	Veselí nad Moravou, odjezdové návěstidlo L1	nezajištěná jízda vlaku Sp 1724 po chybně postavené vlakové cestě na 1. traťovou kolej obsazenou protijedoucím vlakem Sp 1721.	***Chyba řízení dopravy - chybně postavená vlaková cesta*** pro vlak Sp 1724.
2011-02-02	dopravnou Vodňany	Srážka vlaků Os 18003 a Mn 88850 s následným vykolejením vlaku Os 18003.	***Chyba řízení dopravy a chyba strojvedoucího -*** 1.Nesprávné požádání dirigujícího dispečera strojvedoucím vlaku Os 18003 již v dopravně Bavorov o svolení k odjezdu až do přilehlé žst. Čížčenice, přestože měl stanovenou ohlašovací povinnost ještě v mezilehlé dopravně Vodňany. 2. Nesplnění ohlašovací povinnosti strojvedoucího vlaku Os 18003 v dopravně Vodňany, který po příjezdu do ní nepožádal dirigujícího dispečera o souhlas k odjezdu do žst. Čížčenice a s

			vlakem Os 18003 nedovoleně odjel, aniž by vyčkal příjezdu protijedoucího vlaku Mn 88850. 3. Svolení dirigujícího dispečera žst. Prachatice strojvedoucímu vlaku Os 18003 k jízdě z dopravny Bavorov až do žst. Číčenice. 4. Souhlas dirigujícího dispečera žst. Prachatice výpravčímu žst. Číčenice k jízdě vlaku Mn 88850 z Číčenic do Vodňan.
2013-08-02	dopravna Vodňany, výhybka č. 2Sv	vykolejení vlaku Os 18008 na výhybce č. 2Sv se samovratným přestavníkem na dráze železniční, regionální, v dopravně Vodňany.	***Chyba strojvedoucího - neodsouhlasená jízda vlaku*** - nerespektování pokynu provozovatele dráhy dávaného návěstidlem Sv2 strojvedoucímu vlaku před vjezdem na výhybku č. 2Sv.
2014-09-17	Vyšehrad, výhybka č. 12	srážka vlaku R 965 se stojícím posunovým dílem, následně vykolejení hnacího drážního vozidla vlaku R 965 a dvou posledních vozů posunového dílu.	***Chyba řízení dopravy - nesprávně postavená cesta -*** jízda vlaku R 965 po postavené vlakové cestě ze 2. koleje od žst. Praha-Smíchov na 3. staniční kolej přes výhybku č. 12, obsazenou posunovým dílem.
2013-01-13	dopravna Vysoké Mýto, výhybka č. 1	vykolejení vlaku Os 15066 na výhybce se samovratným přestavníkem při vjezdu do dopravny.	***Chyba strojvedoucího - neodsouhlasená jízda vlaku -*** nerespektování pokynu provozovatele dráhy dávaného návěstidlem Sv1 strojvedoucímu vlaku před vjezdem na výhybku č. 1.
2011-04-10	Praha-Žižkov, první kolej, km 3,331	srážka drážních vozidel při nedovolené jízdě s následným vykolejením.	***Chyba strojvedoucího - neodsouhlasená jízda vlaku -*** nedovolená jízda DV za km 3,3, do kterého byla jejich jízda povolena jako PMD; nepřestavení a neuzamčení výhybek pro jízdu na druhou kolej v nákladišti Praha-Žižkov před odjezdem předchozího PMD do žst. Praha-Malešice.
2007-07-14	Čerčany, na 1. staniční koleji	se vlak R 633 srazil s odstavenou soupravou vlaku Os 9122.	***Chyba řízení dopravy - nesprávně postavená cesta -*** dovolení vjezdu vlaku R 633 na 1. staniční kolej železniční stanice Čerčany a odjezdu z ní, při obsazení vlakové cesty pro tento vlak jinými drážními vozidly, a nedodržení podmínek jízdy podle rozhledových poměrů.

2007-06-20	dopravně Černý Kříž	Vlak osobní dopravy Os 18544 se srazil s posunovým dílem obsazeným cestujícími.	***Chyba strojvedoucího - neodsouhlasená jízda vlaku -*** zahájení posunu bezprostředně po odjezdu vlaku Os 18544, který ještě neminul lichoběžníkovou tabulku, a to bez souhlasu odborně způsobilé osoby, která řídí jízdu vlaků, tj. dirigujícího dispečera.
2007-06-21	Chotoviny	vjezdu vlaku R 641, jedoucím z Prahy do Českých Budějovic, na obsazenou 1. staniční kolej vlakem R 644 bez následků. Vlak R 641 zastavil 140 m před čelem vlaku R 644.	***Chyba řízení dopravy - nesprávně postavená cesta -*** jízdy vlaku R 641 na kolej obsazenou vlakem R 644.
2007-02-09	Káranice, na dobřenickém zhlaví	vlak R 957 nezastavil před odjezdovým návěstidlem S1 s návěstí Stůj a následně se bočně srazil s vlakem Pn 63440, který vjížděl na 3. staniční kolej.	***Chyba strojvedoucího - nerespektování návěsti stůj -*** neuposlechnutí pokynů provozovatele při řízení drážní dopravy a následná jízda vlaku R 957 za odjezdové návěstidlo S1 s návěstí Stůj.
2006-02-20	Kropáčova Vrutice v km 51,376	vlak R 940 vjel do boku vjíždějícího vlaku 1.nsl Pn 64439.	***Chyba strojvedoucího - nerespektování návěsti stůj***
2009-09-01	Horní Lipová	srážka posunu mezi dopravnami se stojícím, uvázlým vlakem Os 3613 v km 24,886	***Chyba strojvedoucího - neodsouhlasená jízda vlaku -*** nedovolená jízda posunu mezi dopravnami za kilometr povolené jízdy stanovené pokynem provozovatele dráhy v písemném všeobecném rozkaze pro posun mezi dopravnami.
2007-09-10	Praha-Modřany	jízdě vlaku Os 9009 do prostorového oddílu obsazeného vlakem Os 19010.	***Chyba řízení dopravy - nesprávně postavená cesta -*** dovolení jízdy vlaku Os 9009 ze žst. Praha-Braník do obsazeného prostorového oddílu vlakem Os 19010, bez zavedení dalších opatření.
2008-09-13	Mohelnice, traťová kolej č. 1, km 54,397	srážka vlaků nákladní dopravy – expresního nákladního vlaku (dále jen Nex) 54053 a průběžného nákladního vlaku (dále jen Pn) 66161 mezi železničními	***Chyba řízení dopravy - nesprávně postavená cesta -*** dovolení odjezdu vlaku Nex 54053 do prostorového oddílu obsazeného stojícím vlakem Pn 66161.

		stanicemi (dále jen žst.) Moravičany a Mohelnice.	
2008-05-19	Moravany, 1. staniční kolej, km 291,625	srážka vlaku Lv 72461 s osobním vlakem Os 5011 s následným vykolejením (důsledek selhání návěstních a zabezpečovacích systémů)	***Chyba zabezpečení - selhání návěstních a zabezpečovacích systémů -*** ztráta šuntu kolejového obvodu 1K žst. Moravany vlakem Os 5011, reakce staničního zabezpečovacího zařízení ESA 11 na neočekávanou změnu informace o volnosti 1. staniční koleje
2006-06-18	Nymburk hl. n.	najetí nákladního vlaku č. 64922 na hnací drážní vozidlo (dále jen HDV) 130.021-9, stojící na kusé koleji č. 105b.	***Chyba řízení dopravy - nesprávně postavená cesta -*** výprava vlaku č. 64922 bez splnění stanovených podmínek pro odjezd vlaku.
2009-10-16	Přerov, staniční kolej č. 402A, km 181,3384	Nedovolená jízda vlaku Rn 50238 za hlavní návěstidlo L104 s návěstí „Stůj" a následné násilné přestavení výhybek č. 313 a č. 314 s vykolejením jednoho drážního vozidla jedním podvozkem jako důsledek srážky s vlakem Pn 61121 v železniční stanici Přerov.	***Chyba strojvedoucího - nerespektování návěsti „Stůj"*** odjezdového návěstidla L104 železniční stanice Přerov osobou řídící drážní vozidlo vlaku Rn 50238 s následnou nedovolenou jízdou vlaku Rn 50238 do postavené vlakové cesty pro vlak Pn 61121.
2007-09-01	Vodňany a dopravna Bavorov v km 9,915	čelně srazily vlaky osobní dopravy Os 18003 a Os 18032 obsazené cestujícími.	***Chyba strojvedoucího - neodsouhlasená jízda vlaku -*** nedovolený odjezd vlaku Os 18003 z dopravny Bavorov bez souhlasu odborně způsobilé osoby, která řídí jízdu vlaků, tj. dirigujícího dispečera.
2008-11-10	Ždírec nad Doubravou, km 27,716	srážka vlaku Os 5307 s posunovým dílem	***Chyba strojvedoucího - neodsouhlasená jízda vlaku -*** jízda posunového dílu mimo obvod železniční stanice, aniž by byl tento posun organizován jako posun mezi dopravnami, konkrétně posun kolem návěstidla „S", vymezujícího obvod stanice, na traťovou kolej, organizování drážní dopravy nesprávným způsobem, konkrétně provádění posunu za označník bez přijatého traťového souhlasu pro přilehlý traťový úsek Ždírec nad Doubravou – Hlinsko v Čechách a nezastavení rušícího posunu.

Z tabulky 3 vyplývá, že ***příčinou nehod spojených s oblastí řízení dopravy u vlaků na nádražích*** jsou:

- chyba strojvedoucího,
- chyba stavitele cesty vlaku,
- chyba osoby odpovědné za řízení dopravy,
- chyba signalisty,
- chyba dozorce výhybek,
- dovolení jízdy drážních těles podle rozhledových podmínek,
- kombinace chyby strojvedoucího a chyby osoby odpovědné za řízení dopravy,
- ***selhání zabezpečovacího zařízení v důsledku špatných meteorologických podmínek***.

Z uvedeného vyplývá, že je třeba zavést další zabezpečení, a to především ke snížení chyb strojvedoucích. Je si třeba přiznat, že zrušením funkce výpravčího, který plácačkou odmával odjezd vlaku byla zrušena kritická funkce drážní dopravy, která nebyla ničím nahrazena.

4.2. Příklady selhání systémů řízení dopravy, na kterých se podílela automatizace

Příčiny selhání systémů řízení jsou uvedeny v [1,38,41,44,45]. Uvedeme několik konkrétních příkladů selhání řídících systémů dopravy.

Moravany 2008

Dne 19. května roku 2008 došlo ve 4 hodiny 48 minut na staniční koleji v Moravanech k závažné železniční nehodě, srážce nákladního vlaku s osobním vlakem s následným vykolejením. Následkem nehody bylo jedno úmrtí, 4 lehce zranění a přímá finanční škoda 12643092,- Kč [46]. Zásadní příčinou byla ztráta kontaktu železničního vozidla na styku koleje s vozidlem.

Zpráva z vyšetřování uvedené dopravní nehody uvádí následující příčiny:

1. Bezprostřední příčiny:
   - ztráta šuntu kolejového obvodu 1K žst. Moravany vlakem Os 5011,
   - reakce staničního zabezpečovacího zařízení ESA 11 na neočekávanou změnu informace o volnosti 1. staniční koleje.
2. Zásadní příčiny:
   - nezajištění kompatibility mezi provozovanými hnacími drážními vozidly a kolejovými obvody v oblasti izolujících emisí – pískování,
   - vnitřní logika staničního zabezpečovacího zařízení ESA 11, konkrétně zpracování nové informace o volnosti koleje obdržené připojením výstroje kolejového obvodu po ukončení vysílání kódu traťovou částí vlakového zabezpečovače.
3. Příčina v systému řízení bezpečnosti - připuštění provozu drážních vozidel nekompatibilních s kolejovými obvody bez odpovídajících bezpečnostních opatření.

Uvedená událost není ojedinělá, zdroj [46] dále uvádí: „29. srpna 2008 došlo v žst. Hulín k události se stejným pozadím, jako má mimořádná událost z 19. května 2008 v žst. Moravany. Po stejné závadě pískovacího zařízení hnacího drážního vozidla stejné řady stejného dopravce tam stejným postupem staničního zabezpečovacího zařízení stejného typu došlo v 17:46:55 hodin ke změně indikace stavu 3. staniční koleje na

„volná“, ačkoliv byla stále obsazena stojícím osobním vlakem Os 4256. Tato událost se obešla bez následků jen díky příznivým okolnostem a reakci zúčastněných zaměstnanců.“

V předmětné události jde ve smyslu společných kybernetických příčin [27] o kombinaci dvou příčin, a to chybný SW a nedostatečný HW; došlo ke zkreslení informací zapříčiněné pískováním a ke špatné reakci systému, tj. o chybu na rozhraní kybernetického a fyzického systému.

Santiago de Compostela 2013

Železniční nehoda v roce 2013, která se stala několik kilometrů od španělské železniční stanice Santiago de Compostela, a byla nejhorší železniční nehodou ve Španělsku za posledních čtyřicet let. Nehoda se stala 24. července 2013 v 20 hodin 41 minut, když v oblouku „Angrois“ s předepsanou omezenou rychlostí 80 km/h vykolejil vysokorychlostní vlak osobní přepravy v rychlosti 179 km/h. Po vykolejení většina vozů narazila na betonovou zeď vedoucí podél oblouku a došlo k požáru na hnacím vozidle. Následkem vykolejení vlaku bylo 80 mrtvých a 152 lidí zraněných, tj. téměř všichni pasažéři [47].

Příčinou nehody byla překročená rychlost vlaku a vyšetřovací komise v závěru obvinila strojvedoucího z nedbalosti a nedodržení drážních předpisů. Tento závěr vyšetřovací komise, které nejsou veřejně dostupné, byly zpochybněny Evropskou Drážní Agenturou ERA, která ve svém dokumentu pro EU popisuje také kořenové příčiny nehody (tj. posoudila i nedostatky v celkovém řídicím systému. Předmětná zpráva ERA [47] uvádí následující skutečnosti, které byly příčinami tak velkých dopadů nehody:

1. Předmětem nehody byl vysokorychlostní vlak 150/151 řady Alvia Class 730, který je modifikací řady 130. Oba konce soupravy jsou vybaveny dieselovými motory. *Poznámka: na základě výsledků šetření dopravních nehod na železnici [1] právě rozlitá nafta k pohonu dieselových motorů mohla být hlavní příčinou velkého požáru*.
2. Souprava 150/151 byla složena z 13 vozů: dvou trakčních vozů doplněných motorovými vozy na každém konci; osmi vozů pro přepravu cestujících; a restauračního vozu. Hmotnost vlaku byla 382 tun.
3. Vlak byl vybaven dvěma zabezpečovacími zařízeními: ASFA Digital a ERTMS/ETCS. Kvůli poruchovosti a dostupnosti systému ERTMS vlaku řady 730 na předmětné trase byl provozovatelem schválen provoz s bodovým zabezpečovačem ASFA Digital. *Poznámka: na základě výsledků šetření dopravních nehod na železnici [1] právě neprovázanost v činnosti obou systémů způsobila narušení integrity bezpečnosti a významně přispěla k dopravní nehodě.*
4. Trať 082 Coto da Torre branch-A Grandeira branch (na 85.0 km) je vybavena balízami, ERTMS/ETCS úrovně 1, s výjimkou jejího začátku a konce, a s podporou zabezpečovače ASFA Digital.
5. „Nízko-rychlostí“ oblouk (s maximální rychlostí 80 km/h) má navržený rádius 402 m a je umístěn na konci úseku tratě vybavené výhradní technologií ASFA Digital.
6. Podél oblouku je vybudována masivní betonová stěna. Maximální povolená rychlost v úseku je 80km/h v souladu s tabulkou maximálních rychlostí danou španělským správcem železniční infrastruktury Adif. *Poznámka: na základě výsledků šetření dopravních nehod na železnici [1] právě fakt, že tabulka nebyla příliš zřetelná, přispěl k nehodě.*

7. Signalizace a cesta byly pro vlak 150/151 řady Alvia Class 730 nastaveny tak, že relevantní signalizace indikovala „track clear“, tj. návěst „Volno“. *Poznámka: na základě výsledků šetření dopravních nehod na železnici [1] právě tento nesprávný fakt na mezery v automatickém řídicím systému.*
8. Značka / tabulka indikace změny rychlosti před obloukem na staničení (PK) 84+273 neobsahovala varování. *Poznámka: na základě výsledků šetření dopravních nehod na železnici [1] právě tento zdánlivě malicherný fakt měl podíl na vzniku dopravní nehody.*
9. Kabina strojvedoucího byla vybavena několika komunikačními systémy (tj. radiotelefon mezi vlakem a tratí, mobilní telefon (GSM-R)) pro podnikovou komunikaci v rámci vlaku a vně vlaku, které neměly zřejmou závadu.
10. Jízdní řád pro strojvedoucího ukazoval změnu rychlosti: omezení rychlosti na 80 km/h na PK 84+230 (the Anrois curve). *Poznámka: na základě výsledků šetření dopravních nehod na železnici [1] jde o možný chybný úkon strojvedoucího.*
11. Pokyny k řízení zahrnovaly požadavek, že před vjezdem do oblouku sám strojvedoucí musí včas zahájit brzdění a přizpůsobit rychlost, tj. z 200 km/h na 80 km/h, a to bez pomoci nějakých určitých technických systémů řízení. *Poznámka: na základě výsledků šetření dopravních nehod na železnici [1] jde o možný chybný úkon strojvedoucího.*
12. V daném případě vlak měl 2-3 minuty zpoždění. *Poznámka: na základě výsledků šetření dopravních nehod na železnici [1] právě zpoždění zvyšovalo stress strojvedoucího, který musí dodržovat jízdní řád.*
13. Záznamy ukázaly, že asi 6 000 metrů před vjezdem do oblouku strojvedoucí reagoval na služební volání vlakového manažera na korporátní mobilní telefon. Hovor trval 100 sekund. *Poznámka: na základě výsledků šetření dopravních nehod na železnici [1] jde o možnou příčinu přehlédnutí značky nabádající ke včasnému snížení rychlosti.*
14. Technická analýza ukázala, že brzdy vlaku 150/151 nebyly dostatečně aktivovány pro dosažení požadovaného omezení rychlosti. *Poznámka: na základě výsledků šetření dopravních nehod na železnici [1] jde o pozdní reakci strojvedoucího.*

Závěr ERA konstatoval, že oficiální vyšetřování Komise pro vyšetřování železničních nehod ve Španělsku (CIAF - Comisión de Investigación de Accidentes Ferroviarios) nezvážilo při stanovení kořenové příčiny nehody všechna fakta, protože se opíralo o úzký pohled na záležitost, tj. strojvedoucí musí vždy reagovat kvalitně a nemůže se opírat o upozornění zabezpečovacích systémů, tj. musí ve správný čas brzděním upravit rychlost vlaku na požadovaných 80km/h [47].

Vyhodnocení dopravní nehody, které jsme provedli na základě závěrů ERA a poznámek k 14 oblastem na základě zkušeností z praxe [1,26], ukazuje, že došlo ke kombinaci několika pochybení, a to především v systému řízení bezpečnosti provozu, a na jejich kombinaci se významně podílela složitost systému pro řízení drážní dopravy.

Z hlediska kybernetických příčin [27] se jedná o:

- zkreslení dat z monitorování, kdy dle výpovědí strojvedoucího došlo k jeho zmatení o aktuální pozici,

- nedostatečný HW, kde byla v nebezpečném úseku snížena úroveň zabezpečení, díky vypnutí zabezpečovacího zařízení ERTMS/ETCS úrovně 1 a tím nebyla kontrolovaná povolená traťová rychlost v daném úseku.

Uvedené případové studie ukazují na řadu příčin železničních nehod, kterými jsou kombinace několika pochybení především v systému řízení bezpečnosti provozu. Vzhledem k tomu, že se dnešní procesy řízení technologických děl, které jsou nedílnou součástí např. předmětného řízení bezpečnosti a dalších částí drážního systému (řídicí systémy, infrastruktury, dopravních prostředků a zařízení), neobejdou bez informačních systémů, tak je velmi důležité hledat především kybernetické příčiny uvedených železničních nehod.

Problémy jsou spojené s rozhraním systémů, která jsou ve správě různých subjektů, anebo se jedná o systémy různých fyzikálních povah. Z kritického posouzení drážní legislativy [28] vyplývá, že předmětné oblasti kybernetického prostoru, kyber-fyzických systémů, nejsou v současnosti řádně legislativně podchycené. Na základě výše uvedených výsledků a poznatků, navrhujeme opatření pro ošetření nalezených zranitelností, tj. zvyšování informačního výkonu a zabezpečení informací v kritických procesech systému řízení předmětného technologického díla, a to v celém procesu vzniku informace a jeho zpracování. V případě uplatňování navrhovaných principů práce přispívá k celkovému zvýšení bezpečnosti drah.

Bad Aibling 2016

Srážka rychlíků 9. 2. 2016 mezi stanicemi Bad Aibling a Kolbermoor v Bavorsku měla 11 obětí a 90 zraněných. Příčinou nebyla přímá technická ani kybernetická chyba, ale chyba lidská – obsluha vypnula řídící systém pro pohyb vlaků [48-50].

DuPont, Washington 2017

Dne 18. 12. 2018 vykolejil vlak na mostě a spadl na dálnici. Událost měla 3 oběti, 70 zraněných a způsobila škodu 404 tisíc USD. Příčinou bylo selhání automatického řídícího systému vlaku [51].

Swanwick

Dne 12. prosince 2014 došlo v centru pro řízení letového provozu (NATS) ve městě Swanwick k selhání řídícího počítače a jeho záloh v důsledku špatně nakonfigurovaného maximálního počtu uživatelských rolí v software. Proto bylo zrušeno přibližně 150 letů, 20 dalších přesměrováno mimo vzdušný prostor Velké Británie a 353 letů bylo zpožděno. Náprava pomocí automatizovaných nástrojů a auditu logů byla provedena pracovníky odborné jednotky ETIC a systém byl po několika hodinách restartován jako plně funkční [52].

Let Air France 447

Dne 31. května 2009 vzlétlo letadlo Airbus A330 let AF 447 v 19:03 hod. místního času (22:03 UTC) z letiště Rio de Janiero Galeão, s plánovaným přistáním v Paříži Charles de Gaulle v 11:10 hod. místního času (09:10 UTC). Letadlo bylo v kontaktu s řízením letového provozu Brazílie ATLANTICO na trase INTOL – SALAPU – ORARO – TASIL v letové hladině FL350. Dne 1. června 2009 ve 2h14m28s UTC došlo k pádu letadla Air France 447 do oceánu u břehů Brazílie [53,54].

Analýza černých skříněk ukázala, že k pádu letadla došlo kvůli selhání ukazatelů rychlosti letu (technická závada byla způsobená námrazou). Nesprávné informace přístrojů způsobily nesprávnou reakci posádky. Mezi 02:10 a 02:14 UTC vyslalo letadlo 24 automatických chybových hlášení pomocí systému ACARS, která informovala o technických problémech: nejprve bylo hlášeno odpojení autopilota a přechod do zvláštního režimu kvůli poruše; pak bylo postupně hlášeno mnoho závad na systémech inerciální navigace a primárním i záložním letovém počítači; a poslední přijaté hlášení z 02:14 UTC upozorňovalo na možnou ztrátu přetlaku v letadle [53,54].

Přestože letadlo mělo dle [53] zkušeného pilota a dva kopiloty, 3 systémy pro zpracování informací o rychlosti a další moderní vybavení, tak námraza na ukazatelích rychlosti letu vedla ke komplexní ztrátě informací o rychlosti letu. Jelikož vzniklá situace nebyla správně pochopena piloty, došlo k nadměrným manipulačním vstupům v naklánění a ostrému zvednutí nosu letadla. Vzniklá destabilizace způsobila změnu a ze stoupající letové dráhy došlo ke sklopení dráhy. Chyby v údajích o rychlosti letu a ve zprávách ECAM (centrální elektronický monitoring letadla) způsobily, že posádka se postupně odchylovala od struktury předepsaného postupu a pravděpodobně nikdy nepochopila, že čelila „jednoduché“ ztrátě tří zdrojů informací o rychlosti letu, a proto nepoužila manévr obnovy (vztlaku a zvýšení letové rychlosti) [53]. To znamená, že ke ztrátě informací se přiřadily lidské chyby způsobené nedostatečným výcvikem pilotů.

Ze závěrečné vyšetřovací zprávy [53] vyplynulo, že pilot nepoužil předepsaný postup při nespolehlivých údajích o rychlosti, snažil se s letadlem stoupat a nevšiml si, že dosáhl maximální výšky. Varování při ztrátě vztlaku a hrozbě pádu se ozývalo 56 sekund, aniž by piloti reagovali, ale přerušilo se, když úhel náběhu překročil 35°, což je mohlo zmást. Ačkoli údaje o výšce a rychlosti vůči zemi byly v pořádku, piloti je patrně pokládali za nespolehlivé a nevěnovali jim pozornost.

Dle [53] havárii způsobila kombinace faktorů:

1. Absence jakéhokoli výcviku, v manuálním ovládání letounu ve vysoké nadmořské výšce a v postupu pro „Let se spornými údaji rychlosti“.
2. Nedostatek jasného zobrazení při zjištění nesrovnalostí u rychloměrů pomocí počítačů.
3. Posádka nebrala v úvahu varování před pádem, které mohlo být způsobeno:
    - neschopností identifikovat zvukovou výstrahu z důvodu nízké doby expozice při výcviku varování před pádem,
    - na začátku se vyskytující přechodná varování, mohla být považována za falešná,
    - absence vizuálních informací potvrzujících počátek pádu po ztrátě mezní rychlostí,
    - možná záměna se situací, kdy je překročena mezní (maximální) rychlost, kdy se za symptom také považuje chvění – cloumání,
    - indikací hlavního letového přístroje (Flight director), které mohly vést posádku k přesvědčení, že její akce jsou vhodné, i když tomu tak nebylo,
    - obtížnost rozpoznat a pochopit důsledky rekonfigurace (změn v řízení) v alternativním právu letu bez ochrany úhlu náběhu.

Při letecké havárii zahynulo celkem 228 osob, z toho 216 pasažérů a 12 členů posádky. Došlo ke zničení letadla Airbus A330-203 s registračním označením F-GZCP. Hlavní části vraku letadla se našly na dně Atlantického oceánu v hloubce téměř

4 000 m pod hladinou v dubnu 2011, tedy téměř cca 2 roky po zahájení pátrání. Pátrací akce po troskách letadla byly vyčísleny na cca 32 mil. EUR [54].

Letecká havárie měla značné dopady na bezpečí (životy) lidí, veřejné blaho i na ekonomiku. Proto: byla zavedena úprava ve výcviku pilotů; byla provedena výměna vadných typů rychloměrů u všech letounů, které používaly stejný typ sond (Pitotovy trubice); byla přijata nová opatření a postupy při certifikaci a zkouškách nových velkých letadel; a byl podpořen výzkum pro zjišťování složení hmot mraků ve vysokých nadmořských výškách [53,54].

Let Egypt Air 804

Dne 19. května 2016 v 0h33m UTC (02h33m Egyptského času) došlo k letecké havárii letounu Airbus A320-232 16 km uvnitř vzdušného prostoru Egypta, 290 km od egyptského pobřeží nad Středozemním mořem (zeměpisné souřadnice 33°40′32.52″ N, 28°47′32.64″ E). Let EgyptAir 804 byl pravidelný mezinárodní let společnosti EgyptAir z letiště Charlese de Gaulla v Paříži na mezinárodní letiště do Káhiry [55,56]. Dle [56] let probíhal za jasného počasí

Těsně před zmizením z radarů stanic pro řízení letového provozu se letadlo stočilo o 90 stupňů doleva a následně z letové hladiny 11 280 m (37 000 ft) prudce kleslo na 4600 m (15 000 ft) a poté na 3 000 m (9 800 ft), přičemž se otočilo o 360 stupňů doprava. Let 804 měl v Káhiře přistát ve 01:05 UTC [56]. Trosky letadla spolu s osobními věcmi cestujících byly objeveny 20. května 2016 pátrací skupinou egyptských ozbrojených sil ve Středozemním moři přibližně 290 km severně od pobřeží města Alexandrie [55].

Automatické elektronické zprávy odesílané letadlem pro potřeby servisu a údržby (ACARS messages) odhalily, že detektory kouře sepnuly na toaletě a v oblasti avioniky pod kokpitem několik minut před ztrátou signálu letadla [56]. Dle BEA [56] vyšetřování doposud nebylo skončeno a existují dvě vyšetřovací verze jako možná příčina vzniku havárie:

- požár v důsledku technické závady (agentura BEA),
- výbuch jako možný násilný – teroristický útok (egyptská prokuratura).

Dle francouzské prokuratury [57] letadlo nebylo způsobilé k letu a nemělo vzlétnout, protože u předchozích letů byly hlášeny opakující se výstrahy hlásicí závady v elektroinstalaci, včetně výstrah hlásících možná nebezpečí požáru.

Dne 17. září 2016 převzala agentura Reuters zprávu z francouzského zpravodajství Le Figaro ze dne 16. září, že francouzští forenzní vyšetřovatelé, kteří navštívili Káhiru, zaznamenali na troskách letadla stopy výbušné látky TNT. Podle zdroje Le Figaro navrhl Egypt společnou zprávu s Francií, která oznamuje objev důkazů o výbušnině, ale Francie odmítla s tím, že egyptské soudní orgány neumožnily francouzským vyšetřovatelům „provést adekvátní inspekci, aby zjistili, jak by se tam stopy mohly dostat“.

Dne 15. prosince 2016 egyptští vyšetřovatelé oznámili, že u obětí byly nalezeny stopy výbušnin, ačkoli zdroj blízký francouzskému vyšetřování vyjádřil pochybnosti o posledních zjištěních Egypta [58].

Dne 13. ledna 2017 zveřejnil francouzský deník Le Parisien článek, ve kterém uváděl, že v kokpitu mohl vzniknout náhodný požár způsobený přehřátím baterie mobilního telefonu ko-pilota na pravé straně panelu přístrojů vedle ko-pilota.

Dne 7. května 2017 francouzští představitelé uvedli, že na tělech obětí nebyly nalezeny žádné stopy výbušnin [56].

Následně byla dne 6. července uvedena tisková zpráva BEA, která potvrzuje závěry uvedené v [56], tj., že nejpravděpodobnější hypotézou příčiny havárie letu Egypt Air 804 byl požár v důsledku technické závady a rychlé šíření požáru. Egypt dosud setrvává na příčině výbuch způsobený teroristickým útokem [55].

Při letecké havárii zahynulo celkem 66 osob, z toho 56 pasažérů a 10 členů posádky (2 piloti, 5 letušek a 3 bezpečnostní pracovníci) a došlo ke zničení letadla Airbus A320-232 s registračním označením SU-GCC [55-58]. Přestože letoun měl moderní vybavení, poškození paměťových čipů v černých skříňkách neumožnilo získat jasné informace o tom, co se na palubě letadla stalo [56].

Let Indonesia PK-AXC

Dne 28. 12. 2014 Airbus A320-216 registrovaný kaako PK-AXC na letu z letiště Juanda v Indonésii na letiště Changi v Singapuru se 162 pasažéry se zřítil do moře [59]. Vyšetřování [59] odhalilo, že k havárii přispěly faktory:

- prasklina v pájeném spoji kabelů A B vedla k výpadku elektřiny, a tím ke ztrátě napájení,
- analýza dat o údržbě odhalila, že nebyly vyřešeny opakující se poruchy na směrovém kormidle v krátkém časovém intervalu – stejná porucha se opakovala 4x během daného letu,
- reakce posádky na první 3 poruchy byla v souladu s předpisy a došlo k obnově; po čtvrté poruše došlo ke ztrátě elektrického napájení,
- přerušení elektrického proudu způsobilo, že se ***uvolnil autopilot*** a řízení letu se změnilo z normálního na alternativní a kormidlo se odklonilo od požadovaného směru,
- následná akce posádky vedoucí k neschopnosti řídit letadlo způsobila pád letadla do moře.

Neodstraněná technická závada na směrovém kormidle vedla k přerušení elektrického proudu a následně k chybě autopilota, tj. automatického řízení letu, což vedlo k havárii.

Havárie boeingu 737 MAX 8

Stroj nízkonákladové indonéské společnosti ***Lion Air Boeing 737 MAX 8*** se 181 pasažéry a osmi členy posádky na palubě havaroval 29. října 2018 krátce po startu z letiště v Jakartě [60]. Vyšetřování nehody v Indonésii mimo jiné ukázalo, že letadlo mělo už dříve problémy s ukazatelem rychlosti a výšky letu. Piloti podle vyšetřovatelů zápasili s novým automatickým systémem, kterým Boeing 737 MAX 8 disponoval. Ten automaticky za některých okolností sklopil nos letadla dolů.

Dle zprávy z vyšetřování [60] leteckou nehodu způsobily chyby v designu letadla, špatný výcvik pilotů a problémy s údržbou stroje. Chyby v designu byly chyby v software řídícího systému. Podle závěrů vyšetřovatelů indonéského úřadu pro bezpečnost leteckého provozu (KNKT) přispěly k havárii dále uvedené skutečnosti:

1. Při návrhu a certifikaci Boeingu 737 MAX se vycházelo z předpokladů o reakci posádky, které se ukázaly nesprávné.
2. Na základě nesprávných předpokladů a neúplných informací bylo schváleno, aby systém MCAS závisel jen na jednom AoA senzoru.

3. Systém MCAS závisel pouze na jednom senzoru, což jej činilo náchylným k chybám.
4. Informace o systému MCAS nebyly v manuálu a ani v informacích pro piloty, což ztížilo reakci pilotů na „splašený“ MCAS.
5. Upozornění na nesouhlasná data ze senzorů (AOA DISAGREE) nebylo správně vyznačeno, a tak se toto varování pilotům neobjevilo.
6. Senzor AOA, který byl do letadla nainstalován, byl špatně kalibrovaný, a kontrola tuto chybu neodhalila.
7. Vyšetřovatelé nemohli ověřit správnou instalaci senzoru (chyběly záznamy). Během instalace nedošlo k odhalení chyby.
8. Neúplné záznamy v přehledu oprav vedly k tomu, že posádka se nemohla poučit z problémů, které se vyskytly během předchozího letu letadla.
9. Velké množství varování se pilotům zobrazilo naráz a nebylo možné je efektivně zvládnout. Bylo to způsobeno obtížností situace i chybami, kterých se piloti dopustili při komunikaci a vyhledávání v manuálu. Předmětné chyby se už předtím objevily při výcviku.

Kvůli nižšímu podvozku boeingu 737 Max konstruktéři posunuli motor více před křídlo. Tím se změnily letové vlastnosti stroje. Do stroje byl vložen řídící systém MCAS (Maneuvering Characteristics Augmentation System), tedy systém zaručující, že se letadlo bude chovat stejně jako Boeing 737. Nový automat byl nezávislý na ostatních autopilotech, podle projektu se měl aktivovat ve chvíli, kdy se letadlo dostalo do nebezpečného úhlu náběhu a hrozil mu pád kvůli takzvanému přetažení. V tu chvíli MCAS měl využít výškový stabilizátor k upravení úhlu náběhu.

Piloti jsou zvyklí na to, že autopilot se nechá přetlačit, stačí, když vezmou za knipl. Ale protože MCAS byl navržený pro mezní situace, dostal možnost na deset sekund přetlačit pilota. Pak pět sekund vypnul. Pokud nebezpečný úhel přetrvával, opět se aktivoval na deset sekund. Pak na pět sekund vypnul a tak dále. Systém MCAS bere informace ze senzoru úhlu náběhu. Každé letadlo má dva tyto senzory, avšak systém MCAS čerpal data pouze z jednoho.

Ve sledovaném případě systém, který měl piloty zachránit v kritické situaci, naopak kritickou situaci zavinil. Poškozený senzor tvrdil, že letadlo je příliš nakloněné vzhůru, a MCAS začal tlačit letadlo k zemi. Piloti jej nedokázali přetlačit ani vypnout, vše se odehrálo během několika minut.

Boeing o potenciálním problému se systémem MCAS věděl už před první nehodou, a to díky reakcím pilotů i vlastních zaměstnanců. Až po druhé nehodě a uzemnění celé flotily 737 MAX však firma Boeing veřejně slíbila, že systém MCAS opraví. Nově si bude brát data z obou senzorů úhlu náběhu a nebude se aktivovat opakovaně. Sníží se také síla korekce, aby se pilotům už nemohlo stát, že je systém přetlačí [60].

Mezinárodní komise i NTBS USA potvrdily závěry KNKT a jako další chybu uvedly, že Boeing: neotestoval systém MCAS v realistických podmínkách; počítal s tím, že piloti případný problém rozpoznají během 4 sekund; vyškrtl popis systému MCAS z manuálu pro piloty [60].

K další nehodě boeingu 737 MAX 8 došlo při letu Ethiopian Airlines 302 dne 10. března 2019 nedaleko etiopského města Bishoftu na lince ET 302 z etiopské Adis Abeby do keňské Nairoby. Zemřelo všech 157 osob na palubě (149 cestujících 33 národností a

8 členů posádky) [61]. Po této nehodě byly všechny letouny řady 737 MAX celosvětově uzemněny; chybný software způsobil smrt 350 lidí [61].

Z analýzy výše uvedených případových studií vyplývá, že příčinou dopravních nehod spojených s automatickými řídícími systémy jsou:

- chybné řízení vlaku či letadla způsobené chybnými informacemi z řídícího systému, které byly způsobeny technickou závadou vyvolanou meteorologickými podmínkami,
- chyba v systému řízení bezpečnosti vlaku či letadla - chybný software - vnitřní logika zabezpečovacího systému nezvažovala scénáře všech možných situací,
- slabý informační výkon bezpečnostního zařízení,
- kombinace slabého informačního výkonu bezpečnostního zařízení a lidské nepozornosti,
- lidská chyba – vypnutí zabezpečovacího zařízení; nepozornost obsluhy,
- selhání automatického řízení vlaku či letadla – výpadek elektrického napájení; porucha řídícího počítače; špatné zálohování řídícího počítače; vnitřní požár; přerušení informačního toku,
- nedostatečná výchova a výcvik řídicího personálu v ovládání IT zařízení.

4.3. Selhání I &C používajících kybernetické technologie

Zatímco fyzické a organizační technologie mají za sebou určitý historický vývoj a pro zajištění jejich bezpečnosti existují postupy, standardy a normy, informační (kybernetická) technologie a její infrastruktura jsou vcelku nové, a proto v současné době má jejich problematika zvláštní postavení. Důvodem tohoto stavu je skutečnost, že doposud nejsou kvalifikované standardy pro snížení zranitelnosti kybernetických systémů (tj. IT). Ke specifickému postavení kybernetické infrastruktury přispěla také analýza teroristických útoků spočívající v ocenění schopnosti teroristů použít nástroje IT k poškození veřejných aktiv, a to i u důležitých technických děl, která jsou součástí kritické infrastruktury [1].

Problémy IT se ve vyspělých zemích řeší od 90. let minulého století. Práce [1] obsahuje popis kybernetických systémů, příklady jejich selhání a jejich příčiny a dopady selhání kybernetických technologií. Příčinami jejich selhání byly:

1. Překročení (přetížení) přenosové kapacity vlastní telekomunikační sítě.
2. Havárie technologických celků.
3. Cílené poškození informační a komunikační infrastruktury (sabotáž, hackerství, terorismus, kriminální činnost apod.).
4. Ztráta integrity dat v informačním systému.
5. Živelní pohromy velkého rozsahu jako rozsáhlé požáry, vichřice, sesuvy půdy, povodně apod. s následným poškozením nebo výpadkem informačních a komunikačních systémů (IKS).
6. Radiační havárie s následným poškozením nebo výpadkem řídicího systému objektu.
7. Havárie velkého rozsahu způsobené vybranými nebezpečnými chemickými látkami a chemickými přípravky s následným poškozením nebo výpadkem řídicího systému objektu.

8. Jiné technické a technologické havárie velkého rozsahu – požáry, exploze, destrukce nadzemních a pozemních částí staveb s následným poškozením nebo výpadkem IKS.
9. Destrukce hrází vodohospodářských děl se vznikem povodňové vlny s následným poškozením nebo výpadkem řídicího systému objektu.
10. Narušení dodávek elektrické energie velkého rozsahu.
11. Narušení zákonnosti velkého rozsahu s následným poškozením nebo výpadkem řídicího systému objektu.
12. Výpadky veřejných telekomunikačních sítí.
13. Disfunkční chování řídících a informačních systémů při zabezpečování základních funkcí státu.
14. Výpadek kritických informačních systémů nebo procesů.

Z poznatků shrnutých v práci [1] vyplývá, že:

1. Pohromy, tj. jevy, které působí škody na kybernetickém systému a jeho infrastruktuře mají původ:
   - v samotné technologii a infrastruktuře systému (konstrukce, spolehlivost, materiál, provoz, organizace apod.),
   - ve vnějších pohromách (živelní pohromy, výpadek elektrické energie, nehody a havárie technologických celků – požár, exploze, kontaminace nebezpečnými látkami),
   - v lidském faktoru (selhání lidí, vandalismus, krádeže apod.),
   - v lidském úmyslu (viry, hacking, zneužití technologií proti lidem, skupinám, státům, terorismus apod.).
2. Dopady pohrom na aktiva kybernetického systému a jeho infrastruktury znamenají selhání řídicích systémů, jejichž činnost realizují.
3. Dopady pohrom na aktiva kybernetického systému a jeho infrastruktury, které se dále přenáší na veřejná aktiva, jsou přímé a nepřímé; např. dopady na bezpečí lidí jsou: psychická újma; kolaps naváděcích systémů; kolaps obranyschopnosti státu; policie nemůže využívat počítačové databáze; selhání bezpečnostních zařízení – zvýšení kriminality; nemožnost zajištění bezpečnosti letecké dopravy; kolaps v městské hromadné dopravě; nedostatek informací – občanské nepokoje; selhání přístupu k bankomatům; nefunkčnost dodávek tepla, elektrické energie aj.; problém v zabezpečení budov a následných kontrol lidí; nemožnost vyplácet sociální dávky a důchody apod.

Závěrem lze konstatovat, že kombinace lidských chyb, chyby v technice, chybná software a nedostatečně robustní hardware vedou k poruchám automatizovaných řídících systémů a následně k haváriím.

5. VYHODNOCENÍ SELHÁNÍ SYSTÉMŮ ŘÍZENÍ DOPRAVY A OPATŘENÍ PRO ZABEZPEČENÍ JEJICH SPRÁVNÉ FUNKCE

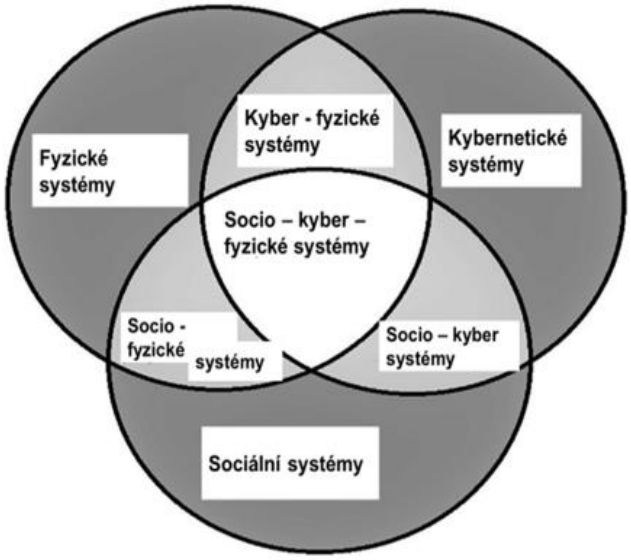
Vzhledem k tomu, že pravidla pro řídící systémy v civilní letecké dopravě jsou upraveny celosvětově ICAO a IATA [9,62], tak se soustředíme na řídící systémy v železniční dopravě. Nejprve provedeme vyhodnocení selhání řídících systémů a pak navrhneme opatření na zvýšení jejich bezpečnosti či zabezpečení. Pro potřebu správného rozhodování je v druhé části stanoven nástroj pro hodnocení integrálního rizika, jelikož příčinou 80 % selhání socio-kyber-fyzických systémů je kombinace více příčin [1,2,39].

5.1. Vyhodnocení selhání systémů řízení v železniční dopravě

Analýza kořenových příčin železničních nehod Moravany a Santiago de Compostela ukázala, že jejich příčinami jsou:

- zkreslení dat z monitorování, kdy dle výpovědí strojvedoucího došlo k jeho zmatení o aktuální pozici, a
- nedostatečný HW, kde byla v nebezpečném úseku snížena úroveň zabezpečení, díky vypnutí zabezpečovacího zařízení ERTMS/ETCS úrovně 1 a tím nebyla kontrolovaná povolená traťová rychlost v daném úseku.

V obou případech uvedených výše se jedná o problém na rozhraních systémů: rozhraní člověk-stroj; a rozhraní mezi systémy pro různé úrovně zabezpečení; obrázek 3.



Obr. 3. Schéma rozhraní v socio-kyber-fyzickém systému.

Z jejich analýzy lze odvodit společné kybernetické příčiny, jimiž jsou především problémy na rozhraních systémů, které jsou navrženy, implementovány i provozovány různými subjekty s ne vždy stanovenou mírou odpovědnosti, jde o:

- problémy na rozhraní člověk – stroj,
- problémy na rozhraních systémů kyber-fyzických,

- problémy na rozhraních systémů socio-technických,
- stanovení odpovědností, a to ne jenom mezi subjekty, ale také mezi procesy systémů, tj. technologických děl.

Předmětnými společnými kořenovými kybernetickými příčinami jsou nedostatečná validita rozhodování systémů, a nízká míra informace v informačních systémech. Analýza provedená v [27] odhalila příčiny:

- ***zkreslení dat z monitorování***, ke kterému dojde v systému pro sběr provozních dat, což způsobí např. nepravdivé informace od strojvedoucích nebo pro strojvedoucí, které způsobí chaos na dispečerských stanovištích, což je příčinou nesprávných úkonů až havárií,
- ***chybný software***, který nezvažuje všechny možné varianty provozních podmínek, což za odchylných provozních podmínek (tj. jiných než těch, na které je sestaven software) způsobí vydání falešných pokynů strojvedoucím a ostatním zaměstnancům, což je příčinou nesprávných úkonů až havárií,
- ***nedostatečně robustní hardware***, který způsobí nesprávné nebo pomalé zpracování a vyhodnocování dat, což má za následek odeslání falešných instrukcí strojvedoucím v provozu, zpoždění zpráv, které vedou k nesprávným úkonům až k haváriím,
- ***hackerský útok*** na řídící centrum dispečerského pracoviště, což způsobí zmatek, který je příčinou nesprávných úkonů až havárií.

Podle poznatků shrnutých v práci [1] specifická rizika pro kritickou část řídících systémů, tj. pro I &C jsou nedostatečně robustní hardware, chybné software, které mohou narušit útoky typu malware, phishing, spear-phishing, whaling, hacking atd. V zájmu minimalizace rizika spojeného s uvedenými škodlivými jevy je na místě implementace odpovídajících preventivních i reaktivních opatření. I přes technický charakter uvedených pohrom (hrozeb) se jako velmi vhodná ukazují být opatření založená na netechnických základech, konkrétně odpovídající výcvik a vzdělání zaměstnanců organizace.

Mezi reaktivní opatření napadeného dopravního řídícího systému by mělo patřit primárně zamezení dalšího šíření škodlivého programu, a to odpojením infikovaného systému od sítě a zavedení náhradního řešení, které zajistí bezpečný provoz složitého systému, který musí pracovat kontinuálně. Poté by mělo následovat očištění systému pomocí speciálních opatření, případně obnovení systému z neinfikované zálohy. V případech, ve kterých je k dispozici dostatečně vyškolený personál, je v rámci reaktivních opatření vhodné provést také určení původního zdroje infekce a přijetí opatření zamezujících jeho využití jiným malware [63].

Vhodná preventivní opatření jsou v případě útoků převážně technické povahy, konkrétně se jedná o instalaci softwarových a hardwarových komponent pro detekci útoku (resp. skenování chování systémů). Vhodným reaktivním opatřením pro případ detekce pokusu o průnik do sítě i pro detekci DoS útoku (jde o odepření služby v důsledku útoku na internetové služby) by mělo být informování odpovídajícího bezpečnostního pracoviště (CERT/CSIRT týmu) a zablokování IP adres, z nichž je útok či průnik veden [64]. V případě trvajícího DoS útoku může být na místě též provedení změny IP adresy postiženého systému či jeho dočasné odpojení od internetu [64]. Přestože výcvik personálu organizace nemůže popsaným typům útoku zabránit, může značným způsobem přispět k jejich odhalení a včasné reakci. Ani v rámci implementace opatření proti hrozbě hackerských útoků by tedy tento aspekt prevence neměl být zanedbáván [62].

V případě systému řízení železniční dopravy však některé výše uvedené způsoby reakce jsou proveditelné pouze v krajním případě, protože z ekonomických a

společenských důvodů jde o to, aby doprava byla plynulá. Proto se aplikuji opatření proti kybernetickým útokům [65,66]:

- umožnění přístupu k řídicím systémům pouze přes specifické přístupové body,
- zavedení bezpečnostního monitoringu provozu na vnitřní síti,
- zajištění dostatečné úrovně znalostí informační bezpečnosti u zaměstnanců.

Standard NIST SP 800-53 [67] obsahuje opatření, která mohla daným útokům zamezit (např. monitorování/omezení vzdáleného přístupu, management uživatelských účtů apod.).

Z poznatků shrnutých v práci [1] lze konstatovat, že kybernetické sítě, a tím i automatické řídicí systémy jsou velmi zranitelné tím, že zvažují pouze náhodné odchylky a nezvažují neurčitosti způsobené jak znalostními nejistotami, tak změnami skokem, které jsou vyvolané pohromami všeho druhu, a to nejen úmyslnými útoky. Z důvodu jejich bezpečnosti dle [63] je nutné, aby měly specifický program pro kybernetické zabezpečení, program na hodnocení rizik a postupy pro jeho realizaci.

Z výzkumu řídicího systému metra [68] je zřejmé, že z důvodu ochrany řídicích systémů musí být chráněna data pro rozhodování, což znamená:

- vstup do kybernetického prostoru musí být chráněn hesly s tím, že se věnuje péče délce hesla, komplexnosti hesla, způsobu používání hesla, pravidelným změnám hesla, indikaci uživatelů, sdílení účtů a speciálně logice řízení přístupu,
- přístup k informacím nesmí být neomezený, musí být sledován a dokumentován nezávisle na uživateli, musí být dozorován a posuzován,
- integrita kybernetického prostoru musí být kontinuálně monitorována a pravidelně prověřována,
- každé narušení kybernetického systému musí být vyšetřeno, musí být posouzena jeho závažnost a musí být přijata opatření, aby se snížily četnost i závažnost jeho opakování,
- důležitá data i způsoby zpracování dat musí být zálohované,
- skartovaná data musí být bezpečně likvidována.

5.2. Opatření pro zvýšení bezpečnosti systému řízení železnice

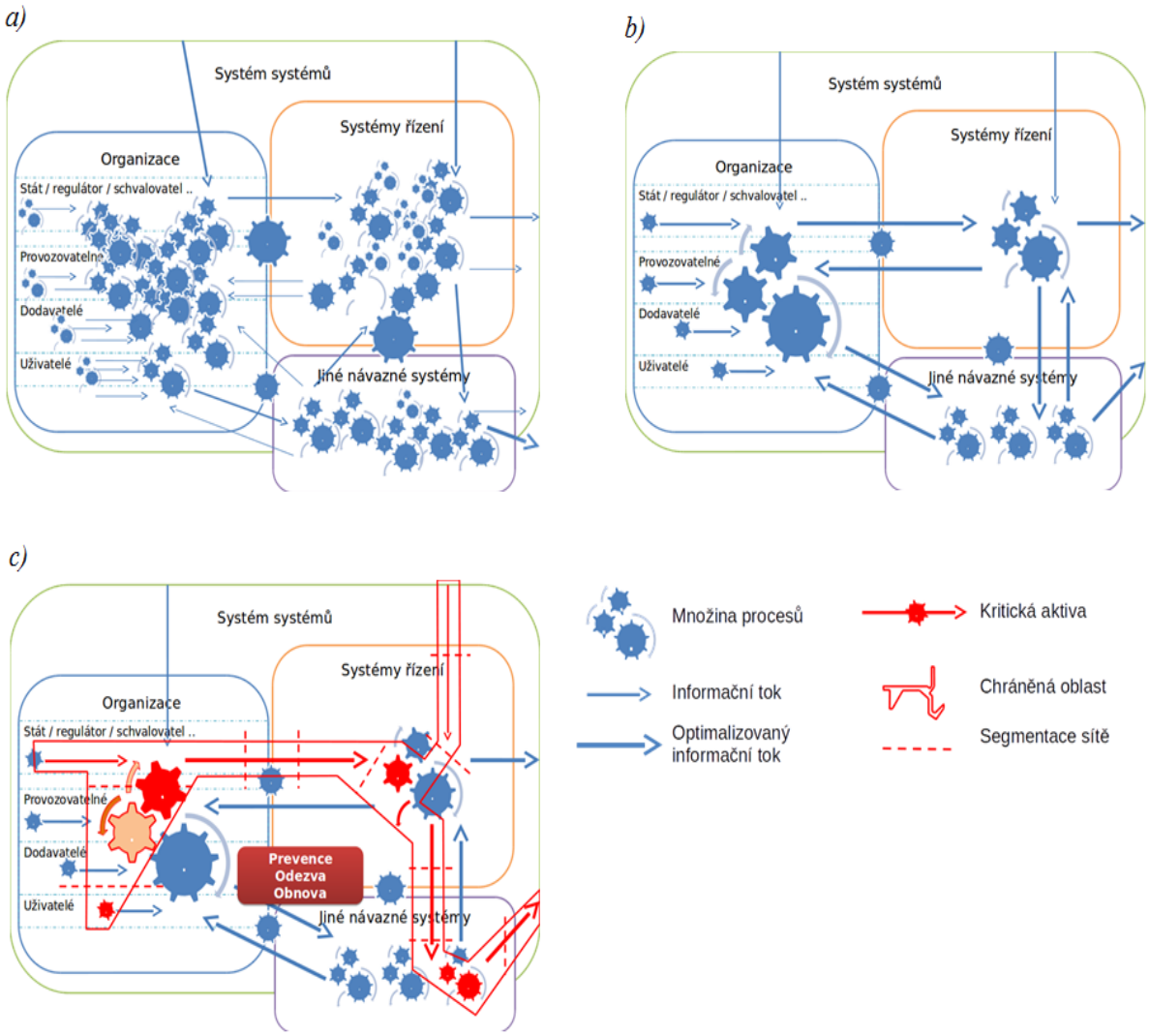
Aby drážní systém, jakožto také část kritické dopravní infrastruktury, vykazoval nejvyšší míru bezpečnosti a tím i informačního výkonu [28,69], musí všechny zúčastněné subjekty aplikovat přístupy TQM se zvážním integrálních rizik [4] spojených s problematikou systémů systémů. Souvislost mezi zvyšováním informačního výkonu a bezpečností kyber-fyzického systému je znázorněna na obrázku 4 [28].

Na obrázku 4 můžeme s určitou mírou abstrakce pozorovat postupnou změnu systému při zavádění různých technik pro zabezpečení systému:

1. Obrázek 4 - a) znázorňuje otevřený systém systému, ve kterém jsou zavedeny procesy a vazby tak, aby vykonával definované funkce. Vzhledem k velkému množství vazeb, interakcí velkého množství subjektů, které se na systému podílí, a návazných i okolních systémů, předmětný systém může za normálních okolností plnit požadované funkce, ale při odchylkách v provozu a v prostředí je náchylný na chyby.
2. Obrázek 4 - b) ukazuje systém systémů s optimalizovaným informačním výkonem, kterým se zvyšuje odolnost a udržovatelnost systému, a tím i jeho bezpečnost.

Optimalizací, tj. usměrněním toků a zlepšením parametrů informačního výkonu se dosáhne toho, že je systém méně náchylný na vnitřní chyby v případě různých známých odchylek v provozu a v okolním prostředí.

3. Obrázek 4 - c) ukazuje dobře zabezpečený systém systémů s optimalizovaným informačním výkonem, který dostaneme z případu, znázorněném na obrázku 3 - b) tím, že ho ochráníme vůči vnějším i vnitřním vlivům, tj. zavedeme preventivní opatření pro snížený významných rizik, připravíme opatření pro přiměřenou odezvu v případě incidentů a opatření obnovy podle řádně testovaných a ověřovaných plánů kontinuity. Z výše uvedeného je zřejmé, že pro bezpečný provoz je velmi důležité se zabývat ne jenom zabezpečením informačních a technologických aktiv, ale také zajistit požadovaný informační výkon systému napříč všemi úrovněmi a dotčenými subjekty.



Obr. 4. Tři typy zabezpečení kyber-fyzického systému [28]: a) běžný systém systémů; b) optimalizovaný systém systémů s vyšším informačním výkonem; c) zabezpečený systém systémů s vyšším informačním výkonem.

V současnosti je kladen velký důraz na vývoj zabezpečených drážních systémů [69-72], a proto nároky jsou zaměřené především na bezpečnost technologické platformy,

která je pro bezpečnost celku velmi důležitá, ale neřeší komplexní problémy (ve smyslu složité), tj. bezpečí lidí. Integrální bezpečnost zaměřená na bezpečí lidí je stále v praxi přehlížená. Množství investic do oblasti bezpečnosti a zabezpečení celků je totiž velmi zatíženo ekonomickými aspekty [3].

Informační systémy v železniční dopravě, založené na informačních technologiích jsou implementované v oblastech: zajištění kvality drážní dopravy; zabezpečení drážních systémů; a bezpečnost provozu drážních systémů. Informační technologie interpretují, pomáhají zvládat, anebo v případě automatizovaného provozu také řídit všechny uvedené kvalitativní a bezpečnostní parametry. Informační systémy a technologie jsou integrální částí drážního systému. Parametry informačního výkonu jsou ovlivněny ve všech procesech vzniku informace, tj. optimalizace se pak zabývá každým procesem a použitou informační technologií uvedenou v tabulce 4.

Tabulka 4. Procesy vzniku informace a informační technologie [29].

	Podproces vzniku informace / množiny objektů	**Dotčené abstraktní uzly**	**Použité informační technologie**	**Vstupy procesu**	**Výstupy procesu**
1	Identifikace objektu	Objekt, pozorovatel	Fyzické receptory (senzory, čidla)	Pozorované stavové (fyzické) veličiny objektu	Signály
2	Pozorování	Pozorovatel, jazyk (syntaxe)	Vzorkování, kvantování, kódování/dekódování	Signály	Data
3	Komunikace mezi zdrojem a příjemcem zprávy	Jazyk (pozorovatele, resp. systému sběru dat), příjemce zprávy	Telekomunikační, přenosové a sdělovací systémy	Data	Data
4	Interpretační množina, vznik informace	Jazyk (pozorovatele, resp. systému sběru dat, nebo příjemce), množina informací (viz 6)	Ontologie, jazyk	Data	Informace

5	Vazby funkcí a strukturálního uspořádání objektu, ověření celistvosti (integrity)	Informace (viz 6), objekt	Akční člen systému, akční informační systém	Objektu, informace	Správnost informace, změna objektu
6	Množina informací v množině informačních systémů	Informační systémy	Informační systémy	Informace	Informace
7	Proces interpretace	Informace (viz 6), nový objekt	Signalizace a technologie reprezentace informace, umělá inteligence	Informace	Obraz objektu, nový objekt

Pro zvýšení informačního výkonu a minimalizaci zdrojů, které jsou nezbytné pro tvorbu těchto systémů, lze v praxi využít řadu metod, např.: COBIT pro audit informačních systémů z hlediska vrcholového managementu [70]; ITIL pro řízení informačních systémů a služeb, jehož části jsou standardizované [71]; refaktoring, tj. změny v systému software, které neovlivní vnější chování informačního systému, ale zlepší jeho vnitřní strukturu [24].

Zavádění systémů řízení [72,73] s podporou informačních systémů navržených pomocí výše uvedených metod, výrazně přispívá ke zlepšení informačního výkonu pouze v případě, pokud se kontext systému řízení zaměřuje na drážní systém jako celek, tj. s jednotnou terminologií a zaměřením na rozhraní systémů napříč všemi zúčastněnými, tj. dotčenými subjekty [28].

Obrázek 4 - c) ukazuje řádně zabezpečený systém s optimalizovaným informačním výkonem, který získáme ochranou optimalizovaného systému proti značným externím a interním vlivům, tj. zavádíme preventivní a zmírňující opatření, a připravujeme opatření na odezvu v případě incidentů, stejně tak jako opatření pro rychlou obnovu pomocí ověřených plánů kontinuity. V oblasti řízení a správy železničního systému a souvisejících organizací se postupně zavádějí systémy a metody podle [7,8,74]. Musí být však implementovány všemi zainteresovanými subjekty, a především je potřeba se vyrovnat s problémy spojenými se systémovými rozhraními; tj. musí zvážit celý proces vzniku informace, použité informační technologie a kvality jejich parametrů.

Zabezpečení systému se zaměřuje na identifikaci a řízení důležitých aktiv. Jelikož nelze zabezpečit vše, musíme vybrat aktiva kritická, tj. kritické procesy, informační toky či jiná podpůrná informační i fyzická aktiva. Na základě kritičností, tj. funkce důležitosti a zranitelnosti, posuzujeme primární rizika systému a zavádíme vhodná preventivní opatření. V případě výskytu pohromy (včetně kybernetického útoku) provádíme odezvu a obnovu dle stanovené politiky.

Podle zásad bezpečnosti systémů systémů je třeba celý drážní systém vybudovat dle přístupu Defence-in-Depth [1,38,39,72] a v jeho rámci zavést různé typy řízení bezpečnosti odrážející očekávané provozní podmínky systému, a popř. pro závažné

pohromy mít i způsob řízení, který bude ochraňovat i jiná aktiva než aktiva technického díla, ve kterém sledujeme fyzická, organizační a kybernetická aktiva [29].

5.3. Nástroj pro stanovení integrálního rizika systémů řízení

Každý řídící systém používaný v dopravě je složitý socio-kyber-fyzický systém. Na základě výsledků podrobného výzkumu technických děl v rámci projektu RIRIZIBE [38,39,76] je nutno věnovat speciální pozornost při řízení rizik ve prospěch bezpečnosti kritickým technickým dílům, do kterých železniční doprava bezesporu patří, při zpracování konceptu návrhu, projektování a provozování. Je to proto, že nestačí sledovat jen dílčí rizika, ale je třeba sledovat integrovaná rizika pro zajištění bezpečnosti procesů a integrální rizika pro zajištění bezpečnosti celku.

Proto dle závěrů práce [77] jsme při konstrukci nástroje pro posuzování jejich míry rizika, tj. systému pro podporu rozhodování (DSS) použili kombinaci kontrolního seznamu, a principů teorie maximálního užitku [78]. Hodnocení kontrolního seznamu je prováděno klasifikační stupnicí 1 až 5 a je navrženo způsobem, že nejvyšší hodnocení (5) u každé hodnocené otázky, připadá nejlepšímu způsobu zvládnutí daného problému (tj. validita techniky je nejvyšší) na základě současných znalostí a zkušeností. Stupnice pro posuzování celkového výsledku kontrolního seznamu je zvolena v souladu s doporučeními v práci [32].

Vytvořený specifický kontrolní seznam je v tabulce 5. Kontrolní seznam obsahuje 72 otázek a stupnice pro jeho celkové vyhodnocení (tj. míry rizika) podle zásad uvedených v [32], je v tabulce 6.

Tabulka 5. Kontrolní seznam pro posuzování integrálního rizika řídícího systému na základě posouzení práce s riziky.

Otázka	**Hodnocení**
Jsou v dokumentaci řídícího systému odlišovány pojmy nebezpečí, ohrožení a riziko?	
Je dokumentace řídícího systému založena na kontextu, který zvažuje jen aktiva řídícího systému?	
Je dokumentace řídícího systému založena na kontextu, který zvažuje aktiva řídícího systému a vybraná veřejná aktiva (zaměstnanci, kontraktoři, návštěvníci, lidé v okolí, pracovní a životní prostředí)?	
Je dokumentace řídícího systému založena na kontextu, který zvažuje aktiva řídícího systému a všechna veřejná aktiva?	
Jsou zvažovány zdroje rizik, které stanovuje zkušenost experta?	
Jsou zvažovány zdroje rizik, které stanovuje legislativa a zkušenost experta?	

Jsou zvažovány zdroje rizik, které zahrnují všechny zdroje rizik spojené s technologií řídícího systému?	
Jsou zvažovány zdroje rizik, které zahrnují všechny zdroje rizik spojené s technologií řídícího systému a lidský faktor spojený se špatně provedenými pracovními úkony?	
Jsou zvažovány zdroje rizik, které zahrnují všechny zdroje rizik spojené s technologií řídícího systému a lidským faktorem v nejširším pojetí?	
Jsou zvažovány zdroje rizik, které zahrnují všechny zdroje rizik spojené s technologií řídícího systému, zdroje spojené s BOZP a zdroje spojené s ochranou pracovního prostředí?	
Jsou zvažovány zdroje rizik, které zahrnují všechny zdroje rizik spojené s technologií řídícího systému, zdroje spojené s BOZP a zdroje spojené s ochranou pracovního prostředí i s ochranou životního prostředí vně řídícího systému?	
Jsou zvažovány zdroje rizik, které zahrnují všechny zdroje rizik spojené s technologií řídícího systému, zdroje spojené s BOZP a zdroje spojené s ochranou pracovního prostředí i s ochranou životního prostředí vně řídícího systému v systémovém pojetí (tj., že všechny zdroje rizik jsou vzájemně propojené)?	
Jsou zvažovány zdroje rizik dle přístupu All-Hazard-Approach [79,80] (tj. systémové pojetí i vnější zdroje)?	
Je zvažováno jen dílčí riziko?	
Jsou zvažována dílčí rizika i integrované riziko?	
Jsou zvažována dílčí rizika, integrovaná rizika i integrální riziko?	
Jsou rizika spojená s řídícím systémem systematicky sledována?	
Jsou rizika spojená s řídícím systémem systematicky sledována až po výstavbě řídícího systému?	
Jsou rizika spojená s řídícím systémem systematicky sledována po celou dobu životnosti řídícího systému už od tvorby jeho projektu?	
Jsou rizika řídícího systému systematicky sledována po celou dobu životnosti řídícího systému už od tvorby jeho projektu a v jeho projektu a provozu je uplatněn přístup Defence-In-Depth [75]?	
Je při práci s riziky řídícího systému systematicky použit procesní model práce s riziky?	
Je při práci s riziky řídícího systému systematicky použit procesní model práce s riziky, který má jasně určena kritéria přijatelnosti rizik?	
Je při práci s riziky řídícího systému systematicky použit procesní model práce s riziky, který má jasně určena kritéria přijatelnosti rizik, která respektují veřejný zájem (tj. mají sociální rozměr)?	
Je při práci s riziky řídícího systému systematicky použit procesní model práce s riziky, který má jasně určena kritéria přijatelnosti rizik a cíle řízení rizik?	

Je při práci s riziky řídícího systému systematicky použit procesní model práce s riziky, který má jasně určena kritéria přijatelnosti rizik a cíle řízení rizik s ohledem na veřejný zájem?	
Je při práci s riziky řídícího systému systematicky použit procesní model práce s riziky, který má jasně určena kritéria přijatelnosti rizik, cíle řízení rizik s ohledem na veřejný zájem a nápravná opatření v monitoringu pro případ, že nebezpečí se stane nepřijatelné?	
Je při práci s riziky řídícího systému systematicky určen a sledován soubor prioritních rizik?	
Zajišťuje technika řízení rizik řídícího systému v každé fázi práce s riziky přezkoumání přínosů a nákladů spojených s opatřeními na vypořádání rizik, aby se zajistilo hospodárné nakládání se silami, zdroji a prostředky řídícího systému?	
Zajišťuje technika řízení rizik řídícího systému v každé fázi práce s riziky přezkoumání přínosů a nákladů spojených s opatřeními na vypořádání rizik, aby se zajistilo hospodárné nakládání se silami, zdroji a prostředky řídícího systému a veřejné správy?	
Jsou v řídícím systému prováděna systematicky preventivní opatření na snížení nebo odvrácení rizik, a to jen některých?	
Jsou v řídícím systému prováděna systematicky preventivní opatření na snížení nebo odvrácení rizik, a to všech prioritních?	
Jsou v řídícím systému prováděna systematicky preventivní opatření na snížení nebo odvrácení rizik, a to všech, které by mohly způsobit závažné ztráty jeho vlastníkovi?	
Jsou v řídícím systému prováděna systematicky preventivní opatření na snížení nebo odvrácení rizik, a to všech, které by mohly způsobit závažné ztráty jeho vlastníkovi a nepřijatelné dopady na okolní životní prostředí?	
Jsou v řídícím systému prováděna systematicky preventivní opatření a připravována zmírňující opatření na snížení největších dopadů rizik, a to jen některých?	
Jsou v řídícím systému prováděna systematicky preventivní opatření a připravována zmírňující opatření na snížení nebo odvrácení rizik, a to všech prioritních?	
Jsou v řídícím systému prováděna systematicky preventivní opatření a připravována zmírňující opatření na snížení nebo odvrácení dopadů rizik, a to všech, které by mohly způsobit závažné ztráty letišti / jeho vlastníku?	
Jsou v řídícím systému prováděna systematicky preventivní opatření a připravována zmírňující opatření na snížení nebo odvrácení dopadů rizik, a to všech, které by mohly způsobit závažné ztráty v řídícímu systému / celému technickému dílu / jeho vlastníku a mít nepřijatelné důsledky pro okolní životní prostředí?	
Je provozovatel řídícího systém pojištěn pro případ realizace rizik?	

Má provozovatel řídícího systému rezervy finanční, materiální, technické, personální a organizační pro odezvu v případě realizace závažného rizika?	
Má provozovatel řídícího systému rezervy finanční, materiální, technické, personální a organizační pro obnovu v případě realizace závažného rizika?	
Má provozovatel řídícího systému rezervy finanční, materiální, technické, personální a organizační pro odezvu a obnovu v případě realizace extrémního neočekávaného rizika?	
Jsou při práci s riziky řídícího systému zohledněny jen výsledky předběžných analýz rizik?	
Jsou při práci s riziky řídícího systému upřednostněny výsledky standardních, rychlých a méně přesných analýz rizik před výsledky předběžných analýz rizik?	
Jsou při práci s riziky řídícího systému upřednostněny výsledky detailních analýz rizik v souhrnném kontextu před výsledky standardních, rychlých a méně přesných analýz rizik a před výsledky předběžných analýz rizik?	
Jsou při práci s riziky řídícího systému upřednostněny výsledky individuálních a specifických analýz rizik před výsledky detailních analýz rizik v souhrnném kontextu, standardních, rychlých a méně přesných analýz rizik a předběžných analýz rizik?	
Jsou při práci s riziky řídícího systému stanovena kritéria pro hodnocení?	
Jsou při práci s riziky řídícího systému stanovena kritéria pro hodnocení technické a ekonomické?	
Jsou při práci s riziky řídícího systému stanovena kritéria pro hodnocení technické a ekonomické, externí a interní?	
Jsou při práci s riziky řídícího systému stanovena kritéria pro hodnocení technické a ekonomické, externí a interní a sociálně – politické?	
Jsou při práci s riziky řídícího systému stanoveny požadavky pro zajištění bezpečnosti?	
Jsou při práci s riziky řídícího systému stanoveny požadavky, standardy a normy pro zajištění bezpečnosti?	
Jsou při práci s riziky řídícího systému stanoveny požadavky, standardy a normy pro zajištění bezpečnosti a dílčí cíle?	
Jsou při práci s riziky řídícího systému stanoveny požadavky, standardy a normy pro zajištění bezpečnosti, dílčí cíle a metody a postupy?	
Jsou při práci s riziky řídícího systému stanoveny požadavky, standardy a normy pro zajištění bezpečnosti, dílčí cíle, metody a postupy a také limity a podmínky?	
Jsou při práci s riziky řídícího systému stanoveny požadavky, standardy a normy pro zajištění bezpečnosti, dílčí cíle, metody, postupy, limity a podmínky, a kompetence osob či institucí?	
Má správce řídícího systému systém řízení bezpečnosti (SMS), který je postaven na zásadách procesního řízení a systematické práce s riziky?	

Má správce řídícího systému systém řízení bezpečnosti, který obsahuje organizační strukturu, odpovědnosti, praktiky, předpisy, postupy a zdroje pro určování a uplatňování prevence pohrom či alespoň zmírnění jejich nepřijatelných dopadů na řídící systém a okolní území?	
Má správce řídícího systému systém řízení bezpečnosti (SMS), který má proces řízení, který obsahuje šest procesů: koncepce a řízení; administrativní postupy; technické záležitosti; vnější spolupráce; nouzová připravenost; a dokumentace a šetření havárií (dopravních nehod a jiných selhání)?	
Má SMS správce řídícího systému proces koncepce a řízení, který obsahuje podprocesy pro: celkovou koncepci; dosahování dílčích cílů bezpečnosti; vedení / správu bezpečnosti; systém řízení bezpečnosti; personál a zahrnuje úseky pro: řízení lidských zdrojů, výcvik a vzdělání, vnitřní komunikaci / informovanost a pracovní prostředí; revize a hodnocení plnění cílů v bezpečnosti?	
Má SMS správce řídícího systému proces administrativního postupu, který obsahuje podprocesy pro: identifikaci ohrožení od možných pohrom a hodnocení rizika; dokumentaci postupů (včetně systémů pracovních povolení); řízení změn; bezpečnosti ve spojení s kontraktory; a dozor nad bezpečností výrobků?	
Má SMS správce řídícího systému proces technické záležitosti, který obsahuje podprocesy pro: výzkum a vývoj; projektování a montáže; inherentně bezpečnější procesy; technické standardy; skladování nebezpečných látek; a údržbu integrity a údržbu zařízení a objektů?	
Má SMS správce řídícího systému proces vnější spolupráce, který obsahuje podprocesy pro: spolupráci se správními úřady; spolupráci s veřejností a dalšími zúčastněnými (včetně akademických pracovišť); a spolupráci s dalšími podniky?	
Má SMS správce řídícího systému proces nouzová připravenost, který obsahuje podprocesy pro: plánování vnitřní (on-site) připravenosti; usnadnění plánování vnější (off-site) připravenosti (za kterou odpovídá veřejná správa); a koordinaci činností resortních organizací při zajišťování nouzové připravenosti a při odezvě?	
Má SMS správce řídícího systému proces dokumentace a šetření havárií, který obsahuje podprocesy pro: zpracování zpráv o pohromách, haváriích, skoro nehodách a dalších poučných zkušenostech; vyšetřování škod, ztrát a újmy a jejich příčin; a odezvu a následné činnosti po pohromách (včetně aplikace poučení a sdílení informací)?	
Je v SMS správce řídícího systému program na zvyšování bezpečnosti, ve kterém jsou stanoveny role zúčastněných, pravidla pro zvyšování kultury bezpečnosti (tzv. zlatá pravidla) a příslušné odpovědnosti?	
Je v SMS správce řídícího systému program na zvyšování bezpečnosti, ve kterém jsou: bezpečnostní plány (strategická, taktická, operativní a technická úroveň); vnitřní a vnější nouzové plány, plány kontinuity a krizové plány?	
Je v SMS správce řídícího systému program na zvyšování bezpečnosti, ve kterém je plán řízení prioritních rizik s jasně stanovenými opatřeními a odpovědnostmi?	

Je v SMS správce řídícího systému program na zvyšování bezpečnosti, ve kterém je plán řízení prioritních rizik s jasně stanovenými opatřeními a odpovědnostmi, který obsahuje jen technická rizika?	
Je v SMS správce řídícího systému program na zvyšování bezpečnosti, ve kterém je plán řízení prioritních rizik s jasně stanovenými opatřeními a odpovědnostmi, který obsahuje technická a organizační rizika?	
Je v SMS správce řídícího systému program na zvyšování bezpečnosti, ve kterém je plán řízení prioritních rizik s jasně stanovenými opatřeními a odpovědnostmi, který obsahuje technická, organizační a vnější rizika?	
Je v SMS správce řídícího systému program na zvyšování bezpečnosti, ve kterém je plán řízení prioritních rizik s jasně stanovenými opatřeními a odpovědnostmi, který obsahuje technická, organizační, vnější a kybernetická rizika?	
Je v SMS správce řídícího systému zajištěn kvalitní monitoring integrálního rizika a závažných dílčích rizik a nápravná opatření pro případ nepřijatelných rizik?	
CELKEM	

Tabulka 6. Hodnotová stupnice pro stanovení míry rizika.

Míra rizika	**Hodnoty v %**	**Výsledek hodnocení**
Extrémní – 5	Méně než 5 %	Méně než 18
Velmi vysoká – 4	5 - 25 %	18 – 90
Vysoká – 3	25 - 45 %	90 – 162
Střední – 2	25 – 45 %	162 - 252
Nízká – 1	45 – 70 %	252 - 342
Zanedbatelná – 0	Více než 95 %	Více než 342

Podle zjištěných hodnot rizika se výsledky posouzení rizika řadí do tří skupin:

- riziko přijatelné – kategorie 0 a 1,
- riziko ALARA, tj. podmíněně přijatelné – kategorie 2 a 3,
- riziko nepřijatelné – kategorie 4 a 5.

Jeli riziko přijatelné, tak není třeba dělat žádná další opatření na zmírnění rizika. Je-li riziko ALARA, tak je třeba v projektu zabudovat technické prvky, které umožní odezvu v případě realizace rizika. V případě nepřijatelného rizika, je nutné provést korekce, např. v materiálu, konstrukci či způsobu propojení a znovu riziko posoudit.

Současná kultura bezpečnosti, vymezená v pracích [1,2,32,38,39,73,74] ukládá managementu, aby praktikoval takový systém řízení bezpečnosti, který udrží procesy v technologických objektech, tj. ve sledovaném případě u řídícího systému, v určitých mezích. Týká se všech účastníků provozu v socio-kyber-fyzickém objektu, protože vlastníků (nositelů) rizik je mnoho.

6. ZABEZPEČENÍ SYSTÉMU ŘÍZENÍ VLAKŮ V EVROPĚ

Úkolem železnice je, aby vlaky jezdily rychle a plnily úkoly bez výskytu dopravních nehod. Vlaky se nemohou navzájem srazit, pokud nemají povoleno obsazení stejného úseku trati ve stejnou dobu, proto jsou železniční tratě rozděleny na úseky známé jako bloky . Za normálních okolností je v každém bloku povolen pouze jeden vlak. Tento princip tvoří základ většiny bezpečnostních systémů železnic.

Bloky mohou být buď pevné (limity bloků jsou fixovány podél čáry), nebo pohyblivé bloky (konce bloků definované vzhledem k pohybujícím se vlakům). Proto se zmíníme o úloze signalizačního systému pro železnici, ukážeme problémy zavedení automatického řízení dopravy a koncept jejího řešení. Nakonec uvedeme koncept zabezpečení železniční dopravy realizovaný v Evropě pod gescí EU.

6.1. Role a vývoj signalizačního systému na železnici

Železniční signalizace je systém, který se používá k nasměrování železniční dopravy a k udržení vlaků v bezpečné vzdálenosti od sebe. Vlaky se pohybují po pevných kolejnicích a nemohou se navzájem vyhnout, takže jsou velmi náchylné ke kolizím. Předmětnou náchylnost umocňuje obrovská hmotnost a hybnost vlaku, což ztěžuje rychlé zastavení při narážení na překážku.

Většina forem řízení vlaků zahrnuje předávání oprávnění k pohybu od osob odpovědných za každou část železniční sítě (např. signalistu nebo vedoucího stanice) k vlakovému personálu. K tomu slouží sada pravidel a fyzické vybavení, které je závislé na podmínkách a legislativě jednotlivých zemí. Nejjednodušší formou provozu, alespoň pokud jde o vybavení, je provozování systému podle časového harmonogramu. Každý vlakový personál mu rozumí a dodržuje pevný harmonogram. Vlaky mohou jezdit na každém úseku trati pouze v plánovaném čase, během kterého mají „majetek“ a žádný jiný vlak nesmí používat stejný úsek. Když vlaky jedou opačným směrem po jednokolejné železnici, jsou naplánována místa setkání („setkávání“), kde každý vlak musí čekat na druhý v místě projíždění. Ani jeden čekající vlak se nesmí pohybovat, než dorazí druhý.

Systém jízdního řádu má několik nevýhod. Za prvé, neexistuje žádné pozitivní potvrzení, že trasa vpřed je průjezdná, pouze to, že je naplánováno, aby byla volná. Druhým problémem je nepružnost systému. Vlaky nelze přidávat, odkládat nebo přeplánovat bez předchozího upozornění. Třetím problémem je důsledek druhého: systém je neefektivní. Aby byla zajištěna flexibilita, musí jízdní řád poskytnout vlakům široké přidělení času, aby bylo možné zpoždění, takže trať není v držení každého vlaku déle, než je jinak nutné.

S příchodem telegrafu v roce 1841 byl možný sofistikovanější systém, protože to poskytovalo prostředky, pomocí nichž bylo možné přenášet zprávy před vlaky. Telegraf umožnil šíření veškerých změn jízdního řádu, známých jako vlakové objednávky. To umožnilo zrušení, přeložení jízdního řádu a přidání vlakových souprav.

Při tomto způsobu vlak nesmí vstoupit do bloku, dokud signál nenaznačí, že vlak může pokračovat; dispečer nebo signalista instruuje strojvedoucího odpovídajícím způsobem. Ve většině případů nemůže vlak vstoupit do bloku, dokud není nejen samotný

blok bez vlaků, ale je také prázdný úsek za koncem bloku alespoň na vzdálenost potřebnou k zastavení vlaku.

Ve 30. a 40. letech 20. století (ve velmi raných dobách železnice) neexistovala pevná signalizace - žádný systém informování strojvedoucího o stavu trati před vlakovou soupravou. Vlaky jezdily „na dohled“. Strojvedoucí museli mít oči otevřené pro jakékoli informace o vlaku vpředu, aby mohli zastavit, než do něj narazili. Praktické zkušenosti však velmi brzy prokázaly, že to nefunguje, a že musí existovat způsob, jak zabránit vzájemné kolizi vlaků. Několik nepříjemných nehod ukázalo, že zastavení vlaku v dohledné vzdálenosti strojvedoucího bylo obtížné. Problémem byla částečně nezkušenost a špatné brzdy, ale skutečným problémem byl (a stále je) poměrně slabý kontakt, který existuje na železnici mezi ocelovým kolem a ocelovou kolejnicí pro trakci a brzdění. Úrovně adheze jsou mnohem nižší a hmotnosti vozidel mnohem vyšší na železnici než na silnicích, a proto vlaky potřebují k zastavení mnohem větší vzdálenost než například automobil jedoucí stejnou rychlostí. Dokonce i za nejlepších podmínek bylo (a ještě více je to dnes, při vysokých rychlostech) často nemožné zastavit vlak v dohledné vzdálenosti jeho řidiče.

V počátcích železnic se předpokládalo, že nejjednodušší způsob, jak zvýšit brzdnou dráhu pro strojvedoucího, bylo zavést časové intervaly mezi vlaky. Většina železnic si jako časový interval zvolila něco jako 10 minut. Povolila vlaku jet plnou rychlostí pouze 10 minut po odjezdu předchozího.

„Výpravčí“ používali červené, žluté a zelené vlajky, aby strojvedoucím ukázali, jak postupovat. Prvních pět minut po odjezdu vlaku byla vyvěšena červená vlajka. Pokud vlak dorazil po 5 minutách, strojvedoucímu se zobrazil žlutý výstražný signál. Zelený signál plné rychlosti se zobrazil až po uplynutí celých 10 minut.

„Systém časových intervalů“, když se pokoušel chránit vlaky, způsobil ve skutečnosti sám o sobě vážné problémy. V té době byly vlaky podstatně méně spolehlivé než dnes a často se mezi stanicemi porouchaly. Rovněž nebylo možné zaručit, že rychlost prvního vlaku bude dostatečná k tomu, aby se zabránilo tomu, že ho druhý vlak nedožene. Výsledkem byla řada ošklivých kolizí zezadu, protože strojvedoucí věřil, že má před sebou 10 minutovou mezeru a neměl žádné varování, že došlo ke zkrácení těchto 10 minut. Když byl čas natolik zkrácen, že viděl vlak jedoucí před ním, často neměl dostatečnou brzdnou kapacitu, aby zabránil srážce.

Dalším vážným problémem z pohledu železnice byla kapacita tratí. I když se strojvedoucí mohli spolehnout na to, že jejich vlaky nebudou neplánovaně zastavovat a celou cestu pojedou stejnou rychlostí, 10 minutový časový interval omezil počet vlaků, které mohly jezdit za hodinu (v tomto případě 6) po dané trati. Když se zjistilo, že je potřeba, aby jezdilo více vlaků, tak se postupně začaly zkracovat časové intervaly mezi vlaky. Zvýšil se počet vlaků za hodinu, ale zvýšil se i počet nehod. Odpovědí bylo zavedení pevné signalizace.

I v systému časových intervalů bylo základním pravidlem rozdělení trati na úseky a zajištění, aby byl v jednom úseku povolen pouze jeden vlak. Toto pravidlo platí i dnes. Každý úsek (nebo blok, jak se často nazývá) je chráněn pevným signálem umístěným na začátku, který se zobrazí strojvedoucímu blížícího se vlaku. Pokud je úsek volný, (není v něm žádný vlak), signál ukazuje „Pokračovat“ - obvykle zvednuté semaforové rameno; nebo zelené světlo na semaforu. V případě, že je úsek obsazen, signál ukazuje „Stop“ (spuštěné rameno semaforu, červené světlo na semaforu) a další vlak musí počkat, dokud vlak před ním nevyklidí úsek. To je základ, na kterém jsou konstruovány a provozovány všechny signalizační systémy.

Při zavedení automatizace v rámci pohybujícího se blokového systému vypočítají počítače „bezpečnou zónu“ kolem každého jedoucího vlaku, do které nesmí vstoupit žádný jiný vlak. Systém závisí na znalosti přesného umístění a rychlosti a směru každého vlaku, což je určeno kombinací několika senzorů: aktivních a pasivních značek podél trati a vlakových rychloměrů (na systémy GPS se nelze spolehnout, protože nefungují v tunelech). Nastavení pohyblivých bloků vyžaduje, aby byly pokyny předány přímo vlaku, místo aby byly použity traťové signály. To má tu výhodu, že to zvyšuje kapacitu tratí tím, že umožňuje vlakům jezdit blíže k sobě při zachování požadovaných bezpečnostních rezerv.

Detekce vlaku se týká přítomnosti nebo nepřítomnosti vlaků v definovaném úseku trati. Nejběžnějším způsobem, jak zjistit, zda je část trati obsazena, je použití kolejového obvodu. Kolejnice na obou koncích každé sekce jsou elektricky izolovány od následující sekce a na obou koncích kolejnic je na jednom konci přiváděn elektrický proud. Relé na druhém konci je spojeno s oběma kolejnicemi. Když je sekce neobsazená, cívka relé zkompletuje elektrický obvod a ten je pod napětím. Když však vlak vstoupí do úseku, zkratuje proud v kolejích a relé je bez napětí. Tato metoda výslovně nemusí však kontrolovat, zda celý vlak opustil sekci. Pokud část vlaku zůstane v úseku, kolejový obvod tuto část detekuje. Tento typ obvodu detekuje nepřítomnost vlaků, a to jak pro nastavení signalizace signálu, tak pro zajištění různých funkcí blokování - například brání v pohybu bodů v době, kdy se k nim vlak přibližuje. Elektrické obvody také dokazují, že body jsou uzamčeny ve vhodné poloze, než bude možné vyčistit signál chránící danou trasu. Na většině železnic jsou fyzické signály vydávány na trati, aby strojvedoucím oznamovaly, zda je před nimi obsazená trať, a aby zajistily dostatečný prostor mezi vlaky, který jim umožní zastavit.

Během doby se používala světelná a mechanická signalizace na trati.. V rámci signalizace trasy byl strojvedoucí informován, kterou cestou bude vlak pokračovat za každým signálem (pokud není možná pouze jedna trasa).

Aby se zabránilo dopravním nehodám způsobeným tím, že strojvedoucí nereaguje na signál, byly vyvinuty různé pomocné bezpečnostní systémy umístěné do kabiny strojvedoucího. Každý takový systém vyžaduje instalaci určitého stupně vlakového zařízení. Některé systémy zasahují pouze v případě předání signálu, že je vlak v nebezpečí (SPAD). Mezi další patří zvukové a / nebo vizuální indikace uvnitř kabiny strojvedoucího, které doplňují signály na trati. Pokud by strojvedoucí nepotvrdil varování, dojde k automatickému zabrzdění vlaku. Některé systémy působí přerušovaně (na každý signál), ale nejsofistikovanější systémy poskytují nepřetržitý dohled.

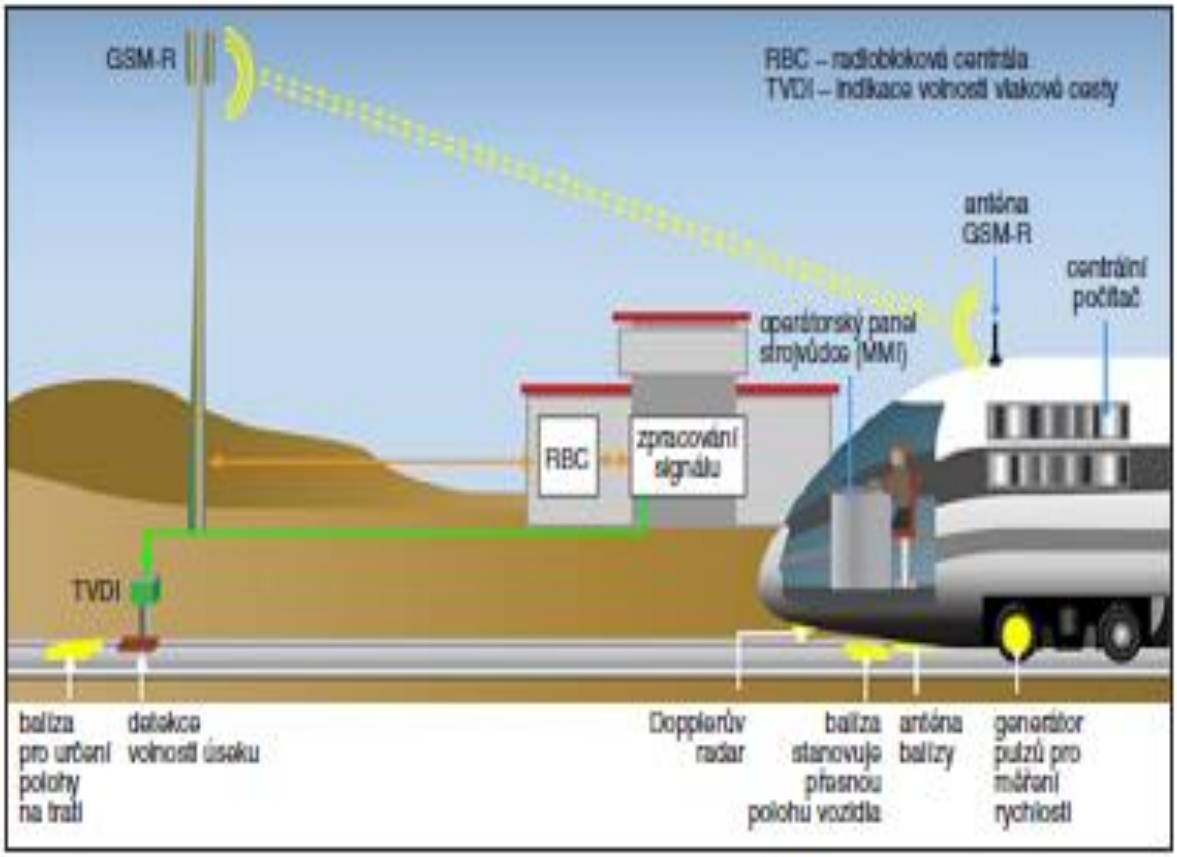
Postupně byl zaveden železniční zabezpečovací systém založený na komunikačním řízení vlaků pomocí systémů CBTC (Communications-based train control). Jde o železniční signalizační systém, který využívá telekomunikace mezi vlakovým a kolejovým zařízením pro řízení provozu a řízení infrastruktury. Prostřednictvím systémů CBTC je přesná poloha vlaku známa přesněji než u tradičních signalizačních systémů. Výsledkem je efektivnější a bezpečnější způsob řízení železničního provozu.

Jde o nepřetržitý, automatický systém využívající určení polohy vlaku s vysokým rozlišením, který je nezávislý na kolejových obvodech. Zajišťuje nepřetržitý, vysokokapacitní, obousměrný datový přenos z vlaku na trať. Vlakové a traťové procesory jsou schopné implementovat funkce automatické ochrany vlaku (ATP), jakož i volitelné funkce pro automatický provoz vlaku (ATO) a pro automatický dohled nad vlakem (ATS), jak jsou definovány ve standardu [81]. Pomocí systémů CBTC je přesná poloha

vlaku známa přesněji než u tradičních zabezpečovacích systémů. Výsledkem je efektivnější a bezpečnější způsob řízení železničního provozu.

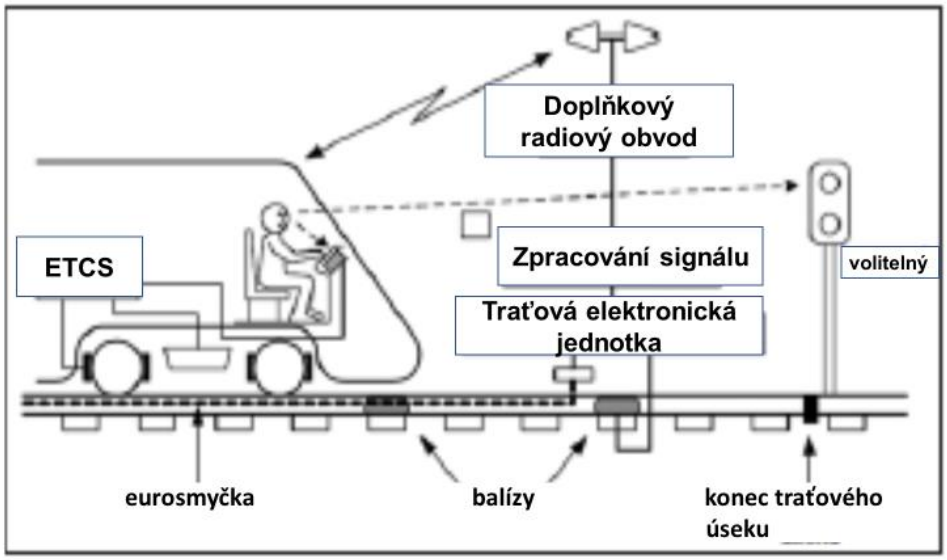
V moderních systémech CBTC vlaky průběžně počítají a sdělují svůj stav pomocí rádia do traťového zařízení distribuovaného po trati. Stav zahrnuje mimo jiné přesnou polohu, rychlost, směr jízdy a brzdnou dráhu a délku vlaku. Předmětné informace umožňují výpočet oblasti potenciálně obsazené vlakem na trati. Umožňují také traťovému zařízení definovat body na trati, do kterých nesmí vjet ostatní vlaky na stejné trati. Body jsou sdělovány ostatním vlakům a podle nich se u vlaků automaticky a průběžně upravuje jejich rychlost při zachování požadavků na bezpečnost a pohodlí cestování. Vlaky nepřetržitě přijímají informace týkající se vzdálenosti k předchozímu vlaku, a tak mohou udržovat bezpečnou vzdálenost od něho.

Informační a řídící systémy I&C u CBTC umožňují, aby se lokomotivy mohly pohybovat po celé Evropě. Obsahují informační systém ERTMS (European Rail Traffic Management System), jehož cílem je interoperabilita lokomotiv. Systém ERTMS se skládá ze dvou základních částí, evropského vlakového zabezpečovacího systému ETCS a mezinárodního systému bezdrátové komunikace GSM-R; obrázek 5. Přenos informace o návěstidlech přímo strojvedoucímu umožňuje zvýšit rychlost vlaků i zlepšit propustnost tratí při vysokém stupni zabezpečení.



Obr. 5. Prvky evropského vlakového zabezpečovacího systému ETCS a mezinárodní komunikace GMS-R; převzato z [82].

Zabezpečovací zařízení ETCS má za úkol zajistit bezpečnost vlakové dopravy a dovolit aktivně zasahovat do řízení vlaku při selhání nebo omylu strojvedoucího. Na základě přenášených informací je sledováno dodržování povelů návěstidel, což v případě ETCS znamená dodržení oprávnění k jízdě (MA – Movement Authority), které obsahuje zejména informaci o délce úseku, pro který je MA platné. Dále sleduje uvedené zabezpečovací zařízení ukazatele: – maximální traťovou rychlost v daném úseku, – maximální rychlost vlaku, – dodržení trasy vlaku, – směr jízdy, – přechodnost vlaku pro daný úsek (dodržení hmotnostního zatížení vlaku na nápravu, popř. na běžný metr), – dodržení přechodných omezení. Zařízení ETCS se skládá z traťové a vozidlové části (obrázek 6). Informace mezi nimi se vyměňují pomocí datových přenosů.



Obr. 6. Schéma zabezpečovače ETCS; zpracováno dle [82].

ETCS (European Train Control System) by měl postupně nahradit národní systémy vlakových zabezpečovačů a umožnit tak vedení vlaků po celém území Evropy bez nutnosti měnit hnací vozidla na hranicích. Od roku 2000 je tento systém zkoušen na vybraných úsecích německých, rakouských a švýcarských drah, postupně se přidávají železnice dalších států.

6.2. Zabezpečení automatického řízení provozu na železnici a koncept jejího řešení

Současný vývoj je spojený s rychlým zaváděním digitálních sítí, otevřených standardních protokolů (např. IP) a komerčního vybavení. Proto inženýři zabývající se signalizací musí zvažovat také kybernetické útoky. Zatímco výrobci zařízení pro zabezpečení zařízení si kladou otázku „jaký je dopad kybernetického zabezpečení na signalizaci“, tak provozovatelé železnic řeší otázku „jaký je dopad signalizace na kybernetické zabezpečení provozu železnice“. Proto provozovatelé železnic a ministerstvo dopravy hledají takové automatizované systémy, které jsou zabezpečené vůči rizikům v kybernetickém prostoru.

6.2.1. Charakteristika systému CBTC

V rámci automatické signalizace bloku signály signalizují, zda vlak může nebo nemůže vstoupit do bloku na základě automatické detekce vlaku. Signály mohou být také řízeny signalistou, takže poskytují indikaci postupu pouze v případě, že signalista odpovídajícím způsobem nastaví signál a blok je jasný.

Moderní systémy CBTC umožňují různé úrovně automatizace nebo stupně automatizace (GoA), jak jsou definovány a klasifikovány v IEC 62290-1 [83]. Dostupné stupně automatizace se pohybují od manuální chráněné operace, GoA 1 (obvykle se používá jako záložní provozní režim) až po plně automatizovaný provoz, GoA 4 (bezobslužný provoz vlaku, UTO). Meziproduktové provozní režimy zahrnují poloautomatický GoA 2 (poloautomatický provozní režim, STO) nebo GoA 3 bez řidiče (vlakový provoz bez strojvedoucího, DTO). Čím vyšší je GoA, tím vyšší musí být úroveň bezpečnosti, funkčnosti a výkonu. Systémy CBTC umožňují optimální využití železniční infrastruktury a dosažení maximální kapacity a minimálního odstupu mezi provozovanými vlaky při zachování bezpečnostních požadavků.

Vývoj technologie a zkušenosti získané v provozu za posledních 30 let znamenají, že moderní systémy CBTC jsou spolehlivější a méně náchylné k poruchám než starší systémy řízení vlaků. Systémy CBTC mají obvykle méně traťových zařízení a jejich diagnostické a monitorovací nástroje byly vylepšeny, což usnadňuje jejich implementaci a, co je důležitější, snadnější údržbu. Technologie CBTC se vyvíjí a využívá nejnovější techniky a komponenty k nabízení kompaktnějších systémů a jednodušších architektur. Například s příchodem moderní elektroniky bylo možné vybudovat redundanci, aby jednotlivé poruchy neměly nepříznivý dopad na provozní dostupnost. Nakonec je důležité zmínit, že systémy CBTC se ukázaly jako energeticky účinnější než tradiční ručně poháněné systémy.

6.2.2. Rizika spojená s provozem CBTC

Primárním rizikem elektronického systému řízení vlaku je, že pokud dojde k přerušení komunikačního spojení mezi kterýmkoli z vlaků, je nutné, aby celý systém nebo jeho část vstoupily do bezpečného stavu, dokud nebude problém odstraněn. V závislosti na závažnosti ztráty komunikace se tento stav může pohybovat od vozidel, která dočasně snižují rychlost, zastavují nebo pracují ve zhoršeném režimu, dokud nebude komunikace obnovena. Pokud je výpadek komunikace trvalý, musí být implementována nějaká pohotovostní operace, která může spočívat v manuálním provozu pomocí absolutního bloku nebo v nejhorším případě použitím alternativní formy dopravy.

Vysoká dostupnost systémů CBTC je zásadní pro správný provoz, zejména pokud se systémy používají ke zvýšení přepravní kapacity a ke snížení pokroku. Proto je třeba důkladně zkontrolovat mechanismy redundance a obnovy systému, aby se dosáhlo vysoké robustnosti v provozu. Se zvýšenou dostupností systému CBTC je spojena také potřeba rozsáhlého školení a pravidelného obnovování provozovatelů systému ohledně postupů obnovy . Ve skutečnosti je jedním z hlavních systémových rizik v systémech CBTC pravděpodobnost lidské chyby a nesprávné použití postupů obnovy, pokud systém nebude k dispozici.

Selhání komunikace může být způsobeno selháním zařízení, elektromagnetickým rušením, slabou silou signálu nebo nasycením komunikačního média [84]. V uvedeném případě může mít přerušení za následek použití provozní brzdy nebo nouzové brzdy, protože situační povědomí v reálném čase je kritickým

bezpečnostním požadavkem pro CBTC a pokud jsou tato přerušení dostatečně častá, může to vážně ovlivnit provoz. Proto systémy CBTC historicky poprvé zavedly systémy rádiové komunikace již v roce 2003, kdy byla požadovaná technologie dostatečně vyspělá pro kritické aplikace.

V systémech se špatnou přímou viditelností nebo omezením spektra / šířky pásma může být pro vylepšení služby vyžadován větší než očekávaný počet transpondérů. To je obvykle více problém s aplikací CBTC na stávající tranzitní systémy v tunelech, které nebyly od počátku navrženy tak, aby to podporovaly. Alternativní metodou pro zlepšení dostupnosti systému v tunelech je použití netěsného napájecího kabelu, který při vyšších počátečních nákladech (materiál + instalace) dosahuje spolehlivějšího rádiového spojení [85].

S rozvíjejícími se službami v otevřených rádiových pásmech ISM (tj. 2,4 GHz a 5,8 GHz) a potenciálním narušením kritických služeb CBTC roste tlak v mezinárodním společenství (viz zpráva 676 organizace UITP, rezervace frekvenčního spektra pro Critical Safety Applications dedicated to Urban Rail Systems) k vyhrazení kmitočtového pásma speciálně pro rádiové městské železniční systémy. Takové rozhodnutí by pomohlo standardizovat systémy CBTC na celém trhu (rostoucí poptávka většiny operátorů) a zajistit dostupnost těchto kritických systémů [85].

Protože je vyžadováno, aby systém CBTC měl vysokou dostupnost, může být poskytnuta sekundární metoda signalizace, která zajistí určitou úroveň nedegradované služby při částečné nebo úplné nedostupnosti CBTC. To je zvláště důležité pro implementace brownfields (tratě s již existujícím signalizačním systémem), kde nelze kontrolovat návrh infrastruktury a je nutná alespoň dočasná koexistence se staršími systémy [85].

V zásadě mohou být systémy CBTC navrženy s centralizovanými systémy dohledu, aby se zlepšila údržba a snížily náklady na instalaci. To nastává, pokud, existuje zvýšené riziko jediného bodu selhání, které by mohlo narušit službu v celém systému nebo lince. Systémy pevných bloků obvykle pracují s distribuovanou logikou, která je obvykle odolnější vůči takovým výpadkům. Během návrhu systému proto musí být provedena pečlivá analýza výhod a rizik dané architektury CBTC (centralizovaná vs. distribuovaná) [84,85].

Pokud se CBTC použije na systémy, které dříve fungovaly pod úplnou lidskou kontrolou s operátory pracujícími na dohled, může to ve skutečnosti vést ke snížení kapacity (i když se zvýšením bezpečnosti). Důvodem je, že CBTC pracuje s menší polohovou jistotou než lidský zrak a také s většími rezervami pro chyby, protože pro návrh jsou použity nejhorší parametry vlaku (např. Garantovaná rychlost nouzového brzdění vs. jmenovitá rychlost brzdění).

6.3. Zabezpečení systému signalizace

Signalizační systém řídí a ovládá provoz vlaku. Železniční zabezpečovací systém zahrnuje: systém řízení vlaku; zabezpečovací systém; CBTC; a centralizovaný systém monitorování návěstidel.

1. Mezinárodní norma IEC 61508 [5] vydaná Mezinárodní komisí pro elektroniku a elektrotechniku v roce 2000, která se týká elektrické / elektronické / funkční bezpečnosti programovatelných elektronických systémů souvisejících s bezpečností. Elektrický / elektronický / programovatelný elektronický systém (E / E / PE)

obsahuje elektrická zařízení, elektronická zařízení a programovatelná elektronická zařízení založená na elektrické / elektronické / programovatelné elektronické technologii. Elektrická zařízení označují motorová zařízení, elektronická zařízení označují pevná a neprogramovatelná elektronická zařízení a programovatelná elektronická zařízení označují elektronická zařízení založená na výpočetní technice. Systémy lze ovládat, chránit a kontrolovat na základě jednoho nebo více programovatelných elektronických zařízení. Skládá se ze všech komponent systému, jako je napájení, snímače, další vstupní zařízení, datové kanály, komunikační kanály a další akční členy i výstupní zařízení. Bezpečnostní systém je systém, který využívá bezpečnostní technologie a opatření ke snížení rizika k provedení požadovaných bezpečnostních funkcí k zajištění bezpečného stavu řídicího zařízení. Jakmile dojde k poruše elektrických / elektronických / programovatelných elektronických bezpečnostních systémů, může to ovlivnit bezpečnost lidí a životního prostředí.

2. Normy železničního signálu formulované CENELEC, jejichž cílem je zabezpečovací systém řízený počítačem jsou:
   - EN50126 [16] Železniční aplikace: specifikace a popis spolehlivosti, použitelnosti, udržovatelnosti a bezpečnosti (RAMS),
   - EN50128 [18] Železniční aplikace: software pro železniční řídicí a ochranné systémy,
   - EN50l29 [17] Železniční aplikace: elektronický systém týkající se bezpečnosti návěstidel,
   - EN50129-1 [17] Železniční aplikace: komunikační, signální a zpracovatelský systém (první část); bezpečná komunikace v uzavřeném přenosovém systému,
   - EN50129-2 [17] Železniční aplikace: komunikační, signální a zpracovatelský systém (druhá část); bezpečná komunikace v otevřeném přenosovém systému.

Vzhledem k tomu, že železniční signál používá mnoho elektronických zařízení, vypracovala ministerstva železnic národní normy, které se staly *d*ůležitějšími bezpečnostními podmínkami, které je třeba dodržovat při používání elektronických součástek v technikách železniční signalizace . Norma rovněž přijímá hlavní bezpečnostní podmínky pro používání elektronických součástek prostřednictvím železniční a signální technologie Mezinárodní unie železnic (UIC). Hlavní obsah tvoří pojmy, hodnocení bezpečnosti železničního zabezpečovacího zařízení a hlavní zásady pro používání elektronických součástek v zabezpečovacím zařízení.

6.3.1. ETCS

V současné době používají evropské železniční správy asi 20 druhů vzájemně neslučitelných vlakových zabezpečovačů, které plní současné požadavky na zabezpečení jízdy vlaků a přenosů návěstí pouze částečně. Nikoli různost napájecích systémů, která rovněž komplikuje přeshraniční železniční dopravu, ale především různost vlakových zabezpečovačů brání stavbě univerzální evropské lokomotivy. Na žádnou lokomotivu se totiž všechny zabezpečovače se svými snímači nevejdou. Má-li železnice uspět v konkurenci silniční dopravy, je nutné snižovat náklady na přepravu a zkracovat přepravní doby. Jednou z překážek tohoto postupu je nutnost výměny hnacích vozidel na hranicích států. Ačkoli se v mezinárodní dopravě již používají hnací vozidla vybavená několika národními zabezpečovači, je toto řešení pouze částečné. Jedním z

předpokladů zabezpečení dostatečně spolehlivého a bezpečného železničního provozu je použití vhodného vlakového zabezpečovacího zařízení.

Evropská komise iniciovala v roce 1989 projekt, který analyzoval problémy v oblasti zabezpečení a řízení jízd vlaků. V roce 1990 z popudu Mezinárodní železniční unie (UIC) sestavil Evropský železniční výzkumný ústav (ERRI) skupinu expertů A200, jejíž cílem bylo stanovit základní požadavky na jednotný evropský zabezpečovač. V roce 1995 definovala Evropská komise globální strategii dalšího vývoje ERTMS (European Rail Traffic Management System) / ETCS, jehož zásady byly zakotveny ve směrnici 96/48 „Interoperabilita evropských vysokorychlostních železničních systémů“ [86], spolu s rádiovým komunikačním systémem GMS-R (Global System for Mobile Communication-Railways). UIC prostřednictvím ERRI vypracovala konkrétní podmínky pro ETCS a spolek šesti evropských železničních správ spolu se svazem evropských výrobců zabezpečovacích zařízení UNISIG je dále rozvinut.

ETCS (European Train Control System) [87] je zkratka pro evropský vlakový zabezpečovaní systém. Je jednou ze součástí ERTMS. Měl by postupně nahradit cca 20 různých národních systémů vlakových zabezpečovačů a tak umožnit vedení vlaků po celém území Evropy bez nutnosti výměn hnacích vozidel. Od roku 1999 započaly testy ETCS u některých železnic. Od roku 2001 platí evropská směrnice 2001/16/ES [88], která stanovuje zásady zavádění ETCS pro konvenční tratě.

Cílem zavedení ETCS není pouze spojení řízení a zabezpečení jízdy vlaků a převedení systémů na současnou úroveň techniky, ale také: snížení nákladů na údržbu a provoz traťové části; odstranění množství národních zabezpečovacích systémů, a tím umožnění interoperability vozidel na evropských železnicích; zvýšení propustnosti tratí; zvýšení traťových rychlostí. Hlavním úkolem ETCS stejně jako každého jiného vlakového zabezpečovače je zajištění bezpečnosti vlakové dopravy a aktivní zásah do řízení vlaku v případě selhání nebo omylu strojvedoucího. Na základě přenášených informací kromě dodržování návěstí, respektive v případě ETCS oprávnění k jízdě (MA - movement authority), které obsahuje zejména informaci o délce úseku, pro který je MA platné, a o maximální rychlosti v daném úseku vyplývající z postavené jízdní cesty, sleduje tento zabezpečovač ještě další ukazatele: maximální traťovou rychlost v daném úseku; maximální rychlost vlaku; dodržení trasy vlaku; směr jízdy; přechodnost vlaku pro daný úsek; dodržení přechodných omezení.

Zařízení ETCS se skládá z traťové a vozidlové části [87]. Informace mezi nimi probíhají v podobě datových přenosů. Traťovou část tvoří: Eurobalíza; traťová elektronická jednotka LEU (Lineside Electronic Unit) - pouze u přepínatelných balíz; Eurosmyčka (Euroloop); Radiobloková centrála RBC (Radio Block Centre); Doplňkový rádiový obvod (Radio in-fill unit).

Eurobalíza [87] je základním prostředkem přenosu informací na vozidlo. Používá se jako pevná nebo přepínatelná. Umísťuje se v ose koleje. Je napájena bezkontaktně z vozidla při jeho průjezdu nad balízou. Délka úseku pro kontakt je cca 1 m. Pro rozlišení směru jízdy nad balízou se seskupují obvykle do tzv. balízových skupin. LEU slouží k přenosu informací ze stávajícího staničního nebo traťového zabezpečovacího zařízení (návěstidel) do přepínatelné balízy. Euroloop umožňuje liniový přenos informace o postavení návěstidla, resp. o změně jeho návěsti tam, kde je to účelné - například v místech pravidelných zastavení. RBC je procesorový elektronický systém, který na základě informací získaných z pevné části zabezpečovacího zařízení a z informací z jednotlivých vozidel vypracovává a prostřednictvím sítě GSM-R vysílá zprávy s MA

(Movement Authority = Oprávnění k jízdě). Doplňkový rádiový obvod podobně jako Euroloop přenáší informace o postavení nejbližšího návěstidla.

Vozidlovou část [87] tvoří: centrální počítač EVC (European Vital Computer); záznamová jednotka JRU (Juridical Recording Unit); zobrazovací jednotka DMI (Driver-Machine Interface); přenosový modul balízy BTM (Balise Transmission Module); a odometrie. Centrální počítač je jádrem celého systému, vyhodnocuje přijaté údaje a vypočítává brzdné křivky, dohlíží na jízdu vlaku a v případě potřeby aktivuje brzdy. JRU slouží k záznamu všech zadaných informací z provozu, její konstrukce vyžaduje vysokou odolnost pro případ mimořádné události. DMI je tvořena obvykle dotykovou obrazovkou, zobrazuje potřebná data (rychlosti, délku povolení k jízdě, průběh rychlostního profilu, režim atd.). BTM vysílá nepřetržitě signál o kmitočtu 27 MHz k napájení balíz, přijímá telegramy z balíz v pásmech 3,9 a 4,5 MHz. Odometrie přesné měření rychlosti a ujeté vzdálenosti je naprosto nezbytná pro správnou a bezpečnou funkci zařízení. ETCS vyžaduje alespoň tři nezávislé způsoby měření. K měření rychlosti se používají snímače otáček na nápravách doplněné o Dopplerovský radar.

Zabezpečovač ETCS [87] je tvořen oddělenými stavebními prvky, které svými kombinacemi a zapojením do stávajícího zabezpečovacího zařízení umožňují dosažení různých úrovní funkce tohoto systému. Aplikační úrovně se značí písmenem L (z anglického Level). Rozlišují se:

ETCS L0 označuje vozidlo s mobilní částí ETCS, které se pohybuje po tratích bez traťové části jakéhokoliv vlakového zabezpečovače. Zařízení tak hlídá pouze maximální rychlost.

ETCS LNTC (dříve LSTM) označuje vozidlo s mobilní částí ETCS, které se pohybuje po tratích vybavených národním vlakovým zabezpečovačem. Zařízení ETCS z něj přijímá informace prostřednictvím STM (Specific Transmission Module).

ETCS L1 označuje zařízení, které pracuje na trati vybavené přepínatelnými balízami. Jeho zařízení pracuje podobně jako bodový vlakový zabezpečovač, avšak s tím rozdílem, že balízy ještě předávají informace o následujícím traťovém úseku, což umožňuje průběžně sledovat nejvyšší dovolenou rychlost vlaku. K přenosu návěstí může být kromě balíz ještě použito smyček a rádiových obvodů.

ETCS L2 označuje zařízení, které pracuje s pevnými balízami, které slouží jako referenční bod, k němuž jsou vztaženy informace týkající se polohy předávané vozidlu ze stacionární části systému reprezentované zejména radioblokovou centrálou RBC. Povolení k jízdě (Movement Authority, MA) získává vlak tedy přímo z RBC prostřednictvím GSM-R. Vozidlová část ETCS získává informace o ujeté vzdálenosti od poslední balízy průběžně prostřednictvím impulsních snímačů otáček na nápravách a Dopplerova radaru na spodku vozidla. Návěstidla pro tuto aplikační úroveň nejsou potřeba, avšak zjišťování volnosti úseků se děje konvenčními prostředky (kolejovými obvody, počítači náprav).

ETCS L3 na rozdíl od L2 dělá změnu lokalizace a kontroly celistvosti vlaku průběžně rádiovými prostředky. Tato aplikační úroveň umožňuje zrušení traťových oddílů a jejich nahrazení „pohyblivým oddílem“. To znamená, že volnost vlakové cesty v délce zábrzdné vzdálenosti pro daný úsek, druh a rychlost vlaku se sleduje průběžně, což umožní zvýšit propustnost tratí. Interoperabilní a bezpečná detekce celistvosti vlaku pro soupravy se svěšenými vozy (nikoliv pro ucelené jednotky) je zatím ve stádiu výzkumů, což brání zavedení této aplikační úrovně do provozu.

ETCS LC je levnější variantou (Low Cost) pro vedlejší tratě. Systém by měl pracovat stejně jako L3, jen počet balíz by byl minimalizován. Balízy by byly využity jen v dopravních obvodech s kolejovým rozvětvením, v úvahu připadá i satelitní navigace pro lokalizaci polohy vlaku na trati.

ETCS může pracovat v různých režimech, tabulka 7. Použití konkrétního režimu musí být umožněno traťovou částí.

Tabulka 7. Přehled režimů ETCS; převzato z [87].

Zkratka	**Název**	**Použití v aplikační úrovni**	**Popis**
FS	Full Supervision	1, 2, 3	Vlak je veden v režimu ETCS
LS	Limited Supervision	1	Vlak je zabezpečen ETCS jako u bodového zabezpečovače; plánováno, tento režim není součástí specifikace SRS 2.3.0
OS	On Sight	1, 2, 3	Vlak pod dohledem ETCS, jízda dle rozhledu
SR	Staff Responsible	1, 2, 3	Strojvedoucí je odpovědný za vedení vlaku, ve většině zemí nesmí v tomto režimu překročit rychlost 30 km/h, což ETCS hlídá
SH	Shunting	0, 1, 2, 3	Posun. ETCS ve většině zemí nedovolí překročit rychlost 30 km/h
UN	Unfitted	0	Vlak není zabezpečen ETCS
SL	Sleeping	0, STM, 1, 2, 3	Lokomotiva s EVC je připojena k jiné lokomotivě s EVC, který přebírá vedení vlaku.
SB	Stand By	0, STM, 1, 2, 3	Vlak je po zapnutí v režimu Stand By
TR	Trip	1, 2, 3	Aktivováno nouzové brzdění až do zastavení vlaku a potvrzení strojvedoucím.
PT	Post Trip	1, 2, 3	Režim po vyloučení režimu Trip strojvedoucím, avšak stále bez oprávnění k další jízdě.
SF	System Failure	0, STM, 1, 2, 3	Vnitřní chyba zařízení, aktivováno nouzové brzdění

IS	Isolation	0, STM, 1, 2, 3	EVC nemá spojení s dalšími zařízeními
NP	No Power	0, STM, 1, 2, 3	EVC je vypnut
NL	Non Leading	0, STM, 1, 2, 3	lokomotiva je připojena k jiné lokomotivě, jejíž EVC převzal vedení vlaku
SE	STM Euro-pean	STM	traťová část národního zabezpečovače přenáší pomocí STM všechny potřebné údaje, jako např. profil trati, do EVC, EVC přejímá funkci zabezpečovače (srovnatelné s režimem FS)
SN	STM National	STM	traťová část národního zabezpečovače přenáší pouze obvyklé návěsti, vozidlová část ETCS pomocí modulu STM kopíruje funkci vozidlové části národního zabezpe-čovače
RV	Reversing	1, 2, 3	Vlak smí jet po dané trase v opačném směru - například couvnout za projeté ná-věstidlo

První systémy ETCS zaváděné do provozu se zakládají na specifikaci UNISIG SRS verze 2.2.2. Současně se však objevily požadavky na změny a rozšíření těchto specifikací. Problémem jsou různé požadavky evropských drah vyplývající z odlišných provozních potřeb a předpisů. Aktuálně platné jsou současně jak specifikace verze Baseline 2 (SRS verze 2.3.0d), tak i první údržbové vydání Baseline 3 (SRS verze 3.4.0). Intenzivně se pracuje na druhém vydání Baseline 3 (SRS verze 3.5.0).

Nevýhody ETCS jsou:

1. ETCS aplikační úrovně 1 bez doplňkových prostředků (Euroloop, In-fill radio) neumožňuje dosažení takové propustnosti tratí, jako některé moderní národní systémy - liniový zabezpečovač CIR-ELKE2. Důvodem je právě použití pouze bodového přenosu informací mezi traťovou a vozidlovou částí systému.
2. V průběhu zavádění musí být vozidla nebo tratě vybaveny oběma systémy (ETCS i národním vlakovým zabezpečovačem), což zvyšuje náklady. Tato doba nezbytné koexistence obou systémů se označuje jako migrační období.
3. Je zřejmé, že kapacita kanálů sítě GSM-R pro aplikační úroveň 2 v oblastech železničních uzlů a seřaďovacích nádraží nestačí. Zde musí být instalována aplikační úroveň 1.

V roce 1999 bylo zařízení ETCS dle specifikací UIC úspěšně vyzkoušeno na trase Vídeň–Budapešť, poté následovaly další zkušební instalace v různě modifikovaných verzích:

- 2000: FS Firenze Campo di Marte–Arezzo (ETCS Level 1)
- 2000: SNCF Marles-en-Brie–Tournan (ETCS Level 1)

- 2001: ÖBB Wien–Nickelsdorf (ETCS Level 1, pravidelný provoz)
- 2002: SBB Zofingen–Sempach (ETCS Level 2; v současnosti odstraněno)
- 2004: SBB Neubaustrecke Mattstetten–Rothrist ETCS Level 2; Plánované nasazení do pravidelného provozu v prosinci 2004 se nezdařilo. 2. července 2006 započal zkušební provoz v nočních hodinách, vlaky po 21.30 h jezdí rychlostí 160 km/h. Od konce roku 2007 má na této trati jezdit denně 240 vlaků rychlostí do 200 km/h
- 2005: DB Halle (Saale)/Leipzig–Jüterbog–Berlin (ETCS Level 2); První pravidelný vlak DB v režimu ETCS byl 5. prosince 2005 IC 2519/2518
- 2006: RENFE Madrid–Lleida (ETCS Level 1; první komerční využití pro rychlost 250 km/h)
- 2007: BLS Lötschberg-Basislinie (ETCS Level 2; pravidelný provoz)
- 2010: ŽSR Svätý Jur–Nové Mesto nad Váhom (ETCS Level 1, pravidelný provoz)

Zástupci ČSD, resp. ČD [87] se účastnili prací na vývoji evropského zabezpečovacího zařízení již od samého počátku. Zároveň byly zastaveny práce na vývoji přídavného bodového systému ke stávajícímu liniovému zabezpečovači. ČD již v roce 1995 předložily přípravnou studii pro pilotní projekt ETCS na trase Drážďany-Praha, avšak česká strana nedokázala dostatečně pružně reagovat na administrativní požadavky orgánů EU a možnost spolufinancování z programu PHARE, takže byl tento projekt časem vyřazen a nahrazen trasou Drážďany-Lipsko.

V letech 2001-2002 zpracovala TÚDC (Technická ústředna dopravní cesty) na základě specifikace VÚŽ (Výzkumný ústav železniční) přípravnou dokumentaci pro pilotní projekt v úseku Poříčany-Kolín. V lednu 2002 byl ustaven Řídící tým ERTMS Českých drah s.r.o. V dubnu 2004 bylo vyhlášeno výběrové řízení na realizaci uvedeného pilotního projektu. S vítězem byla koncem roku 2004 zahájena jednání, v dubnu 2005 byla podepsána smlouva a 1. 7. 2005 byla zahájena realizace. Lhůta činí 40 měsíců, z toho 12 měsíců projekt, 15 měsíců stavba a 13 měsíců testování. Do roku 2011 pak měl být ETCS zaveden v trasách Děčín st. hranice - Praha - Česká Třebová - Brno - Břeclav st. hranice, Lanžhot st. hranice - Břeclav - Přerov - Ostrava - Petrovice u Karviné st. hranice a Česká Třebová - Přerov, resp. Prosenice. Do roku 2013 se měly připojit ještě úseky Praha - Plzeň - Cheb st. hranice a Praha - České Budějovice - Horní Dvořiště státní hranice.

Z vozidel ČD jsou dosud vybavena ETCS pouze jednotky ř. 680 a kromě toho i lokomotiva 124.601 VÚŽ. Od srpna 2008 je ETCS vybavena lokomotiva 362.166 a zařízení je namontováno na 151.008 a na jednotce 471.042.

Od roku 2005 jsou v České republice v souladu s Národním implementačním plánem ERTMS (European Rail Traffic Management System) zaváděny traťové komponenty systému ERTMS, a to již zmíněné ECTS a GSM-R (Global System for Mobile Communications – Railway) aplikační úrovně 2 (Level 2 vyhovující základní normě 3 – Baseline 3) státní organizací Správa železniční dopravní cesty [87]. Dle tohoto plánu implementace, resp. dle Prováděcího nařízení komise (EU) 2017/6, o evropském prováděcím plánu evropského systému řízení železničního provozu, dojde k postupnému vybavení všech hlavních železničních koridorů TEN-T (Trans-European Transport Networks) v ČR traťovými komponenty systému ERTMS [87].

V rámci realizace projektu se prvky ERTMS, konkrétně palubními komponenty systému ETCS vybavuje 99 vozidel společnosti ČD, a.s., operujících na koridorech TEN-T uvnitř ČR, které se po instalaci ETCS stanou plně interoperabilní a vhodné také pro hladkou mezinárodní spolupráci na koridorech TEN-T, resp. CNC (Core Network Corridors – koridorech hlavní sítě).

Směrnice (EU) 2016/797 [89] definuje subsystémy, ať už strukturální nebo funkční, tvořící součást železničního systému Evropské unie. Specifikace ERTMS jsou spravovány podle ERA Change Control Management (CCM). ERA je odpovědná za identifikaci všech chyb, které by potenciálně nemohly systému umožnit poskytovat běžnou službu, a co nejdříve zveřejnit příslušná řešení k jejich nápravě, jakož i vyhodnocení jejich dopadu na kompatibilitu a stabilitu stávajícího nasazení ERTMS .

6.3.2. Evropská legislativa pro zabezpečení provozu vlaků

Systém signalizace železnice je technický systém, jehož cílem je zajistit bezpečný provoz železnice; zahrnuje lidi, procesy a zařízení. Při použití IT je zranitelný riziky, které mají původ v kyber prostoru. Pro zabezpečení sítě se používají např.: firewalls, ověřovací moduly a šifrování a design sítě (architektura, implementace procesů). Úkolem CSMS je udržovat kybernetické zabezpečení železnice na přijatelné úrovni. V systému řízení bezpečnosti SMS musí být zabudována schopnost detekce realizace rizik a systém odezvy na ně [38,39].

Inženýr odpovědný za systém signalizace odpovídá za bezpečný systém signalizace, musí prokázat jeho bezpečnost, limity systémů vztažených k bezpečnosti a vnější faktory, které ovlivňují bezpečnost. Proto hodnocení rizika je součástí řízení kybernetického zabezpečení.

Jsou zdroje rizik, které mají dopad na bezpečnost železnice a nemají dopad na zabezpečení a obráceně. Požár v řídícím centru má dopad na zabezpečení. Porucha v zašifrování kritické komunikace nebo nezamčené dveře k zařízením signalizace mají dopad na bezpečnost. Když systém není zabezpečen, tak nemůže být bezpečný.

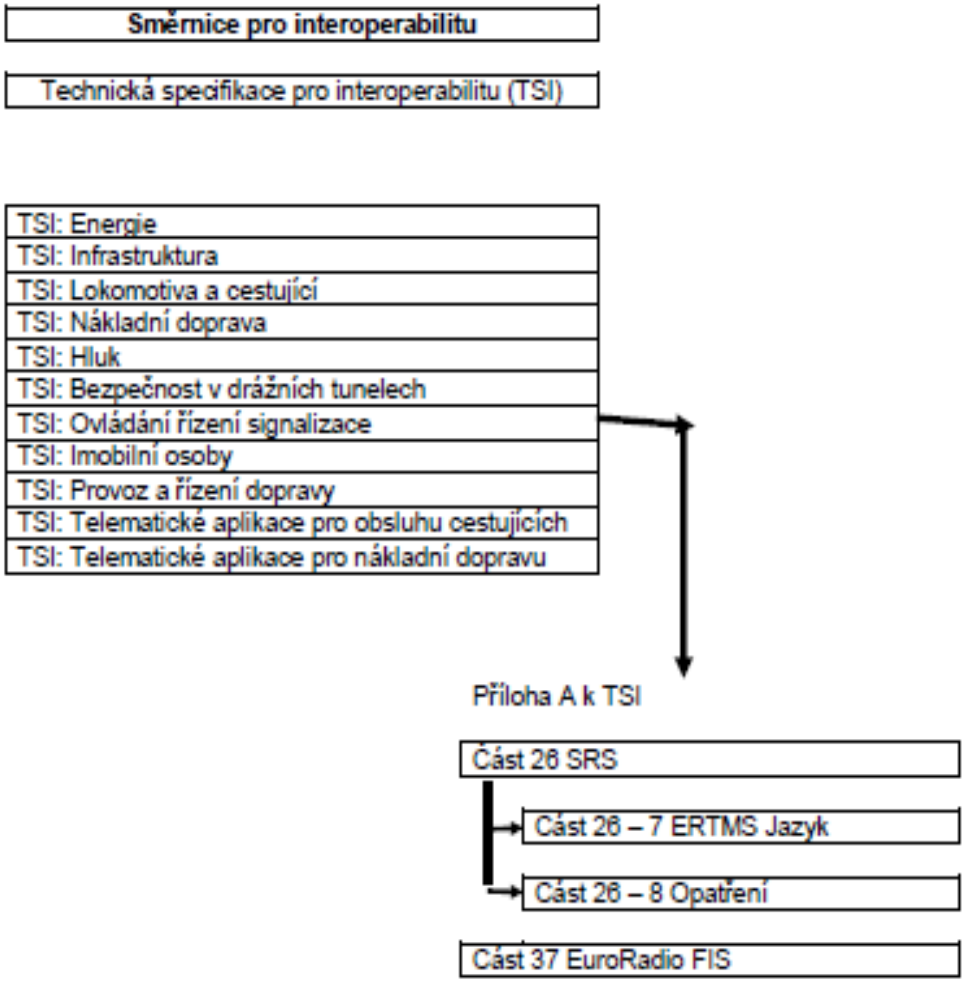
V praxi jsou dva odlišné procesy spojené se zacílením analýzy rizik:

- dosažení SIL (safety integrity level),
- dosažení SL (security level).

Inženýr odpovědný za systém signalizace odpovídá za bezpečný provozní výkon systému signalizace. Inženýr odpovědný za zabezpečení odpovídá za identifikaci zdrojů rizik pro zabezpečení, vyhodnocení velikosti těchto rizik a za návrh efektivních protiopatření. Základem je vložení kybernetického zabezpečení do systémů, které jsou kritické pro bezpečnost.

Je si třeba uvědomit, že kybernetické zabezpečení a signalizace na železnici jsou dva odlišné světy a každý svět má své experty. Problém je jejich spolupráce, tak jako je tomu u jiných technických děl [38,39]. Pro odstranění nedostatku je důležité najít způsob interakce mezi inženýrem odpovědným za signalizační systém a inženýrem pro zabezpečení železnice.

EU používá normu Technical Standards for Interoperability (TSI) [90]. Části 26 a 37 definují opatření, které přispívají ke kybernetickému zabezpečení. Jeho struktura je uvedena na obrázku 7.



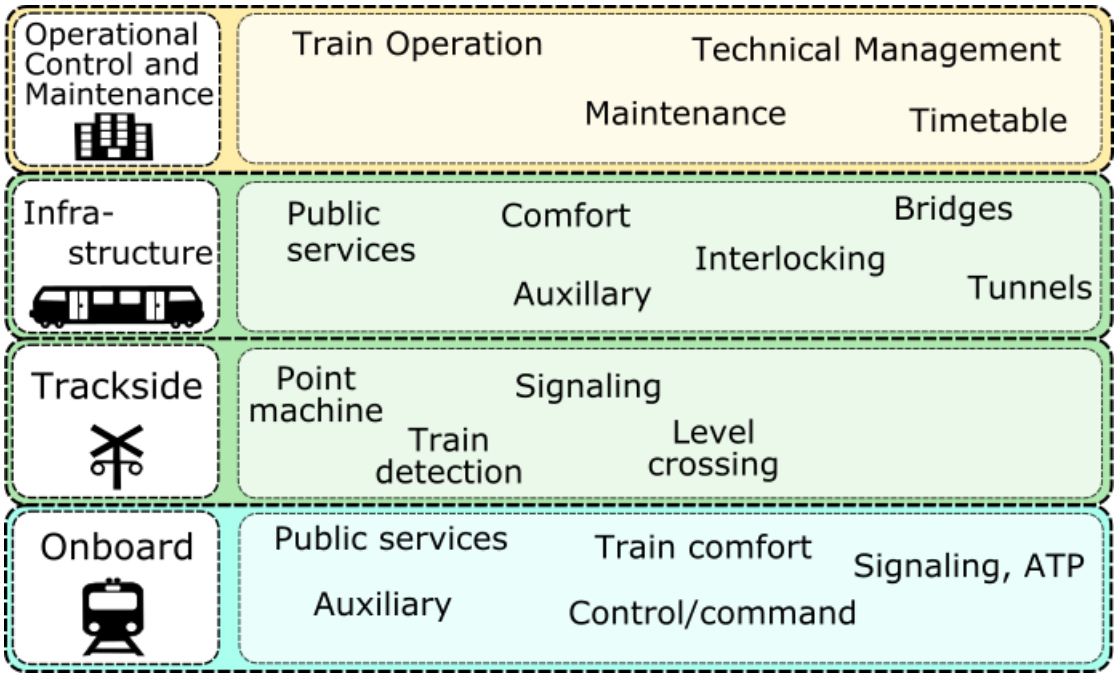
Obr. 7. Struktura interoperability; převzato z [90].

EU má od r. 2016 směrnici, která obsahuje opatření k zajištění úrovně bezpečnosti sítí v Evropě [91] a nařízení o kybernetickém zabezpečení [92] bylo v EU přijato v roce 2019. Tím se vytvořila agentura pro zabezpečení ENISA. Pro hodnocení rizik pro potřeby zabezpečení informací platí ISO 27005 [93].

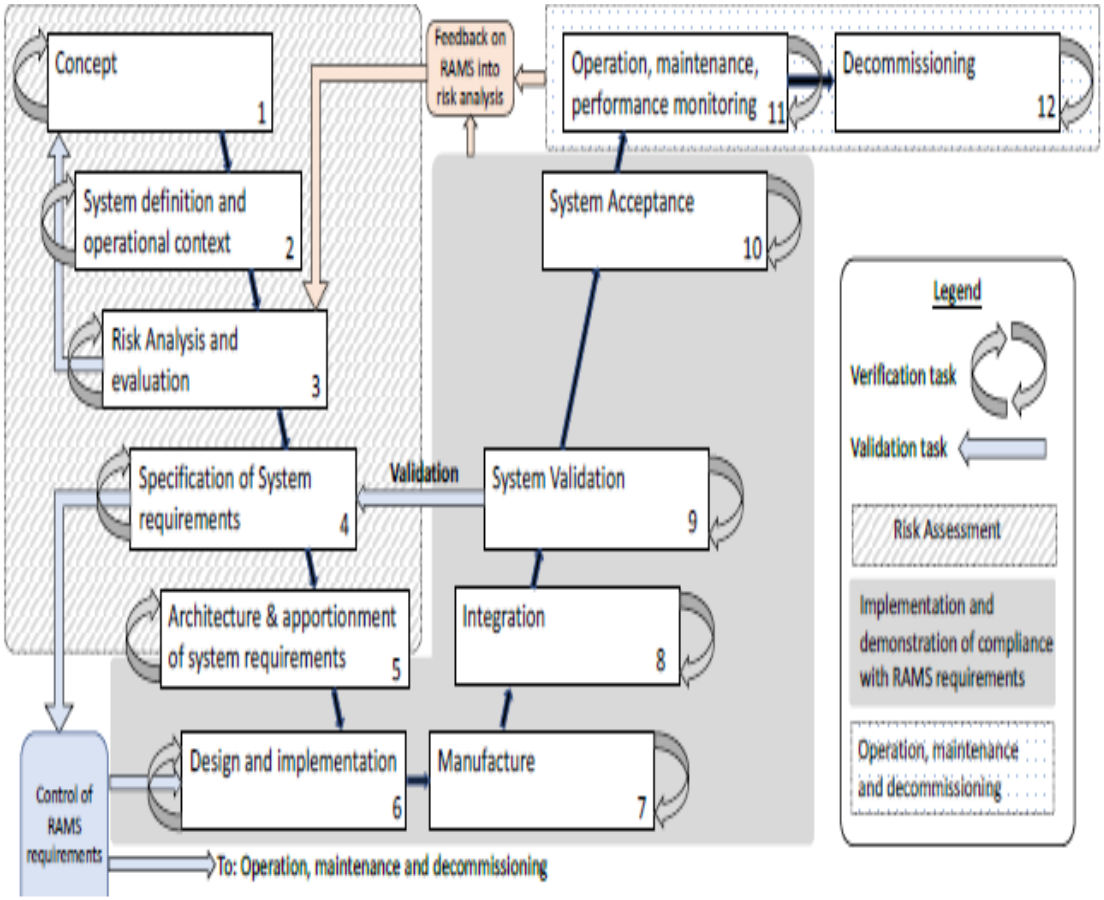
Převedení systémového pohledu standardu IEC 62443 [7] do oblasti železnice, je cílem technické specifikace TS 50701 [94]. Jejím cílem je vytvářet nástroj pro všechny zainteresované strany v oblasti železniční dopravy pro odpovídající implementaci požadavků definovaných v normě IEC 62443, obrázek 8 [94].

EN 50126 [16] definuje životnost systémů signalizace železnice, tj. proces RAMS, a to od konceptu přes provoz až po ukončení provozu, obrázek 9.

EN 50129 [17] poskytuje požadavky pro řízení procesu dodání bezpečnosti. Nespecifikuje však přijatelné bezpečné technické řešení. Definuje požadavky pro řízení kvality a řízení bezpečnosti při vývoji systémů pro signalizaci, které používají elektronické nebo procesní systémy. QM zajišťuje, že procesy jsou aplikovány a dokumentovány. Řízení bezpečnosti zajišťuje, že správní procesy jsou aplikovány ve stanovené fázi vývoje systému a ve vhodné struktuře režimu.

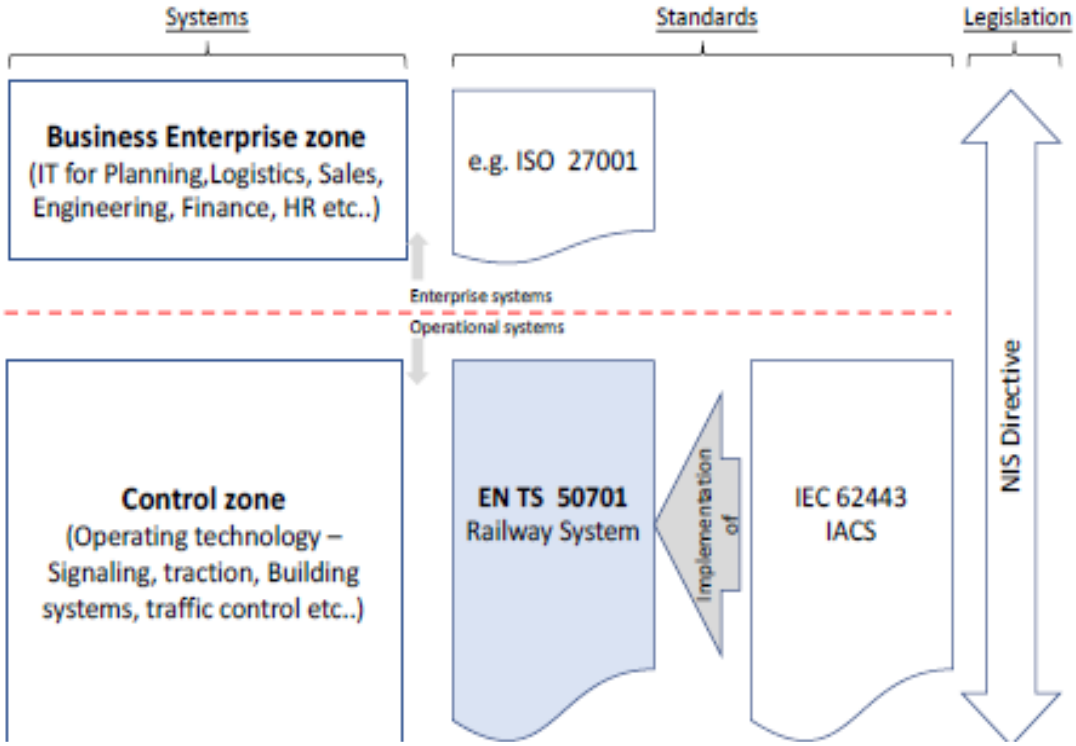


Obr. 8. Jednotlivé oblasti železniční dopravy a jejich zastoupení v kybernetickém prostoru železnice [94].



Obr. 9. Proces RAMS dle [16].

TS 50701 [94] je aplikace IEC 62443 pro železnici. Ukazuje, jak zavést požadavky na kybernetické zabezpečení na železnici, obrázek 10. Standard TS 50701 [94] pro systém železnice vyvíjený a modernizovaný na základě analýza rizik ohrožujících kybernetické zabezpečení; ISO 27001 [67] se zabývá systémem řízení zabezpečení informací a směrnice EU 2016/1148 – NIS directive [91] se věnuje zabezpečení sítí a informačních systémů.



Obr. 10. Vztah mezi standardem [89] a dalšími standardy; převzato z [94].

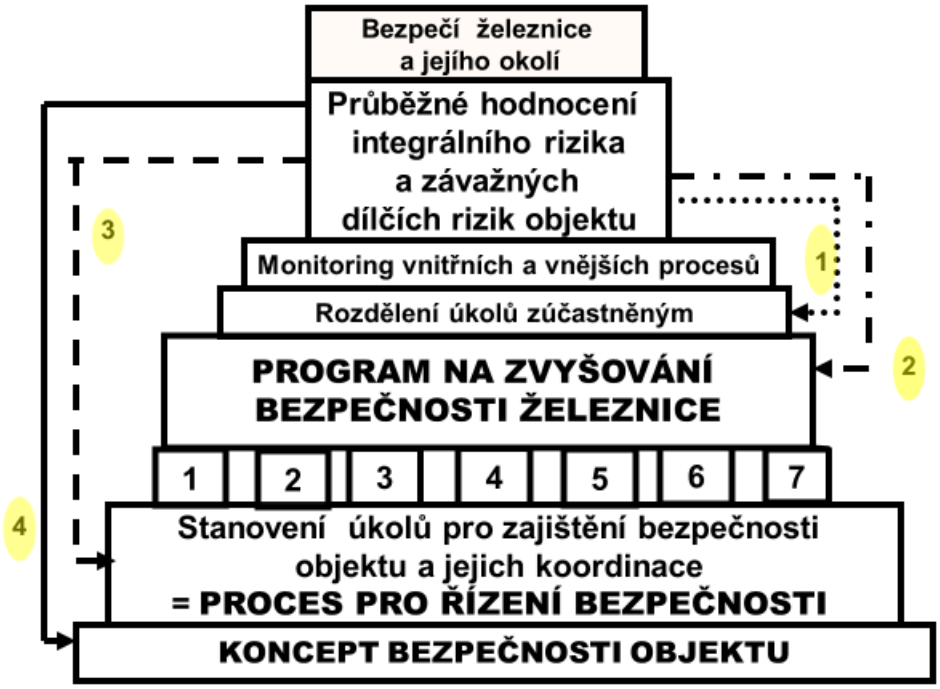
6.3.3. Koncept pro zabezpečení řízení vlaků

Železnice je složitý socio-kyber-fyzický systém s vysokým počtem různých propojení. Podle projektu všechny komponenty a propojení mají své limity, které jsou nastaveny na určité podmínky tak, aby společně plnily zadaný cíl (tj. aby byly interoperabilní). Jelikož v důsledku dynamického vývoje světa se podmínky mění, tak se mění i podmínky pro interoperabilitu. Proto bezpečnost železnice se mění v závislosti na dále se vyvíjejících podmínkách.

V souladu s požadavky OECD [95] a s výsledky pro technická díla [38,39], železnice musí mít program pro řízení bezpečnosti železnice, který je založen na řízení rizik, a to od projektování, přes výstavbu až po provoz [38,39], dále též údržbu, obnovu, kompletaci a inovaci. Proto z důvodu důležitosti role kybernetické infrastruktury spojené s automatizovaným systémem řízení musí SMS také sledovat kybernetické zabezpečení a obsahovat CSMS (kybernetické zabezpečení systému řízení bezpečnosti); tj. systém SMS na obrázku 2 musí být doplněn o další proces, který zajišťuje kybernetické zabezpečení - obrázek 11.

Hlavním cílem zabezpečení drážní infrastruktury při automatickém řízení je, aby instrukce pro systémy ovládající provoz vlaků byly jasné a přesné, tj. aby nebyly

ovlivněny jevy, které je zkreslí. Proto byly dříve na železnici používány signalizační systémy, které byly uzavřené a patentované.



Obr. 11. Model řízení bezpečnosti železnice s automatizovaným řízením v čase. Procesy: 1- koncepce a řízení; 2 - administrativní postupy; 3 - technické procesy; 4 - vnější spolupráce; 5 - nouzová připravenost; 6 - dokumentace a šetření havárií; 7- kybernetické zabezpečení. Zpětné vazby: 1-4.

Dle práce [96] je třeba vytvořit pravidla pro spolupráci expertů z oblastí zabezpečení a signalizace, což souhlasí s doporučeními v pracích [38,39]. V práci [96] je na základě kritické analýzy problémů obou oblastí navrženo 14 pravidel pro spolupráci expertů. Tabulka 8 obsahuje vodítka pro spolupráci uvedené v citované práci a doplněné o poznatky z [39].

Tabulka 8. Způsoby zajištění spolupráce mezi inženýry, kteří odpovídají na železnici za signalizaci a za kybernetické zabezpečení.

Kritická oblast	**Vodítko pro spolupráci**
Systém ochrany	1. Kybernetické zabezpečení by mělo směřovat k ochraně systémů železnice. Aby se dosáhlo komplexního řešení kybernetické bezpečnosti systému signalizace, je nutné ustanovit řízení kybernetického zabezpečení celé železnice a signalizaci do něho včlenit. - ISO 27001 [67]

	Vyhodnocení rizik ukazuje, že je velké množství rizik, které ohrožují zabezpečení systému signalizace. Příčiny rizik jsou uvnitř systému signalizace, vně i na rozhraní.
Odpovědnost	2. Jedna osoba musí být odpovědná za kybernetické zabezpečení celé železnice (a to není inženýr odpovědný za signalizaci). 3. Inženýr odpovědný za signalizaci odpovídá za systém signalizace. EN 51029 [17] 4. Interakce mezi signalizací a oblastí zabezpečení musí být řešeny spoluprací, při které musí být jasně stanoveny odpovědnosti - TS 50701 [94] a způsoby řešení konfliktů [39].
Systém řízení	5. Systém řízení kybernetického zabezpečení (CSMS – Cyber Security Management System) musí být založen na řízení rizik. - IEC 62443-2-1 [7] Požadavek se vztahuje na výrobce a údržbu konsolidovaného registru rizik pro celou železnici. Za systém řízení bezpečnosti (Safety management systém – SMS) CSMS odpovídá inženýr odpovědný za signalizaci. – EN 51029 [97] 6. Musí se zavést soubor opatření, který zahrnuje 4 dimenze kybernetického zabezpečení: zabezpečení sítě; podpora od zpravodajských služeb u incidentů; CSMS; a řízení celé železnice.
Zabezpečovací opatření a jejich implementace	7. Pro opatření pro zabezpečení sítě platí: - bezpečnost nesmí být kompromisem, - zajištění zabezpečení sítě se musí vztahovat na železnici jako celek, - tam, kde nejsou sektorové a průmyslové standardy, tam musí být vytvořeny a zavedeny jasné instrukce, - při výběru opatření na zajištění sítě je třeba zvažovat požadavky údržby a oprav (záplatování je nežádoucí, protože bere často v úvahu jen omezené množství problémů), - v případě potřeby přehodnotit architekturu signalizace. IEC-62443-3-3 [7], NIST SP800-82 [98], ISO 27002 [99], TS 50701 [94]. 8. Nutno podporovat zpravodajskou činnost a budovat schopnost odezvy na incidenty. 9. CSMS musí být vytvořen na úrovni celé železnice a musí zahrnovat signalizaci. Kybernetická rizika pro zabezpečení spojená se systémem signalizace musí být řízena jako součást řízení kybernetických rizik celé železnice. – IEC 62443-2-1 [7], IEC 62443-2-2 [7], NIST SP800-30 [100], ISO 27005 [101].

	10. Kybernetické zabezpečení železnice musí být vytvořeno a provozována na úrovni top managementu celé železnice. – ISO 27001 [67], IEC 62443 [7]
Způsob importování ovládacích prvků do systému zabezpečení	11. Ovládací prvky zvládání rizik pro celou železnici, která jsou řešena zabezpečeními v signalizačním systému, musí být schválena kompetentním inženýrem pro signalizaci.
Plánování a odůvodnění nákladů na kybernetické zabezpečení systému signalizace	12. Sestavit víceletý program na zabezpečené celé železnice s tím, že musí obsahovat požadavky na zabezpečení systému signalizace založený na hodnocení rizik. 13. Náklady na kybernetické zabezpečení vyplynou z CSMS.
Způsob zajištění aktuálnosti kybernetického zabezpečení	14. Platnost a účinnost opatření kybernetického zabezpečení lze dosáhnout permanentním přizpůsobováním CSMS podmínkám. Role inženýra odpovědného za signalizaci jako poradce inženýra pro zabezpečení je kritická role při provádění analýzy rizik, která odráží skutečnou situaci. Program pro zabezpečení v rámci CSMS musí být pravidelně revidován, aby se zajistila jeho aktuálnost. IEC-62443-2-2 [7], ISO 27005 [101].

6.3.4. Nástroj pro bezpečné řízení vlaků

Na základě současného poznání, shrnutého v pracích [2,39] bezpečné řízení vlaků dosáhneme tím, že budeme správně řídit rizika systému řízení vlaků ve prospěch bezpečnosti. Systém pro podporu řízení rizik zacílený na bezpečný provoz systému řízení vlaků (SŘV) při provozu jsme sestavili analogicky k systému, vypracovanému pro technická díla v práci [39] se zvážením obrázku 11 s tím, že jsme použili jen části, které odpovídají povaze systému řízení vlaků v systémovém pojetí. Pro jeho pochopení uvádíme:

- systém řízení vlaků (SŘV) je socio-kyber-technický (fyzický) systém,
- jsou zváženy poznatky o projevech lidského faktoru a je bráno v úvahu, že kompetence a odpovědnosti, které uvolňují potřebné zdroje na opatření a činnosti na řízení a vypořádání rizik ve prospěch bezpečnosti závisí na úrovni organizační struktury. Nejvyšší kompetence jsou na nejvyšších úrovních (nejvyšších postech) SŘV, jak ukazuje práce [1]. Proto také na této úrovni jsou největší odpovědnosti za řízení rizik systému řízení vlaků ve prospěch bezpečnosti,
- je zvážen princip odpovědnosti, který je běžný v Evropě [102], což v daném případě znamená, že odpovědnost za bezpečnost provozu systému řízení vlaků, tj. za úroveň práce s riziky spojenými se systémem řízení vlaků, má vlastník i veřejná správa, která má povinnost dohledu ve veřejném zájmu.

Organizační struktura *správy systému řízení vlaků* (SSŘV) je mechanismus, který slouží ke koordinaci a řízení provozu systému řízení vlaků (SŘV). Dle [103-105] vymezuje hierarchické uspořádání vztahů nadřízenosti a podřízenosti a řeší vzájemné pravomoci (kompetence), vazby a odpovědnost. Uvolnění velkých finančních a dalších prostředků na řízení a vypořádání rizik pochopitelně je jen na nejvyšší hierarchické úrovni SSŘV. Na základě legislativy ČR je zvážena struktura: vrcholový management SSŘV; střední management SSŘV; technický management SSŘV; kybernetický management SŘV; a personál (kritický a podpůrný) SSŘV, a také role veřejné správy, která, jak již bylo uvedeno, vykonává dohled nad bezpečností ve veřejném zájmu.

Při sestavování systému pro podporování rozhodování o rizicích jsou brány v úvahu aspekty, které posuzují: způsob zvažování rizik a jejich zdrojů; dosaženou úroveň zabezpečení i bezpečnosti při daném provedení systému řízení vlaků; technickou úroveň zavedených opatření; materiálovou a energetickou náročnost; rychlost realizace opatření; nároky na personál; nároky na informační zajištění; nároky na finance; nároky na odpovědnost; a také nároky na řízení všech zúčastněných (tj. jak řízení systému řízení vlaků, tak řízení zájmového území). Tabulka 9 obsahuje zdroje rizik, které mají potenciál narušit integrální bezpečnost SŘV, tj. koexistenci SŘV a jeho okolí. Způsob vyhodnocování systému pro podporu řízení rizik ve prospěch je stejný jako v práci [39] (je třeba pouze nahradit číselnou hodnotu n, která je u původního nástroje rovna 302 a u SŘV je rovna 263), a proto zde není uváděn.

Tabulka 9. Nástroj pro řízení rizik SSŘV a jeho okolí ve prospěch bezpečnosti SŘV kompetentními hodnotiteli - experty. Počet kritérií n= 263.

Kritérium	**Hodnocení**	**Pozn.**
Míra, v jaké top management SSŘV chápe a realizuje odpovědnost za integrální bezpečnost SŘV.		
Míra, v jaké top management SSŘV zvažuje při řízení rizik SŘV dopady pohrom dle přístupu All-Hazard-Approach, které jsou možné v zájmovém území a míra v jaké provádí nápravy nedostatků.		
Míra, v jaké top management SSŘV zvažuje při řízení rizik SŘV dopady možných nadprojektových živelních pohrom v daném území a míra v jaké provádí nápravy nedostatků.		
Míra, v jaké top management SSŘV zvažuje při řízení rizik SŘV dopady pádu letadla, požáru a výbuchu v okolí SŘV a provádí nápravu nedostatků.		
Míra, v jaké top management SSŘV zvažuje při řízení rizik SŘV dopady výpadku vnější elektrické sítě a provádí nápravu nedostatků.		
Míra, v jaké top management SSŘV zvažuje při řízení rizik SŘV dopady výpadku vnějších dodávek vody a provádí nápravu nedostatků.		

Míra, v jaké top management SSŘV zvažuje při řízení rizik SŘV dopady ztráty komunikačního spojení se světem a provádí nápravu nedostatků		
Míra, v jaké top management SSŘV zvažuje při řízení rizik SŘV dopady poruchy spojení se světem.		
Míra, v jaké top management SSŘV zvažuje při řízení rizik SŘV dopady poruch v dodávkách materiálu.		
Míra, v jaké top management SSŘV zvažuje při řízení rizik SŘV dopady poruch v odběru zboží a provádí nápravu nedostatků.		
Míra, v jaké top management SSŘV zvažuje při řízení rizik SŘV dopady změn orientace veřejné správy (ztráta podpory) a provádí nápravu nedostatků.		
Míra, v jaké top management SSŘV zvažuje při řízení rizik SŘV dopady nedostatku pracovních sil a provádí nápravu nedostatků.		
Míra, v jaké top management SSŘV zvažuje při řízení rizik SŘV dopady nedostatku kvalifikovaných pracovních sil a provádí nápravu nedostatků.		
Míra, v jaké top management SSŘV zvažuje při řízení rizik SŘV dopady výrazného zvýšení daní a provádí nápravu nedostatků.		
Míra, v jaké top management SSŘV zvažuje při řízení rizik SŘV dopady výrazné změny úrokových sazeb a provádí nápravu nedostatků.		
Míra, v jaké top management SSŘV zvažuje při řízení rizik SŘV dopady nepřidělení dotací a provádí nápravu nedostatků.		
Míra, v jaké top management SSŘV zvažuje při řízení rizik SŘV dopady odbytové krize a provádí nápravu nedostatků.		
Míra, v jaké top management SSŘV zvažuje při řízení rizik SŘV dopady rychlých a výrazných změn v cenové politice na trhu a provádí nápravu nedostatků.		
Míra, v jaké top management SSŘV zvažuje při řízení rizik SŘV dopady nesolventnosti zákazníků a provádí nápravu nedostatků.		
Míra, v jaké top management SSŘV zvažuje při řízení rizik SŘV dopady selhání smluv s dodavateli a provádí nápravu nedostatků.		
Míra, v jaké top management SSŘV zvažuje při řízení rizik SŘV dopady selhání smluv s odběrateli služeb a provádí nápravu nedostatků.		
Míra, v jaké top management SSŘV zvažuje při řízení rizik SŘV dopady války a provádí ochranná opatření.		

Míra, v jaké top management SSŘV zvažuje při řízení rizik SŘV dopady boje o moc mezi politickými rivaly a provádí ochranná opatření.		
Míra, v jaké top management SSŘV zvažuje při řízení rizik SŘV dopady úmyslného poškozování good will a provádí ochranná opatření		
Míra, v jaké top management SSŘV zvažuje při řízení rizik SŘV dopady teroristického fyzického útoku z okolí a provádí ochranná opatření.		
Míra, v jaké top management SSŘV zvažuje při řízení rizik SŘV dopady hackerského útoku z okolí a provádí ochranná opatření.		
Míra, v jaké top management SSŘV zvažuje při řízení rizik SŘV dopady útoků nátlakových skupin a provádí ochranná opatření.		
Míra, v jaké top management SSŘV zvažuje při řízení rizik SŘV dopady neoprávněného užívání duševního vlastnictví firmy a provádí ochranná opatření.		
Míra, v jaké top management SSŘV zvažuje při řízení rizik SŘV dopady špatné spolupráce s místní veřejnou správou a provádí nápravu nedostatků.		
Míra, v jaké top management SSŘV zvažuje při řízení rizik SŘV dopady vnitřního požáru a provádí nápravu nedostatků.		
Míra, v jaké top management SSŘV zvažuje při řízení rizik SŘV dopady vnitřního výbuchu a provádí nápravu nedostatků.		
Míra, v jaké top management SSŘV zvažuje při řízení rizik SŘV dopady kontaminace ovzduší v okolí SŘV a provádí nápravu nedostatků.		
Míra, v jaké top management SSŘV zvažuje při řízení rizik SŘV dopady kontaminace pitné a užitkové vody v okolí SŘV a provádí nápravu nedostatků.		
Míra, v jaké top management SSŘV zvažuje při řízení rizik SŘV dopady kontaminace zařízení a staveb v okolí SŘV a provádí nápravu nedostatků.		
Míra, v jaké top management SSŘV zvažuje při řízení rizik SŘV dopady výpadku vnitřního rozvodu elektrické energie v SŘV a provádí nápravu nedostatků.		
Míra, v jaké top management SSŘV zvažuje při řízení rizik SŘV dopady výpadku vnitřního osvětlení a provádí nápravu nedostatků.		
Míra, v jaké top management SSŘV zvažuje při řízení rizik SŘV dopady výpadku vnitřního rozvodu pitné a užitkové vody a provádí nápravu nedostatků.		

Míra, v jaké top management SSŘV zvažuje při řízení rizik SŘV dopady výpadku chladícího systému SŘV a provádí nápravu nedostatků.		
Míra, v jaké top management SSŘV zvažuje při řízení rizik SŘV dopady výpadku větrání v SŘV a provádí nápravu nedostatků.		
Míra, v jaké top management SSŘV zvažuje při řízení rizik SŘV dopady výpadku vnitřní komunikační sítě SŘV a provádí nápravu nedostatků.		
Míra, v jaké top management SSŘV zvažuje při řízení rizik SŘV dopady poruchy přísunu materiálu či polotovarů mezi úseky SRV a provádí nápravu nedostatků.		
Míra, v jaké top management SSŘV zvažuje při řízení rizik SŘV dopady poruchy předávání materiálů mezi úseky SŘV a provádí nápravu nedostatků.		
Míra, v jaké top management SSŘV zvažuje při řízení rizik SŘV dopady výpadku nouzového osvětlení SŘV a provádí nápravu nedostatků.		
Míra, v jaké top management SSŘV zvažuje při řízení rizik SŘV dopady výpadku nouzového komunikačního systému a provádí nápravu nedostatků.		
Míra, v jaké top management SSŘV zvažuje při řízení rizik SŘV dopady výpadku nouzového hasícího zařízení a provádí nápravu nedostatků.		
Míra, v jaké top management SSŘV zvažuje při řízení rizik SŘV dopady nepřijetí nápravných opatření v případě zjištění chyb v projektu či konstrukci technologického vybavení a provádí nápravu nedostatků.		
Míra, v jaké top management SSŘV zvažuje při řízení rizik SŘV dopady nesledování skoro nehod a malých nehod a nevypracování poučení s cílem jim zabránit a provádí nápravu nedostatků.		
Míra, v jaké top management SSŘV zvažuje při řízení rizik SŘV dopady neprovedení nápravných opatření (technických i organizačních) s cílem snížit výskyt skoro nehod a malých nehod a provádí nápravu nedostatků.		
Míra, v jaké top management SSŘV zvažuje při řízení rizik SŘV dopady nezavedení kvalitního monitoringu stavu kritických zařízení, kritických komponent a kritických systémů s cílem včas odhalit: poškození tlakových potrubí s chladícím médiem nebo užitkovou vodou nutnou pro provoz; poškození nebo netěsností ventilů u tlakových nádob, a provádí nápravu nedostatků.		

Míra, v jaké top management SSŘV zvažuje při řízení rizik SŘV dopady špatné údržby a provádí nápravu zjištěných nedostatků.		
Míra, v jaké top management SSŘV zvažuje při řízení rizik SŘV dopady špatně provedených oprav technických zařízení a jejich propojení a provádí nápravu nedostatků.		
Míra, v jaké top management SSŘV zvažuje při řízení rizik SŘV dopady špatné reakce technických zařízení a jejich propojení na změnu provozních podmínek s cílem zajistit včasnou výměnu nebo modifikace strojů, zařízení, komponent či systémů, a provádí nápravu nedostatků.		
Míra, v jaké top management SSŘV zvažuje při řízení rizik SŘV dopady neexistence ochranných bariér pro: práci obsluhy; opatření pro práci v nepříznivých podmínkách; kritické činnosti; a nakládání s odpady, a provádí nápravu nedostatků.		
Míra, v jaké top management SSŘV zvažuje při řízení rizik SŘV dopady chyb v podporách provozu a provádí nápravu nedostatků.		
Míra, v jaké top management SSŘV zvažuje při řízení rizik SŘV dopady nedostatku místa v SŘV pro umístění materiálu a provádí nápravu nedostatků.		
Míra, v jaké top management SSŘV zvažuje při řízení rizik SŘV dopady nedostatku místa v SŘV pro umístění / skladování přepravovaných produktů a provádí nápravu nedostatků.		
Míra, v jaké top management SSŘV zvažuje při řízení rizik SŘV dopady chybějících záložních zdrojů energie pro zařízení, která musí pracovat v nepřetržitém provozu a provádí nápravu nedostatků.		
Míra, v jaké top management SSŘV zvažuje při řízení rizik SŘV dopady chybějících záložních zdrojů chladiva pro zařízení, která musí pracovat v nepřetržitém provozu a provádí nápravu nedostatků.		
Míra, v jaké top management SSŘV zvažuje při řízení rizik SŘV dopady chyb na úseku strategie, koncepce a provozních podmínek a provádí nápravu nedostatků.		
Míra, v jaké top management SSŘV zvažuje při řízení rizik SŘV dopady chyb na úseku systému řízení integrální bezpečnosti a provádí nápravu nedostatků.		
Míra, v jaké top management SSŘV zvažuje při řízení rizik SŘV dopady chyb na úseku dlouhodobé strategie rozvoje a provádí nápravu nedostatků.		
Míra, v jaké top management SSŘV zvažuje při řízení rizik SŘV dopady chyb na úseku řešení konfliktů a provádí nápravu nedostatků.		

Míra, v jaké top management SSŘV zvažuje při řízení rizik SŘV dopady chyb na úseku efektivity řízení a provádí nápravu nedostatků.		
Míra, v jaké top management SSŘV zvažuje při řízení rizik SŘV dopady chyb na úseku vertikální i horizontální komunikace a provádí nápravu nedostatků.		
Míra, v jaké top management SSŘV zvažuje při řízení rizik SŘV dopady chyb na úseku řídícího stylu a provádí nápravu nedostatků.		
Míra, v jaké top management SSŘV zvažuje při řízení rizik SŘV dopady chyb na úseku funkčnosti koordinace funkcí a provádí nápravu nedostatků.		
Míra, v jaké top management SSŘV zvažuje při řízení rizik SŘV dopady chyb na úseku řídící schopnosti a provádí nápravu nedostatků.		
Míra, v jaké top management SSŘV zvažuje při řízení rizik SŘV dopady chyb na úseku porozumění zákazníkům a provádí nápravu nedostatků.		
Míra, v jaké top management SSŘV zvažuje při řízení rizik SŘV dopady chyb na úseku schopnosti předpokládat vývoj vnějšího prostředí a provádí nápravu nedostatků.		
Míra, v jaké top management SSŘV zvažuje při řízení rizik SŘV dopady chyb na úseku objektivity hodnocení organizačních kompetencí a provádí nápravu nedostatků.		
Míra, v jaké top management SSŘV zvažuje při řízení rizik SŘV dopady chyb na úseku využití rozvojového potenciálu a provádí nápravu nedostatků.		
Míra, v jaké top management SSŘV zvažuje při řízení rizik SŘV dopady chyb na úseku angažovanosti top managementu ve prospěch SŘV a provádí nápravu nedostatků.		
Míra, v jaké top management SSŘV zvažuje při řízení rizik SŘV dopady chyb na úseku časových nároků provozu a provádí nápravu nedostatků.		
Míra, v jaké top management SSŘV zvažuje při řízení rizik SŘV dopady chyb na úseku komunikační strategie s příslušnou veřejnou správou a provádí nápravu nedostatků.		
Míra, v jaké top management SSŘV zvažuje při řízení rizik SŘV dopady chyb na úseku komunikační strategie s podřízenými a provádí nápravu nedostatků.		
Míra, v jaké top management SSŘV zvažuje při řízení rizik SŘV dopady chyb na úseku dostatečnosti monitorování výsledků a provádí nápravu nedostatků.		

Míra, v jaké top management SSŘV zvažuje při řízení rizik SŘV dopady chyb na úseku dostatečného využití lidských zdrojů a provádí nápravu nedostatků.		
Míra, v jaké top management SSŘV zvažuje při řízení rizik SŘV dopady chyb na úseku smluvního zajištění včasných dodávek materiálů či služeb a provádí nápravu nedostatků.		
Míra, v jaké top management SSŘV zvažuje při řízení rizik SŘV dopady chyb na úseku smluvního zajištění včasného odběru produktů nebo služeb a provádí nápravu nedostatků.		
Míra, v jaké top management SSŘV zvažuje při řízení rizik SŘV dopady chyb na úseku schopnosti přizpůsobit se změnám obecně závazných předpisů a provádí nápravu nedostatků.		
Míra, v jaké top management SSŘV zvažuje při řízení rizik SŘV dopady chyb na úseku schopnosti přizpůsobit se změnám v systému daní a provádí nápravu nedostatků.		
Míra, v jaké top management SSŘV zvažuje při řízení rizik SŘV dopady chyb na úseku schopnosti přizpůsobit se změnám v úrokových sazbách a provádí nápravu nedostatků.		
Míra, v jaké top management SSŘV zvažuje při řízení rizik SŘV dopady chyb na úseku schopnosti přizpůsobit se změnám situace na trhu a provádí nápravu nedostatků.		
Míra, v jaké top management SSŘV zvažuje při řízení rizik SŘV dopady chyb na úseku schopnosti přizpůsobit se změnám podpory ze strany státu a provádí nápravu nedostatků.		
Míra, v jaké top management SSŘV zvažuje při řízení rizik SŘV dopady chyb na úseku schopnosti zajistit dostatečné množství kvalifikovaného personálu a provádí nápravu nedostatků.		
Míra, v jaké top management SSŘV zvažuje při řízení rizik SŘV dopady chyb na úseku schopnosti zajistit finanční rezervy pro provoz při vnějších změnách a provádí nápravu nedostatků.		
Míra, v jaké top management SSŘV zvažuje při řízení rizik SŘV dopady chyb na úseku zájmu o bezpečný SŘV a provádí nápravu nedostatků.		
Míra, v jaké top management SSŘV zvažuje při řízení rizik SŘV dopady chyb na úseku úrovně potřebných technických znalostí a provádí nápravu nedostatků.		
Míra, v jaké top management SSŘV zvažuje při řízení rizik SŘV dopady chyb na úseku dokumentace pro bezpečný provoz a provádí nápravu nedostatků.		

Míra, v jaké top management SSŘV zvažuje při řízení rizik SŘV dopady chyb na úseku kvality standardů, norem a postupů pro řízení změn a provádí nápravu nedostatků.		
Míra, v jaké top management SSŘV zvažuje při řízení rizik SŘV dopady na úseku dohledu a kontroly provozu a provádí nápravu nedostatků.		
Míra, v jaké top management SSŘV zvažuje při řízení rizik SŘV dopady chyb na úseku stanovení odpovědností a provádí nápravu nedostatků.		
Míra, v jaké top management SSŘV zvažuje při řízení rizik SŘV dopady na úseku zajištění informovanosti a provádí nápravu nedostatků.		
Míra, v jaké top management SSŘV zvažuje při řízení rizik SŘV dopady chyb na úseku zajištění dostatečného systému odezvy na nouzové situace a provádí nápravu nedostatků.		
Míra, v jaké top management SSŘV zvažuje při řízení rizik SŘV dopady chyb na úseku stanovení požadavků na kvalifikovanost a dovednost obsluhy a provádí nápravu nedostatků.		
Míra, v jaké top management SSŘV zvažuje při řízení rizik SŘV dopady chyb na úseku zajištění kvalitního systému vzdělávání personálu a provádí nápravu nedostatků.		
Míra, v jaké top management SSŘV zvažuje při řízení rizik SŘV dopady chyb na úseku zajištění pracovní disciplíny při práci v nebezpečných provozech a provádí nápravu nedostatků.		
Míra, v jaké top management SSŘV zvažuje při řízení rizik SŘV dopady chyb na úseku zajištění kvalitního technického řízení strojů, zařízení, komponent a systémů a provádí nápravu nedostatků.		
Míra, v jaké top management SSŘV zvažuje při řízení rizik SŘV dopady chyb na úseku zajištění kvalitního automatického řízení strojů, zařízení, komponent a systémů a provádí nápravu nedostatků.		
Míra, v jaké top management SSŘV zvažuje při řízení rizik SŘV dopady chyb na úseku monitoringu provozu zacíleného na bezpečnost provozu a provádí nápravu nedostatků.		
Míra, v jaké top management SSŘV zvažuje při řízení rizik SŘV dopady chyb na úseku systému provádění technických inspekcí a provádí nápravu nedostatků.		
Míra, v jaké top management SSŘV zvažuje při řízení rizik SŘV dopady chyb na úseku systému financování zacíleného na bezpečnost provozu a provádí nápravu nedostatků.		
Míra, v jaké top management SSŘV zvažuje při řízení rizik SŘV dopady chyb na úseku finančních rezerv na obnovu		

strojů, zařízení, komponent a systémů po provozní havárii a provádí nápravu nedostatků.		
Míra, v jaké top management SSŘV zvažuje při řízení rizik SŘV dopady chyb na úseku finančních rezerv na obnovu strojů, zařízení, komponent a systémů po nadprojektové havárii a provádí nápravu nedostatků.		
Míra, v jaké top management SSŘV zvažuje při řízení rizik SŘV dopady chyb na úseku zpracování poplachového plánu a provádí nápravu nedostatků.		
Míra, v jaké top management SSŘV zvažuje při řízení rizik SŘV dopady chyb na úseku zpracování potřebných nouzových (vnitřních) plánů a provádí nápravu nedostatků.		
Míra, v jaké top management SSŘV zvažuje při řízení rizik SŘV dopady chyb na úseku zpracování plánu kontinuity pro extrémní situace a provádí nápravu nedostatků.		
Míra, v jaké top management SSŘV zvažuje při řízení rizik SŘV dopady chyb na úseku rozmístění požární signalizace a hasících přístrojů a provádí nápravu nedostatků.		
Míra, v jaké top management SSŘV zvažuje při řízení rizik SŘV dopady chyb na úseku ochrany proti organizačním haváriím (tj. není: strategická koncepce řízení SŘV v čase, kvalitní monitoring rizik a program na zvyšování bezpečnosti) a provádí nápravu nedostatků.		
Míra, v jaké top management SSŘV zvažuje při řízení rizik SŘV dopady chyb na úseku kvality provozních předpisů pro normální provoz a provádí nápravu nedostatků.		
Míra, v jaké top management SSŘV zvažuje při řízení rizik SŘV dopady chyb na úseku kvality provozních předpisů pro abnormální provoz a provádí nápravu nedostatků.		
Míra, v jaké top management SSŘV zvažuje při řízení rizik SŘV dopady chyb na úseku kvality provozních předpisů pro kritický provoz a provádí nápravu nedostatků.		
Míra, v jaké top management SSŘV zvažuje při řízení rizik SŘV dopady chyb na úseku kvalitní přípravy obslužných procesů před jejich zahájením a provádí nápravu nedostatků.		
Míra, v jaké top management SSŘV zvažuje při řízení rizik SŘV dopady chyb na úseku kontroly strojů a zařízení před zahájením kritické operace a provádí nápravu nedostatků.		
Míra, v jaké top management SSŘV zvažuje při řízení rizik SŘV dopady chyb na úseku ověřování kvalifikace a dovednosti kritického personálu a provádí nápravu nedostatků.		
Míra, v jaké top management SSŘV zvažuje při řízení rizik SŘV dopady chyb na úseku sestavení a ověření postupů pro kritické procesy a provádí nápravu nedostatků.		

Míra, v jaké top management SSŘV zvažuje při řízení rizik SŘV dopady chyb na úseku důkladné kontroly kvality výstupů z kritických procesů a provádí nápravu nedostatků.		
Míra, v jaké top management SSŘV zvažuje při řízení rizik SŘV dopady chyb na úseku postupů pro účinnou odezvu na kritické podmínky a materiální, technické, finanční a personální rezervy na její provedení a provádí nápravu nedostatků.		
Míra, v jaké top management SSŘV zvažuje při řízení rizik SŘV dopady chyb na úseku předpisů pro obsluhu při výskytu: vnějších pohrom (živelní pohromy, pád letadla, nepříznivé klimatické podmínky, přerušení zásobování nádraží elektřinou, vodou apod. od vnějších sítí; vnitřních pohrom (požár, výbuch, výpadek elektrické energie, výpadek dodávek vody či jiného chladiva, výpadek nouzového osvětlení, zatopení objektu, výpadek vnitřní komunikační sítě, požár, výbuch, výpadek informační sítě); technických poruch (neseřízené stroje; neseřízená zařízení; neseřízené komponenty; neseřízené systémy; použití špatných údajů při seřízení zařízení; porucha nebo selhání bezpečnostních pojistek, zařízení či systémů; poškození kritických zařízení, komponent či potrubí – např. tlakové nádoby, potrubí s chladivem; netěsné ventily; selhání blokovacích zařízení; poruchy svarů, kabelů, čerpadel, kompresorů, diesel generátorů; elektrický zkrat; nefunkčnost zařízení pro varování v případě nouze; vyřazení automatických hasicích přístrojů v případě nouze; zaseknutý pojistný ventil; nedostatečné chlazení; nedostatečná ochrana při práci s nebezpečnými látkami nebo ionizujícím zářením; nedostatečná úprava práce s nebezpečnými látkami či ionizujícím zářením; špatné kontakty na relé v řídicím systému; nevhodné kontejnery pro skladování nebo přesun nebezpečných látek; špatně provedená přeprava materiálů, polotovarů či výrobků; apod.); nejsou určeny odpovědnosti za výrobní operace a zásady vzájemné pomoci (kultura bezpečnosti), a provádí nápravu nedostatků; tj. míra úrovně zajištění bezpečného provozu v daném případě.		
Míra, v jaké top management SSŘV zvažuje při řízení rizik SŘV dopady chyb na úseku dostatečnosti ochrany prioritních strojů, zařízení, komponent a systémů při nadprojektové havárii a provádí nápravu nedostatků.		
Míra, v jaké top management SSŘV zvažuje při řízení rizik SŘV dopady chyb na úseku zajištění kvalitních pracovních podmínek pro lidí a kvalitní režimová opatření pro provozu strojů, zařízení, komponent a systémů zohledňující možnosti obslužného personálu a provádí nápravu nedostatků.		
Míra, v jaké top management SSŘV zvažuje při řízení rizik SŘV dopady chyb na úseku zajištění dostatečné ochrany životů, zdraví a bezpečí obslužného personálu za všech možných podmínek a provádí nápravu nedostatků.		

Míra, v jaké top management SSŘV zvažuje při řízení rizik SŘV dopady chyb na úseku zajištění dostatečné ochrany životů, zdraví a bezpečí kontraktorů za všech možných podmínek a provádí nápravu nedostatků.		
Míra, v jaké top management SSŘV zvažuje při řízení rizik SŘV dopady chyb na úseku zajištění dostatečné ochrany životů, zdraví a bezpečí návštěvníků za všech možných podmínek a provádí nápravu nedostatků.		
Míra, v jaké top management SSŘV zvažuje při řízení rizik SŘV dopady chyb na úseku zajištění dostatečné ochrany strojů, zařízení, komponent a systémů technického zařízení před podvodným nebo nebezpečným jednáním lidí z obsluhy, personálu kontraktorů či skupiny návštěvníků a provádí nápravu nedostatků.		
Míra, v jaké top management SSŘV zvažuje při řízení rizik SŘV dopady chyb na úseku zajištění vytváření příznivé atmosféry v systému řízení vlaků a provádí nápravu nedostatků.		
Míra, v jaké top management SSŘV zvažuje při řízení rizik SŘV dopady chyb na úseku zajištění prosazování zásad kultury bezpečnosti v SŘV a provádí nápravu nedostatků.		
Míra, v jaké top management SSŘV zvažuje při řízení rizik SŘV dopady chyb na úseku zajištění motivace obslužného personálu ke kvalitní práci a k bezpečnému chování pomocí zvláštní péče o pracovníky, výcviku a finančních odměn a provádí nápravu nedostatků.		
Míra, v jaké top management SSŘV zvažuje při řízení rizik SŘV dopady chyb na úseku zajištění otevřené komunikace na všech úrovních řízení SŘV a mezi nimi o problémech provozních, bezpečnostních a dalších a provádí nápravu nedostatků.		
Míra, v jaké top management SSŘV zvažuje při řízení rizik SŘV dopady chyb na úseku zajištění fyzické ochrany prioritních strojů, zařízení, komponent a systémů při normálních, abnormálních a kritických podmínkách a provádí nápravu nedostatků.		
Míra, v jaké top management SSŘV zvažuje při řízení rizik SŘV dopady chyb na úseku zajištění kybernetické ochrany prioritních automatických strojů, zařízení, komponent a systémů při normálních, abnormálních a kritických podmínkách a provádí nápravu nedostatků.		
Míra, v jaké top management SSŘV zvažuje při řízení rizik SŘV dopady chyb na úseku zajištění rezerv na dekontaminaci strojů, zařízení, komponent a systémů po ukončení provozu a provádí nápravu nedostatků.		
Míra, v jaké top management SSŘV zvažuje při řízení rizik SŘV dopady chyb na úseku zajištění kvalitní spolupráce s		

veřejnou správou, jako je předávání podkladů pro vnější nouzové (havarijní) plány a vzájemné podpory zacílené na zvládnutí krizových situaci a provádí nápravu nedostatků.		
Míra, v jaké top management SSŘV zvažuje při řízení rizik SŘV dopady chyb na úseku zajištění prověřování účinnosti organizačních opatření a provádí nápravu nedostatků.		
Míra, v jaké top management SSŘV zvažuje při řízení rizik SŘV dopady chyb na úseku zajištění kvalitní spolupráce s ostatními SŘV, které jsou vzájemně provázané územně, výrobou, podobnou technologií aj. a provádí nápravu nedostatků.		
Míra, v jaké top management SSŘV zvažuje při řízení rizik SŘV dopady chyb na úseku zajištění správného vyhodnocování rizik a provádí nápravu nedostatků.		
Míra, v jaké top management SSŘV zvažuje při řízení rizik SŘV dopady chyb na úseku zajištění ověřených předpisů pro: řízení přepravy, manipulace a skladování materiálů a odpadů, a provádí nápravu nedostatků.		
Míra, v jaké top management SSŘV chápe a realizuje odpovědnost za bezpečnost SŘV.		
Míra, v jaké střední management SSŘV zvažuje při řízení rizik SŘV dopady chyb na úseku realizace účinného řízení bezpečnosti procesů a provádí nápravu nedostatků.		
Míra, v jaké střední management SSŘV zvažuje při řízení rizik SŘV dopady chyb na úseku realizace nedostatečného povědomí o rizicích a bezpečnosti a provádí nápravu nedostatků.		
Míra, v jaké střední management SSŘV zvažuje při řízení rizik SŘV dopady chyb na úseku realizace komunikace vertikální i horizontální a provádí nápravu nedostatků.		
Míra, v jaké střední management SSŘV zvažuje při řízení rizik SŘV dopady chyb na úseku realizace řídícího stylu a provádí nápravu nedostatků.		
Míra, v jaké střední management SSŘV zvažuje při řízení rizik SŘV dopady chyb na úseku realizace slabé angažovanosti středního managementu ve prospěch procesu a provádí nápravu nedostatků.		
Míra, v jaké střední management SSŘV zvažuje při řízení rizik SŘV dopady chyb na úseku monitoringu výsledků projektu a provádí nápravu nedostatků.		
Míra, v jaké střední management SSŘV zvažuje při řízení rizik SŘV dopady chyb na úseku využití lidských zdrojů a provádí nápravu nedostatků.		
Míra, v jaké střední management SSŘV zvažuje při řízení rizik SŘV dopady chyb na úseku dohledu a kontroly nad procesem a provádí nápravu nedostatků.		

Míra, v jaké střední management SSŘV zvažuje při řízení rizik SŘV dopady chyb na úseku stanovení odpovědností u procesů a provádí nápravu nedostatků.		
Míra, v jaké střední management SSŘV zvažuje při řízení rizik SŘV dopady chyb na úseku zajištění informovanosti a provádí nápravu nedostatků.		
Míra, v jaké střední management SSŘV zvažuje při řízení rizik SŘV dopady chyb na úseku odezvy na nouzové situace a provádí nápravu nedostatků.		
Míra, v jaké střední management SSŘV zvažuje při řízení rizik SŘV dopady chyb na úseku řízení v oblasti technické, IT, organizace pro ovládání obsluhy, strojů, zařízení, komponent a systémů a nakládání s odpady, a provádí nápravu nedostatků.		
Míra, v jaké střední management SSŘV zvažuje při řízení rizik SŘV dopady chyb na úseku odezvy na nouzové situace a provádí nápravu nedostatků.		
Míra, v jaké střední management SSŘV zvažuje při řízení rizik SŘV dopady chyb na úseku monitoringu provozu zacíleného na bezpečnost zahrnující kvalitní obslužnost a provádí nápravu nedostatků.		
Míra, v jaké střední management SSŘV zvažuje při řízení rizik SŘV dopady chyb na úseku provádění technických inspekcí a provádí nápravu nedostatků.		
Míra, v jaké střední management SSŘV zvažuje při řízení rizik SŘV dopady chyb na úseku provozních předpisů pro normální provoz a provádí nápravu nedostatků.		
Míra, v jaké střední management SSŘV zvažuje při řízení rizik SŘV dopady chyb na úseku provozních předpisů pro abnormální provoz a provádí nápravu nedostatků.		
Míra, v jaké střední management SSŘV zvažuje při řízení rizik SŘV dopady chyb na úseku provozních předpisů pro kritický provoz a provádí nápravu nedostatků.		
Míra, v jaké střední management SSŘV zvažuje při řízení rizik SŘV dopady chyb na úseku údržby a kontroly její kvality a provádí nápravu nedostatků.		
Míra, v jaké střední management SSŘV zvažuje při řízení rizik SŘV dopady chyb na úseku kvalitní přípravy kritických procesů před jejich zahájením a provádí nápravu nedostatků.		
Míra, v jaké střední management SSŘV zvažuje při řízení rizik SŘV dopady chyb na úseku požadavku na kontrolu strojů a zařízení před zahájením kritické operace a provádí nápravu nedostatků.		

Míra, v jaké střední management SSŘV zvažuje při řízení rizik SŘV dopady chyb na úseku ověřování kvalifikace a dovednost kritického personálu a provádí nápravu nedostatků.		
Míra, v jaké střední management SSŘV zvažuje při řízení rizik SŘV dopady chyb na úseku zajištění kvalitních pracovních podmínek lidí a kvalitních režimových opatření při provozu strojů, zařízení, komponent a systémů zohledňující možnosti obslužného personálu a provádí nápravu nedostatků.		
Míra, v jaké střední management SSŘV zvažuje při řízení rizik SŘV dopady chyb na úseku ochrany životů, zdraví a bezpečí obslužného personálu za všech podmínek v pracovním prostředí (ochranné pomůcky, úkryty, evakuace) a provádí nápravu nedostatků.		
Míra, v jaké střední management SSŘV zvažuje při řízení rizik SŘV dopady chyb na úseku provozních předpisů pro kritický provoz a provádí nápravu nedostatků.		
Míra, v jaké střední management SSŘV zvažuje při řízení rizik SŘV dopady chyb na úseku vytváření příznivé atmosféry v SŘV a provádí nápravu nedostatků.		
Míra, v jaké střední management SSŘV zvažuje při řízení rizik SŘV dopady chyb na úseku prosazování zásad kultury bezpečnosti, a provádí nápravu nedostatků.		
Míra, v jaké střední management SSŘV zvažuje při řízení rizik SŘV dopady chyb na úseku motivace obslužného personálu ke kvalitní práci a k bezpečnému chování pomocí zvláštní péče o pracovníky, výcviku, financí a provádění nápravy nedostatků.		
Míra, v jaké střední management SSŘV zvažuje při řízení rizik SŘV dopady chyb na úseku otevřenosti komunikace na všech úrovních řízení SŘV a mezi nimi o problémech servisních, bezpečnostních a dalších a provádí nápravu nedostatků.		
Míra, v jaké střední management SSŘV zvažuje při řízení rizik SŘV dopady chyb na úseku fyzické ochrany prioritních strojů, zařízení, komponent a systémů při normálních, abnormálních a kritických podmínkách a provádí nápravu nedostatků.		
Míra, v jaké střední management SSŘV zvažuje při řízení rizik SŘV dopady chyb na úseku kybernetické ochrany prioritních strojů, zařízení, komponent a systémů při normálních, abnormálních a kritických podmínkách a provádí nápravu nedostatků.		
Míra, v jaké střední management SSŘV zvažuje při řízení rizik SŘV dopady chyb na úseku práce s riziky a provádí nápravu nedostatků.		

Míra, v jaké střední management SSŘV zvažuje při řízení rizik SŘV dopady chyb na úseku manipulace a přepravy materiálů, meziproduktů a výrobků, a provádí nápravu nedostatků.		
Míra, v jaké střední management SSŘV zvažuje při řízení rizik SŘV dopady chyb na úseku skladování a provádí nápravu nedostatků.		
Míra, v jaké střední management SSŘV zvažuje při řízení rizik SŘV dopady chyb na úseku řízení provozu provázaných systémů technických zařízení a provádí nápravu nedostatků.		
Míra, v jaké střední management SSŘV zvažuje při řízení rizik SŘV dopady chyb na úseku řízení klíčových procesů (process safety management) a provádí nápravu nedostatků.		
Míra, v jaké střední management SSŘV zvažuje při řízení rizik SŘV dopady chyb na úseku pracovních režimů u kritických zařízení, komponent a systémů (integrity management strategy) a provádí nápravu nedostatků.		
Míra, v jaké střední management SSŘV zvažuje při řízení rizik SŘV dopady chyb na úseku stanovení bariér, limit a podmínek pro kritické procesy a provádí nápravu nedostatků.		
Míra, v jaké střední management SSŘV zvažuje při řízení rizik SŘV dopady chyb na úseku stanovení reakcí na změny a provádí nápravu nedostatků.		
Míra, v jaké střední management SSŘV zvažuje při řízení rizik SŘV dopady chyb na úseku zabránění práci / provozu mimo dovolené limity (znamenající porušení provozních předpisů), a provádí nápravu nedostatků.		
Míra, v jaké střední management SSŘV zvažuje při řízení rizik SŘV dopady chyb na úseku strategie údržby kritických technických zařízení, jejich propojení a infrastruktur podporujících jejich provoz a provádí nápravu nedostatků.		
Míra, v jaké střední management SSŘV zvažuje při řízení rizik SŘV dopady chyb na úseku plánů pro zvládání nouzových situací a provádí nápravu nedostatků.		
Míra, v jaké střední management SSŘV zvažuje při řízení rizik SŘV dopady chyb na úseku správnosti informací o provozu a provádí nápravu nedostatků.		
Míra, v jaké střední management SSŘV zvažuje při řízení rizik SŘV dopady chyb na úseku zásobování materiálem a provádí nápravu nedostatků.		
Míra, v jaké střední management SSŘV zvažuje při řízení rizik SŘV dopady chyb na úseku pořádku v SŘV a provádí nápravu nedostatků.		

Míra, v jaké střední management SSŘV zvažuje při řízení rizik SŘV dopady chyb na úseku vzdělávání personálu a provádí nápravu nedostatků.		
Míra, v jaké střední management SSŘV zvažuje při řízení rizik SŘV dopady chyb na úseku motivace kritického personálu a provádí nápravu nedostatků.		
Míra, v jaké střední management SSŘV zvažuje při řízení rizik SŘV dopady chyb na úseku varovacího systému, a provádí nápravu nedostatků.		
Míra, v jaké střední management SSŘV zvažuje při řízení rizik SŘV dopady chyb na úseku vyznačení evakuačních tras, a provádí nápravu nedostatků.		
Míra, v jaké střední management SSŘV zvažuje při řízení rizik SŘV dopady chyb na úseku úkrytů pro zaměstnance pro případ potřeby a provádí nápravu nedostatků.		
Míra, v jaké střední management SSŘV zvažuje při řízení rizik SŘV dopady chyb na úseku odzkoušení způsobu přechodu činností z obvyklých zařízení, komponent či systémů na záložní, a provádí nápravu nedostatků.		
Míra, v jaké střední management SSŘV chápe a realizuje odpovědnost za bezpečnost konkrétních technických zařízení a celého SŘV.		
Míra, v jaké technický management SSŘV zvažuje při řízení rizik SŘV dopady chyb na úseku údržby a kontroly její kvality, a provádí nápravu nedostatků.		
Míra, v jaké technický management SSŘV zvažuje při řízení rizik SŘV dopady chyb na úseku řízení bezpečnosti, a provádí nápravu nedostatků.		
Míra, v jaké technický management SSŘV zvažuje při řízení rizik SŘV dopady chyb na úseku správnosti pracovního režimu a nakládání s odpady, a provádí nápravu nedostatků.		
Míra, v jaké technický management SSŘV zvažuje při řízení rizik SŘV dopady chyb na úseku komunikace vertikální i horizontální, a provádí nápravu nedostatků.		
Míra, v jaké technický management SSŘV zvažuje při řízení rizik SŘV dopady chyb na úseku péče zaměřené na vytváření příznivé atmosféry na pracovišti, a provádí nápravu nedostatků.		
Míra, v jaké technický management SSŘV zvažuje při řízení rizik SŘV dopady chyb na úseku prosazování zásad kultury bezpečnosti, a provádí nápravu nedostatků.		
Míra, v jaké technický management SSŘV zvažuje při řízení rizik SŘV dopady chyb na úseku posilování motivace obslužného personálu ke kvalitní práci a k bezpečnému chování		

pomocí zvláštní péče o pracovníky, výcviku, financí, a provádí nápravu nedostatků.		
Míra, v jaké technický management SSŘV zvažuje při řízení rizik SŘV dopady chyb na úseku zajištění otevřené komunikace o problémech obslužných, bezpečnostních a dalších, a provádí nápravu nedostatků.		
Míra, v jaké technický management SSŘV zvažuje při řízení rizik SŘV dopady chyb na úseku zajištění fyzické ochrany prioritních strojů a zařízení při normálních, abnormálních a kritických podmínkách, a provádí nápravu nedostatků.		
Míra, v jaké technický management SSŘV zvažuje při řízení rizik SŘV dopady chyb na úseku zajištění kybernetické ochrany prioritních strojů a zařízení při normálních, abnormálních a kritických podmínkách, a provádí nápravu nedostatků.		
Míra, v jaké technický management SSŘV zvažuje při řízení rizik SŘV dopady chyb na úseku práce s riziky, a provádí nápravu nedostatků.		
Míra, v jaké technický management SSŘV zvažuje při řízení rizik SŘV dopady chyb na úseku manipulace a přepravy materiálů, odpadů a osob, a provádí nápravu nedostatků.		
Míra, v jaké technický management SSŘV zvažuje při řízení rizik SŘV dopady chyb na úseku skladování materiálů, meziproduktů a výrobků, nakládání s odpady, a provádí nápravu nedostatků.		
Míra, v jaké technický management SSŘV zvažuje při řízení rizik SŘV dopady chyb na úseku řízení bezpečnosti při provádění klíčových operací, a provádí nápravu nedostatků.		
Míra, v jaké technický management SSŘV zvažuje při řízení rizik SŘV dopady chyb na úseku dodržování pracovních režimů u kritických operací, a provádí nápravu nedostatků.		
Míra, v jaké technický management SSŘV zvažuje při řízení rizik SŘV dopady chyb na úseku dodržování bariér, limit a podmínek při kritických operacích, a provádí nápravu nedostatků.		
Míra, v jaké technický management SSŘV zvažuje při řízení rizik SŘV dopady chyb na úseku dodržování předepsaných reakcí na změny, a provádí nápravu nedostatků.		
Míra, v jaké technický management SSŘV zvažuje při řízení rizik SŘV dopady chyb na úseku zabraňování práci /provozu mimo dovolené limity, a provádí nápravu nedostatků.		
Míra, v jaké technický management SSŘV zvažuje při řízení rizik SŘV dopady chyb na úseku zvládání nouzových situací, a provádí nápravu nedostatků.		

Míra, v jaké technický management SSŘV zvažuje při řízení rizik SŘV dopady chyb na úseku dodržování požadavků BOZP, a provádí nápravu nedostatků.		
Míra, v jaké technický management SSŘV zvažuje při řízení rizik SŘV dopady chyb na úseku správnosti údajů o provozu, a provádí nápravu nedostatků.		
Míra, v jaké technický management SSŘV zvažuje při řízení rizik SŘV dopady chyb na úseku zásobování materiálem, a provádí nápravu nedostatků.		
Míra, v jaké technický management SSŘV zvažuje při řízení rizik SŘV dopady chyb na úseku pořádku v SŘV, a provádí nápravu nedostatků.		
Míra, v jaké technický management SSŘV zvažuje při řízení rizik SŘV dopady chyb na úseku vzdělávání obsluhy, a provádí nápravu nedostatků.		
Míra, v jaké technický management SSŘV zvažuje při řízení rizik SŘV dopady chyb na úseku motivace kritického personálu, a provádí nápravu nedostatků.		
Míra, v jaké technický management SSŘV zvažuje při řízení rizik SŘV dopady chyb na úseku varovacího systému, a provádí nápravu nedostatků.		
Míra, v jaké technický management SSŘV zvažuje při řízení rizik SŘV dopady chyb na úseku vyznačení evakuačních tras, a provádí nápravu nedostatků.		
Míra, v jaké technický management SSŘV zvažuje při řízení rizik SŘV dopady chyb na úseku úkrytů pro zaměstnance pro případ potřeby, a provádí nápravu nedostatků.		
Míra, v jaké technický management SSŘV zvažuje při řízení rizik SŘV dopady chyb na úseku odzkoušení způsobu přechodu činnosti z obvyklých zařízení, komponent či systémů na záložní, a provádí nápravu nedostatků.		
Míra, v jaké technický management SSŘV zvažuje při řízení rizik SŘV dopady chyb na úseku dodržování pravidel preventivní údržby, a provádí nápravu nedostatků.		
Míra, v jaké technický management SSŘV zvažuje při řízení rizik SŘV dopady chyb na úseku navrženého postupu (režimu) práce, a provádí nápravu nedostatků.		
Míra, v jaké technický management SSŘV zvažuje při řízení rizik SŘV dopady chyb na úseku výcviku obsluhy technických zařízení, a provádí nápravu nedostatků.		
Míra, v jaké technický management SSŘV zvažuje při řízení rizik SŘV dopady chyb na úseku zajištění funkčnosti bariér a dodržování limit a podmínek při kritických operacích, a provádí nápravu nedostatků.		

Míra, v jaké technický management SSŘV zvažuje při řízení rizik SŘV dopady chyb na úseku dodržování stanovených reakcí na změny, a provádí nápravu nedostatků.		
Míra, v jaké technický management SSŘV provádí konkrétní pracovní úkony v provozu a realizuje odpovědnost za bezpečnost úkonů a bezpečnost SŘV.		
Míra, v jaké kritický pracovník SSŘV má vzdělání pro provádění konkrétních pracovních úkonů.		
Míra, v jaké kritický pracovník SSŘV má výcvik a dovednost pro provádění konkrétních úkolů.		
Míra, v jaké kritický pracovník SSŘV má povědomí o rizicích a bezpečnosti.		
Míra, v jaké kritický pracovník SSŘV dodržuje pravidla kultury bezpečnosti.		
Míra, v jaké kritický pracovník SSŘV má schopnost a motivaci dodržovat výrobní předpisy a pravidla správného nakládání s odpady.		
Míra, v jaké kritický pracovník SSŘV může mít nekalý úmysl.		
Míra, v jaké kritický pracovník SSŘV chápe provázanost technického zařízení se zařízeními IT.		
Míra, v jaké je kritický pracovník SSŘV schopen rozpoznat selhání propojení technického zařízení se zařízeními IT a zajistit odezvu dle předpisů.		
Míra, v jaké je kritický pracovník SSŘV schopen provést okamžitou úpravu propojení technického zařízení se zařízeními IT v zájmu zajištění bezpečnosti.		
Míra, v jaké je kritický pracovník SSŘV schopen zabránit narušení propojení technického zařízení se zařízeními IT.		
Míra, v jaké kritický pracovník SSŘV chápe a realizuje odpovědnost za bezpečnost úkonů.		
Míra, v jaké kritický pracovník SSŘV dodržuje provozní předpisy.		
Míra, v jaké kritický pracovník SSŘV má motivaci provádět úkony bezpečně a správně nakládat s odpady.		
Míra, v jaké pomocný personál SSŘV může mít nekalý úmysl.		
Míra, v jaké je pomocný personál SSŘV schopen rozpoznat selhání propojení technického zařízení se zařízeními IT a informovat dle předpisu.		
Míra, v jaké je pomocný personál SSŘV schopen zabránit narušení propojení technického zařízení se zařízeními IT.		

Míra, v jaké hardware I&C SŘV podporující provoz je zabezpečené proti dopadům pohrom určeným dle přístupu All-Hazard-Approach [74], které jsou možné v SŘV a okolí.		
Míra, v jaké software I&C SŘV podporujícího provoz je zabezpečené proti dopadům pohrom určeným dle přístupu All-Hazard-Approach [74], které jsou možné v I&C SŘV a okolí.		
Míra, v jaké software I&C SŘV podporujícího provoz respektuje limity technických zařízení při různých podmínkách.		
Míra, v jaké software I&C SŘV podporujícího provoz respektuje odpovědnosti osob stanovené legislativou.		
Míra, v jaké software I&C SŘV podporujícího provoz podporuje řízení procesů (proces safety management).		
Míra, v jaké software I&C SŘV podporujícího provoz podporuje integritu řízení (integrity safety management)		
Míra, v jaké software I&C SŘV podporujícího provoz respektuje limity obsluhy a cestujících ve vlaku při různých podmínkách.		
Míra, v jaké kanály pro přenos informací technických i organizačních v SŘV jsou zabezpečené proti dopadům pohrom určeným dle přístupu All-Hazard-Approach [74], které jsou možné v I&C SŘV a v okolí.		
Míra, v jaké je zajištěn přenos informací technických i organizačních v I&C SŘV při selhání informační infrastruktury.		
Míra, v jaké je zabráněno nakažení kritických informačních systémů SŘV červy, útokům hackerů apod.		
Míra, v jaké software I&C SŘV podporujícího provoz je schopno informovat o nedostupnosti dat, anebo o selháních systému.		
Míra, v jaké software I&C SŘV podporujícího provoz rozpozná útok, neprovede úkon a informuje obsluhu.		
Míra, v jaké platná legislativa vyžaduje od SSŘV zajištění integrální bezpečnosti SŘV.		
Míra, v jaké platná legislativa stanovuje odpovědnost SSŘV za bezpečnost SŘV.		
Míra, v jaké stát zajišťuje kvalitu vzdělání o rizicích a bezpečnosti.		
Míra, v jaké stát provádí dozor nad integrální bezpečností SŘV.		
Míra, v jaké stát prosazuje u SSŘV opatření podporující integrální bezpečnost SŘV.		
Míra, v jaké stát monitoruje integrální bezpečnost SŘV.		

Míra, v jaké stát kontroluje v SSŘV dodržování požadavků BOZP.		
Míra, v jaké kontroluje SSŘV dodržování požadavků ochrany životního prostředí.		
Míra, v jaké stát kontroluje SSŘV dodržování požadavků ochrany spotřebitele.		
Míra, v jaké stát spolupracuje s SSŘV při zvládnutí nouzových situací a zajišťování bezpečnosti SŘV v kritických situacích.		

Hodnocení konkrétního případu, tj. hodnocení souboru očekávaných variant provozu systému řízení vlaků dle tabulky 9 musí dělat tým specialistů z různých odborů nezávisle při použití klasifikační stupnice (0-5) a konceptu „čím vyšší hodnota, tím vyšší riziko“ [78] s pomocí stupnice v tabulce 10.

Tabulka 10. Stupnice pro stanovení míry rizika; N = pětinásobku počtu kritérií v tabulce 9, tj. N = 1315.

Míra rizika	**Hodnoty v % N**
Extrémní – 5	Více než 95 %
Velmi vysoká – 4	70–95 %
Vysoká – 3	45–70 %
Střední – 2	25–45 %
Nízká – 1	5–25 %
Zanedbatelná – 0	Méně než 5 %

V praxi se osvědčil tým [2,38,39], který v daném případě je složený z: pracovníka veřejné správy odpovědného za bezpečnost území; pracovníka veřejné správy odpovědného za dozor nad provozem systému řízení vlaků; pracovníka systému řízení vlaků, odpovědného za řízení rizik; pracovníka odborné instituce pro posuzování bezpečnosti systému řízení vlaků – např. z technické / kybernetické inspekce; a pracovníka Integrovaného záchranného systému odpovědného za odezvu na havárie a selhání technických děl. Výsledná hodnota u každého kritéria je medián, přičemž v případě velkého rozptylu hodnot u některého kritéria je třeba, aby pracovník veřejné správy odpovědný za bezpečnost území zajistil další šetření, na kterém každý hodnotitel sdělí zdůvodnění svého hodnocení v předmětném případě a na základě panelové diskuse nebo brainstormingu se určí výsledné hodnocení.

6.4. Výsledky Českých expertů na úseku zabezpečení železniční dopravy

Vlak je složitý systém systémů, který má povahu socio-kyber-fyzickou. Jeho zabezpečovací systém má povahu kyber-fyzickou. Zejména v čase, kdy je v pohybu. Vedle pevných prvků, jako jsou kola, dveře, okna nebo sedačky se skládá i z dalších částí.

Při provozu vlaku musíme počítat s cestujícími, kteří mají v dnešní době větší nároky na komunikační služby během cesty. Pro posádku a cestující pak musíme zajistit jistou úroveň komfortu, světlo, teplo nebo toalety. Vlak obsahuje podsystémy, které ovládají a kontrolují správnou a bezpečnou funkci jeho částí, jako jsou například dveře. Máme zde řídící systémy pro strojvedoucího. Další systémy vlaku pak slouží jako podpora pro centrální řídící systémy železnice, se kterými vlak komunikuje. V neposlední řadě pak musí řídící systém vlaku obsahovat funkce a opatření pro zvládání nouzových a kritických situací.

Řada těchto systémů byla v minulosti, nebo ještě je ovládána z vlaku samotného, manuálně, nebo semi-automaticky. Při původním nastavení celý systém závisel na dohledu posádky nad veškerými jeho částmi a vzhledem k prostorové distribuci na ni kladl vysoké požadavky. Postupně se ale řada funkcí převádí na automatizované systémy s dohledem v kabině strojvedoucího, nebo na pozemní centrále. Lidský faktor sice nadále hraje roli, ale při správném nastavení systémů a školení na něj nejsou kladené takové požadavky [106,107].

Automatizace vytváří kyber-fyzický systém. Rozhraní mezi fyzickým a kybernetickým prostorem je místem vzniku nových rizik. Je proto nutné zavádět nové principy a opatření pro jejich pokrytí. V rámci bezpečnostních systémů kyber-fyzických systémů jsou pak běžně převáděné ověřené principy a přístupy z fyzického prostoru do prostoru kybernetického. Jedním takovým přístupem je uzavření a segmentace jednotlivých částí prostoru podle potřeby jeho zabezpečení a rozdílného přístupu [106,107].

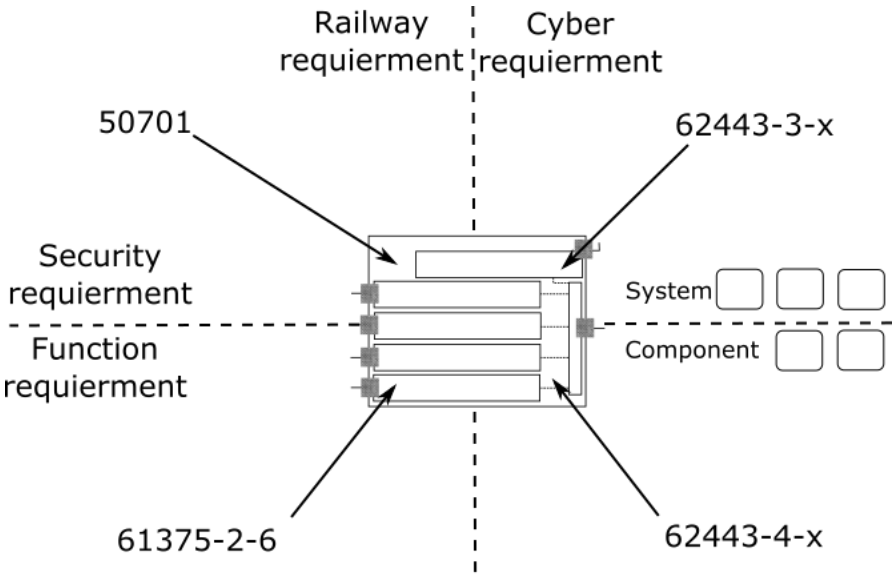
Železnice je otevřený komplexní systém. V rámci lidského systému je propojená s řadou dalších systémů a musí tak při zajištění zabezpečení a bezpečnosti v rámci přístupu systému systémů (SoS) respektovat propojení s ostatními systémy. V rámci dlouhé historie a tradice byly zavedeny postupy na řešení konfliktů s ostatními systémy v území, jako jsou například ostatní dopravní infrastruktury, nebo lidská sídla [106,107].

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

Na rozdíl od provázanosti mezi systémy ve stejném (fyzickém) prostoru se kyber-fyzický systém vypořádává s provázaností ve dvou prostorech s vlastními pravidly fungování. Zajistit správné fungování je tak mnohem náročnější [106,107]. Řešení konfliktu požadavků mezi kybernetickou a fyzickou částí je nutné ve všech fázích života kyber-fyzického systému. Následující text je zaměřen pouze na problematiku první fáze, kdy potřebujeme navrhnout bezpečnou architekturu komunikační brány vlaku tak, aby respektovala požadavky obou prostorů v rámci jejichž průniku se nachází.

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

V rámci vnitřního rámce vyžadujeme správné plnění funkcí certifikovaným produktem. Funkční požadavky mohou vycházet jak z kybernetické, tak z fyzické části systému. Vedle funkčních požadavků pak sledujeme i bezpečnostní požadavky (obrázek 12). Systém musí být opět zabezpečen proti hrozbám a ohrožením fyzické i kybernetické povahy.



Obr. 12. Vnitřní certifikační rámec kybernetické brány vlaku..

Zatímco vnitřní certifikační rámec klade požadavky přímo na certifikovaný produkt, vnější certifikační rámec se dotýká spíše prostředí vývoje a prostředí instalace. Nebývá tak certifikován přímo s produktem. Roli hrají především dvě normy. První se zabývá řízením zabezpečení informací v prostředí vývoje ISO/IEC 27001 [70]. V případě snadného odcizení informací o produktu klesá i jeho důvěryhodnost.

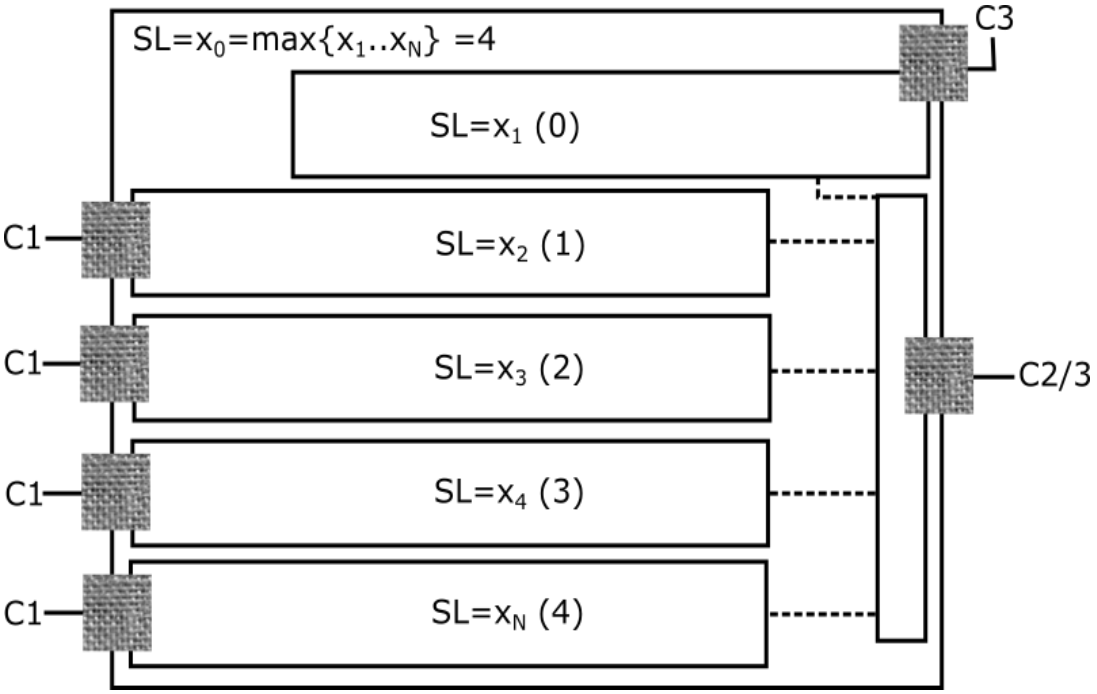
V celém rámci funkčních a bezpečnostních požadavků chybí ještě požadavky, které jsou spojené s nejdůležitějšími veřejnými zájmy lidského systému. Kyber-fyzický systém proto vyžaduje zvážení i požadavků na bezpečí lidí. Zvážení a implementace těchto požadavků je explicitně požadováno standardem TS 50701 [94]. Jejich určení je však velmi specifické vzhledem k místu instalace a jeho okolního prostředí. V souvislosti s tím lze zmínit normu ČSN / EN 50126-1 [16], v rámci, které lze předmětné požadavky definovat.

Další vnitřní vlakové systémy by na základě požadavků normy IEC 61375-2-6 [108] měly být kategorie 1. Požadavky na kategorie sítí opět definujeme podle normy ISA/IEC 62443 [7]. Výsledná struktura je znázorněná na obrázku 13.

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

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

Ve výzkumu [106,107] se zabýváme využitím MILS platformy pro potřeby komunikačního dělení na kybernetické bráně vlaku. Optimalizace certifikačního cyklu platformy MILS je předmětem evropského projektu certMILS [109]. Sestavení požadavků a jejich verifikace pro různá prostředí se vyvíjí pod vlivem nových norem.



Obr. 13. Diagram komunikačních kanálů v kybernetické bráně vlaku.

S novými komunikačními technologiemi rostou i požadavky na zabezpečení komunikačních systémů jednotlivých infrastruktur. V případě železnice jde o vytvoření nové technické specifikace TS 50701 [94], která přenáší kybernetické požadavky do prostředí dráhy. Nové požadavky se v něčem překrývají s požadavky starými a v něčem je rozšiřují. Jsou i aspekty kybernetických norem, jejichž překlad pro potřeby praxe může vytvořit jisté kontroverze.

S nárůstem funkcí, které jsou ve vlaku řízeny digitálně, roste počet potenciálně izolovaných segmentů, které kybernetická sít vlaku může obsahovat. Jde o celkem 5 různých vnitřních částí sítě vlaku [106,107].

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

Jelikož jednotlivé části sítě jsou spojené s různými požadavky na zabezpečení a sdílejí přitom společnou komunikační bránu, je potřeba zajisti důslednou ochranu hranic jednotlivých zón. Segmentace komunikace musí být zabezpečená tak, aby narušení jedné části, neohrozilo funkce jiných. Jednou z cest je aplikace platformy MILS [110].

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

V dnešní době je platforma MILS požívána v nejrůznějších oblastech lidského systému s vysokou kritičností rizik v kyberprostoru. Vnitřní prostředí výpočetní jednotky je rozděleno do nezávislých oddílů, které mohou sloužit pro zajištění bezpečnosti, ale i pro poskytování dalších funkcí. Platforma MILS tak může souběžně podporovat kritické funkce s vysokými požadavky na zabezpečení a služby v otevřeném prostoru pro cestující s širokým vektorem útoku. Ztráta důvěryhodnosti otevřené části přitom nijak neohrožuje ostatní oddělení.

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

Odpovědí na uvedené potřeby je platforma MILS, která se dá snadno implementovat i v podmínkách pohybujícího se dopravního prostředku. Zajištění nezávislosti jednotlivých oddělení platformy MILS vyžaduje implementaci bezpečnostní architektury ve všech rovinách technologie, ať už se jedná o roviny řídící, nebo funkční. V některých případech komunikační brány je používán operační systém PikeOS [111] jako hypervisor. Zařízení je ve fázi verifikace a certifikace v rámci evropského projektu certMILS [109] a připravuje se jeho testování v podmínka české železnice v rámci projektu ADMORPH [112].

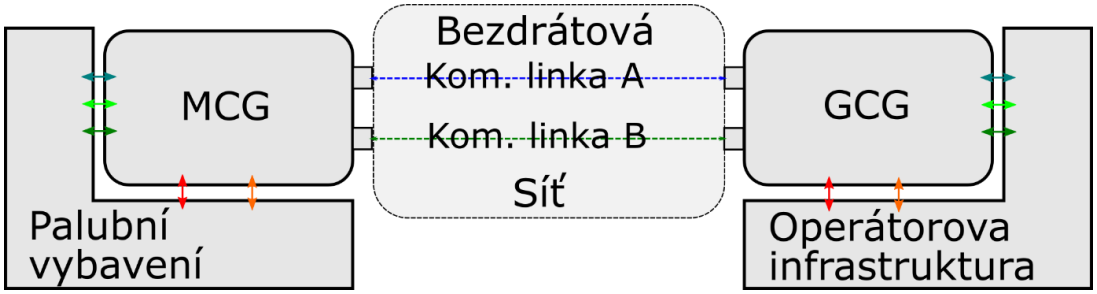
Vlak se pohybuje, a proto je třeba řešit problémy mobilní komunikační brány (MCG). Komunikace nemůže probíhat skrze uzavřený komunikační systém, ale musí probíhat otevřeným prostorem skrze distribuované komunikační portály, pozemní komunikační bránu (GCG). Na základě výše uvedených poznatků MCG musí být vybavena tak, aby umožnila identifikaci a autentizaci osob či procesů s oprávněným přístupem. Zároveň musí být zajištěna proti neoprávněnému vniknutí.

Základním problémem je komunikace mezi vlaky a komunikace vlaku s dispečinkem pomocí CBTC. Protože vlak se pohybuje, tak dochází vlivem vnějších podmínek k proměně podmínek spojení mezi důležitými subjekty, které mají kyber-fyzickou povahu. To znamená, že je třeba vyřešit úskalí spojená s uvedeným problémem.

Konstrukce MCG musí zajistit klasické funkce vstupní brány, jako je identifikace a autentizace, zamezení vstupu neoprávněným osobám a procesům, dostatečnou kapacitu vyžadované komunikace. Protože se ale nachází v otevřeném prostoru, jak fyzickém, tak kybernetickém, často v pohybu, je naše kontrola nad podmínkami prostředí omezená. MCG tak potřebuje být schopna dynamicky reagovat na změny prostředí způsobené úmyslnými útoky či neúmyslnými změnami v systému. Schopnost adaptace musí být dána MCG při její konstrukci. Příkladem je MCG na obrázku 14, které využívá segmentace systému za využití přístupu Multiple Independent Levels of Security (MILS). MILS umožňuje odezvu na problémy na MCG za pomocí redundance a redistribuce zdrojů, popřípadě změny v softwarových procesech.

Mobilní komunikační brána je kyber-fyzické zařízení, které zajišťuje spojení pohyblivého systému jako je vlak s pevnou pozemní infrastrukturou. Mobilní komunikační brány se musí řídit celou řadou standardů a pravidel, určených oblastí jejich nasazení. V případě vlaku je soupis standardů v rámci certifikačního cyklu podrobněji rozepsán v článku [113]. V rámci komunikace mezi vlakem a pozemní infrastrukturou máme na obou stranách komunikační brány, mezi kterými komunikace probíhá. Brána na straně pozemní infrastruktury se nazývá pozemní komunikační brána (GCG) a brána na

straně mobilního systému, jako je vlak, se nazývá mobilní komunikační brána, obrázek 14.



Obr. 14. Schéma komunikace mezi vlakem a pozemní infrastrukturou.

Kybernetická síť vlaku je rozdělena do několika oblastí, jako jsou služby veřejnosti, pohodlí ve vlaku, pomocné systémy vlaku, řídící systémy vlaku a kritické systémy vlaku [94]. Komunikace pro uvedené oblasti může být zajištěna nezávislými komunikačními kanály. Praktičtější je ale použití jednoho komunikačního kanálu, kdy komunikační brány na obou stranách podporují komunikace s odlišnou kritičností.

Pro zajištění komunikací s rozdílnou kritičností, využívá námi navrhovaná brána principů většího počtu nezávislých úrovní bezpečnosti (MILS) [110,114]. Komunikační brány na obrázku 14 dále obsahují redundantní komunikační linky, pro případ bezpečnostních incidentů na hlavní lince A. Bezdrátová komunikace probíhá otevřeným systémem. Jedná se o pásmo, vyhrazené operátorem pro potřeby provozovatele vlaků. Není ale možné zaručit vniknutí cizích činitelů.

Bezpečnost kybernetické sítě vlaku je tak nutné zajistit na straně komunikační brány vlaku. Komunikační brána vlaků, MCG, která zajišťuje bezpečnou komunikaci pro různé systémy vlaku za pomocí operačního systému PikeOS [111] a principů MILS je na obrázku 15.

Na obrázku 15 vidíme i strukturu GCG, která reflektuje strukturu MCG. Struktura MCG:

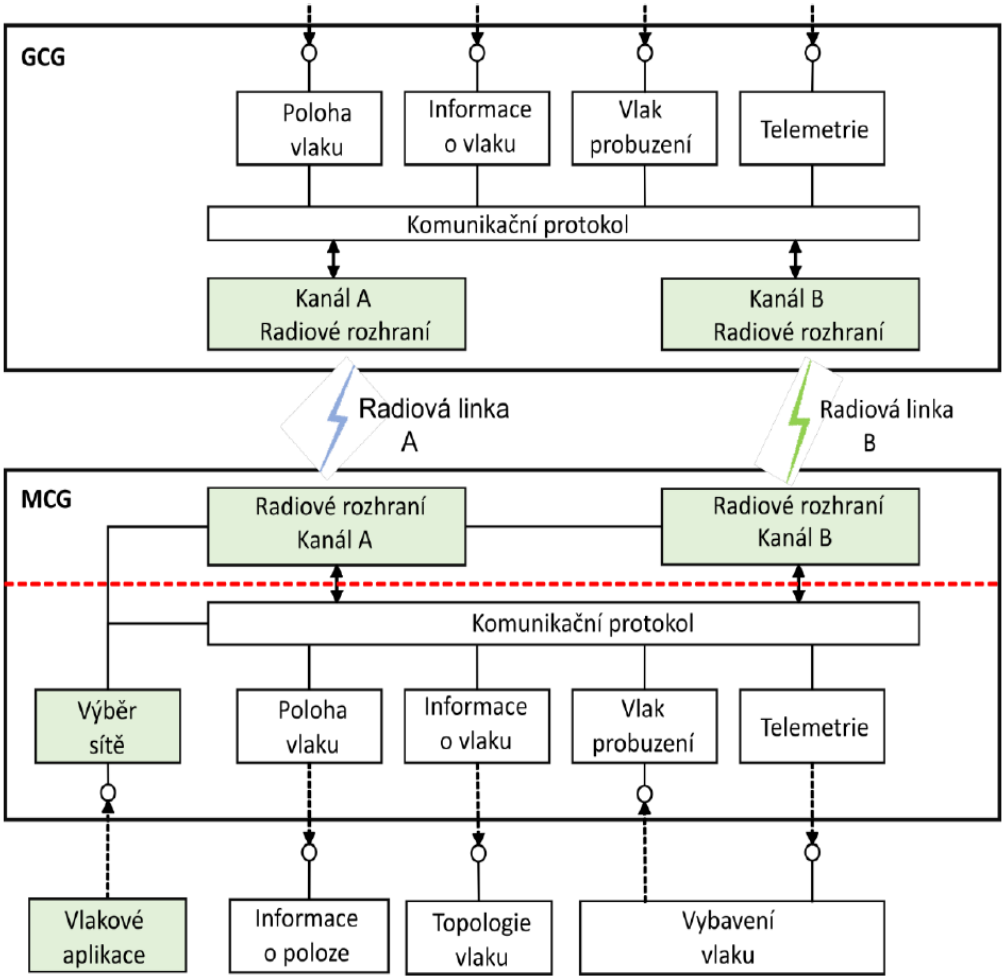
- vychází z funkčních požadavků vlakového dopravce
- reflektuje normu TS50701 [94].

Zabezpečení jednotlivých zón 349 pak vychází z bezpečnostních požadavků standardu IEC 62443 [7].

Jako jeden z prvních úkonů tak byla provedena analýza rizik v rámci daného kontextu umístění v síti. Během analýzy rizik bylo identifikováno 28 specifických hrozeb [45], jejíž zdroj se nacházel uvnitř i vně systému železniční infrastruktury. Identifikovaná rizika byla vyhodnocena a k nim byla navrhnuta opatření v rámci požadavku z normy IEC 62443.

V rámci aktuální situace v oblasti komunikační bezpečnosti v místě nasazení (u českého železničního dopravce) stačí k dosažení požadované bezpečnosti opatření nastavená před uvedením do provozu. S rostoucími nároky na bezpečnost v oblasti komunikací je ale potřeba vyvinout nástroje, které umožní provozovateli reagovat na vzniklé situace při provozu.

V rámci identifikovaných hrozeb jsme vytipovali hrozby, které mají potenciál s růstem do budoucna, které je zároveň možné přímo nebo nepřímo monitorovat. Vybraná rizika jsou uvedena v tabulce 11.



Obr. 15. Struktura MCG a GCG rozdělená do jednotlivých podporovaných oblastí komunikace.

Tabulka 11. Vybraná rizika komunikační brány. Rizika, pro která je MCG vybavena monitoringem.

Oblast rizika	**Příčina rizika**
1	Útočník se připojí přes bránu a bude manipulovat se systémy vnitřní sítě.
2	Útočník se připojí k bráně a dostane se k firemním informacím.
3	Selhání hardwaru
4	Chybná provozní vstupní data.
5	Velké množství neoprávněných přístupů, zahlcení služeb.
6	Komunikace nebude probíhat kvůli nedostatku zdrojů.

V tabulce 11 je sice uvedeno 6 vybraných rizik, pro které bude MCG vybavena monitoringem. To však neznamená, že brána je vybavena 6 rozdílnými monitorovacími systémy, každý pro jednotlivá rizika. Některá rizika lze odhalit jedním monitoringem, ale

stejně tak platí, že pro odhalení jiných rizik by bylo potřeba připravit monitoring pro různé scénáře realizace rizika. Rizika a jejich scénáře jsme si proto rozdělili do tří oblastí pro potřeby dalšího zpracování.

První oblast se zabývá správným fungováním fyzické části MCG. Špatné fungování hardwaru může být způsobeno technickými chybami, pozměněním funkcí systémů útočníkem, nebo cíleným přetížením MCG.

Druhá oblast se týká informačního toku, který do brány vstupuje. Vedle kvality informačního toku, zda nedošlo k jeho pozměnění, můžeme sledovat i kvantitu, tedy zda jeho hustota odpovídá standardním hodnotám.

Třetí oblast je potom spojena s aktivitami na MCG, které mohou souviset s pokusy o vniknutí či úspěšným vniknutím do MCG.

Rizika z tabulky 11, respektive jejich scénáře dopadů pak přidělíme do jednotlivých oblasti. Každá ze tří oblastí je pak spojena s monitorovacím systémem, který je popsán dále. S rozvojem technologií se může zvýšit množství monitorovaných rizik. Vždy ale bude nutné vybírat nejkritičtější z nich s ohledem na dostupné zdroje MCG.

Na základě oblastí rizik, které jsou uvedeny v tabulce 11 se vyvíjí tři různé systémy pro monitoring jevů. Každý z monitorovacích systémů můžeme rozdělit na:

1. Síť čidel či detektory, které sledují veličinu, nebo veličiny spojené s monitorovaným jevem.
2. Přenosový kanál s protokolem zpráv,
3. Vyhodnocování sledovaných veličin v čase.

V rámci námi sestavované MCG je pro přenos informací mezi detektory, čidly na jedné straně a vyhodnocením na straně druhé použit protokol MQTT [115] a využity jsou již nastavené informační kanály. Výpočetní jednotka pro vyhodnocení může být v budoucnu umístěna ve vlaku pro zvýšení jeho nezávislosti při adaptivitě. Brány, které vytváříme počítají s jednotným serverem pro monitoring všech aktivních MCG. V souvislosti s informacemi, které se dostanou do monitorovacího serveru, je potřeba nastavit správně limity pro sledované veličiny.

Monitorovací čidla či detektory jen zřídka rozpoznají problém jako takový, pouze nastavení limitů pro definování zelených, oranžových a rudých oblastí pro sledované veličiny vede k spuštění poplachu, či jiným postupům. Špatné nastavení limitů může vést k necitlivosti monitoringu, nebo naopak k falešným poplachům. Rozsáhlá proměnlivost železniční infrastruktury pak může vést ke kolísavosti provozních parametrů.

Pro jednoduchost, sdílejí všechny tři monitorovací systémy komunikační protokoly a server pro vyhodnocení monitoringu. Liší se pak v použitých čidlech a detektorech jednotlivých monitorovacích systémů. Jednotlivé systémy monitoringu můžeme označit jako:

1. Fyzikální monitoring MCG.
2. Komunikační tok do MCG.
3. Narušitel na MCG.

Hlavním monitorovacím systémem sestavované MCG je monitoring fyzikálních parametrů brány. V rámci CPS (kyber-fyzický systém), jsou kybernetické procesy podporovány technologiemi zastoupenými ve fyzickém prostoru. Při změnách

v kybernetických procesech tak může dojít ke změně stavů v rámci fyzické části systému. Fyzikální monitoring může ale zachytit i selhání fyzické části CPS.

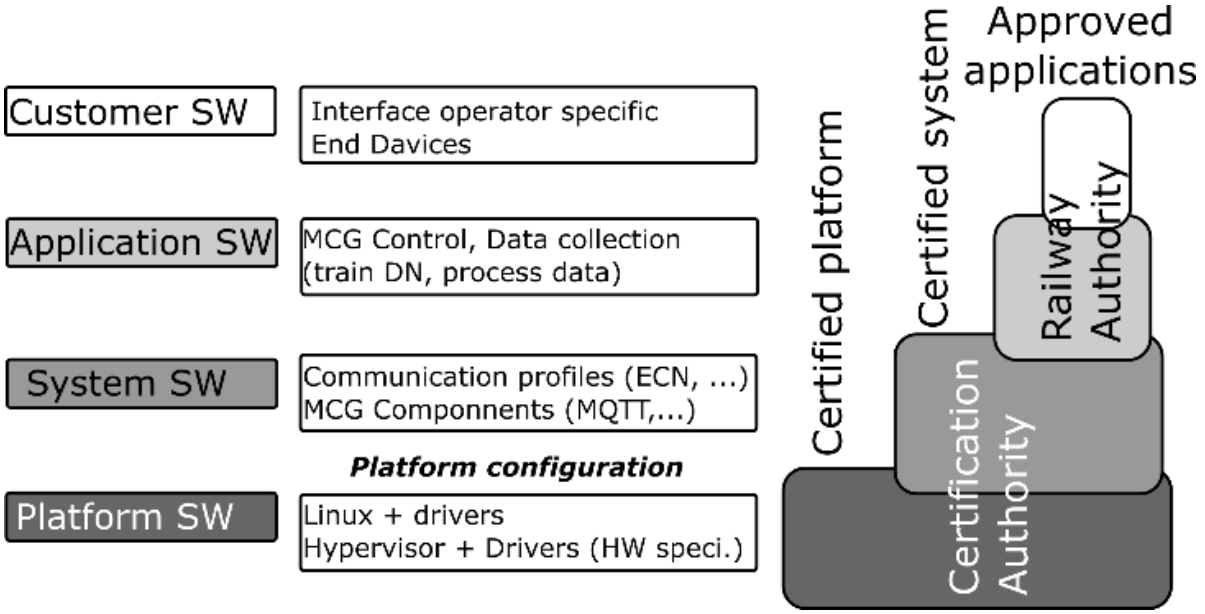
Fyzikální monitoring se bude skládat z několika čidel. V současné době jsou implementována čidla na měření teploty na CPU a na zdroji energie [116]. Teplotní čidlo bude sledovat i stav jednotlivých periferií, které budou do brány připojeny. Poslední teplotní čidlo pak bude sledovat referenční teplotu prostředí. Dalším sledovaným parametrem je vlhkost vnitřního prostředí. Připravuje se i umístění čidel na měření elektrického napětí v systému.

Hlavním cílem fyzikálního monitoringu je sledování intenzity aktivit klíčových součástí hardwaru. Intenzita výkonu jednotlivých součástí hardwaru má standardní provozní pásmo hodnot. Výrazný odklon od těchto hodnot pak může odhalit mimoprovozní aktivity na MCG dříve, než dojde ke kritickému přetížení systému například vlivem DDoS útoku, či k jiným nežádoucím změnám. Fyzikální monitoring byl vyvinut s partnery v rámci projektu ADMORPH [112].

Komunikační tok do MCG je monitorován čistě na základě statistiky odeslaných a příchozích paketů. Informace o intenzitě paketů, přijaté pakety a chybové pakety, se ukládají. Případný odklon od běžných provozních intenzit, či zvýšení zamítnutých paketů je pak posouzen. Monitoring komunikačního toku na MCG je implementován v rámci projektu ADMORPH jako referenční k fyzikálnímu monitoringu.

Aktivity narušitele lze detekovat i přes fyzikální změny na MCG. Pokud se ale bude narušitel chovat dostatečně nenápadně, může jeho aktivita zůstat skryta v rámci tolerance odchylek. Proto je potřeba připravit další monitorovací systém pro aktivity uvnitř MCG.

V rámci projektu COSMOS [117] počítáme s vývojem systému pro sledování softwarových procesů. Softwarová reprezentace MCG předpokládá 4 rozdílné úrovně struktury, obrázek 16. Každá s těchto úrovní je pak spojena s určitými procesy pro ni povolenými. Zatím co procesy na úrovní operátorem specifikovaného softwaru mohou mít jistou míru fluktuace. Odhalení provozních odchylek v nižších vrstvách může být citlivější.



Obr. 16. Struktura softwaru MCG; převzato z [117].

Odezva MCG je podmíněna zaznamenáním nežádoucí situace monitoringem. Monitorovací systémy odesílají informace o MCG do serveru pro posouzení sledovaných veličin. Odezva pak začíná na tomto serveru. Monitorované veličiny jsou posuzovány na základě definovaného algoritmu a pokud dojde k vyhodnocení situace jako nouzová či kritická, je spuštěn příslušný poplach a s ním i odezva.

Rozvoj IT systémů je v dnešní době spojován s vývojem kognitivních funkcí umělé inteligence a její schopnosti reagovat na předložené problémy. Předmětný přistup je v oblasti kritické infrastruktury zatím velmi nebezpečný, protože kognitivní IT systémy potřebují čas na učení, nebo kladou velké nároky na počáteční naprogramování. Námi vytvářená MCG proto počítá s konzervativním přístupem, tj. s řízením dle nastavených pravidel. MCG řízená na základě pravidel má přesně dané chování, jak se má chovat při jisté definované situaci, tj. chová se zcela deterministicky.

Pro sledované veličiny, jako je teplota na jednotlivých čidlech, napětí, intenzita informačního toku, nebo množství zamítnutých paketů, máme čtyři oblasti, ve kterých se hodnota může pohybovat, obrázek 17.

Obr. 17. Oblasti, možného detekování sledovaných hodnot. Zelená odpovídá běžným provozním hodnotám.

Zelená je oblast předpokládaných provozních hodnot. Šedá oblast odpovídá hodnotám menším a signalizuje, že některý z vnitřních systémů neběží či nefunguje. Oranžová oblast značí překročení limity pro provozní parametry, nic méně může jít o překročení způsobené nekritickými vlivy. Červená je pak oblast vyžadující rychlou odpověď systému na situaci.

Pokud jsou sledované hodnoty v šedé oblasti, pak systém může používat alternativní komunikační kanál, obrázky 14 a 15. MCG nemá žádnou kontrolu nad interními vlaky nebo externími systémy provozovatele a může posílat varování pouze o příčině jejich poruchy. Zelená plocha nevyžaduje žádnou odpověď.

Oranžové a červené oblasti jsou spojeny se stejnou odpovědí. Rozdíl je v tom, že v případě oranžové oblasti je nejprve nutné porovnat tento výstup s výstupy z jiných monitorů. Odpověď se tedy nespouští bezprostředně, ale pouze po porovnání více dat. Pokud je podezření potvrzeno jinými sledovanými parametry nebo pokud je sledované množství v oranžové oblasti delší, spustí se stejný alarm jako v červené oblasti. Alarm se okamžitě spustí v červené oblasti.

Šedá oblast odpovídá nereálným datům a značí problém monitorovacího systémů. V šedé oblasti se mohou nacházet i parametry v daný moment neaktivních částí MCG. V prvním případě je opět nutná odezva.

Nástroje pro řízení odezvy musí být zavedeny v MCG proaktivně, obrázek 15, aby je MCG mohla použít v případě procesu adaptace. MCG z obrázku 15 má 2 komunikační kanály a další zdroje, které podporují tyto komunikační kanály. Musí být zajištěna nezávislost jednotlivých zón MCG, aby reakce na selhání kanálu nebo útok na kanál fungovaly.

MCG z obrázku 15 používá PikeOS [111] k naznačování přístupu MILS. Pokud je kanál A nebo jeden z jeho zdrojů ohrožen, systém se přepne na kanál B. kanál B má své vlastní prostředky a je nezávislý na kanálu A. Kanál B nebude ovlivněn selháním kanálu A útočník bude muset zahájit útok na kanál B od začátku. Kanál A se mezitím může restartovat ve snaze vyřešit technický problém. Nevyužívaný kanál je neaktivní, takže na něj není možné zaútočit.

Pro základní bezpečnost MCG je důležitá ochrana obrazu nastavení systému. Obraz MCG, ověřený výrobcem, digitálně podepsaný a šifrovaný je uzavřen v samostatné zóně. V případě jakéhokoliv problému tak můžou jednotlivé částí, nebo celý systém být automaticky restartovány a načteny podle uloženého obrazu.

Výzkum zacílený na aplikaci platformy MILS v praxi pokračuje ve spolupráci s odborníky v Evropské unii s cílem identifikovat opatření, která buď zabrání selhání, anebo při selháních zajistí kvalitní odezvu.

7. ZÁVĚR

Protože dnešní společnost je závislá na technických a kybernetických systémech, které přispívají k uspokojení základních potřeb lidí, tak se práce zabývá socio-kyber-fyzickými systémy, které potřebují pro svoji správnou funkci správné a včasné informace z reálného fyzického prostředí. Protože informační a komunikační systémy dokáží zpracovat informace rychleji než člověk, tak se automatizace stále více rozšiřuje.

Čím větší je úsilí lidí ke zlepšení a usměrnění procesů k jejich vyššímu ekonomickému užitku, tím je vyšší závislost lidské společnosti na informačních technologiích, a proto neustále vzrůstá potřeba vývoje uvedených technologií. Zlepšováním a usměrňováním procesů ve směru k ekonomickému užitku, zavádíme stále nová spojení, tj. vazby, a tím vytváříme systémy stále komplexnější, a tím i zranitelnější. Zranitelnosti vedou k selhání systémů v kritických podmínkách, které mají v mnoha případech dopady na bezpečí lidí, zajištění základních lidských potřeb a hlavních funkcí států. Proto také v oblasti informačních technologií hovoříme o kritické informační infrastruktuře, která je navíc propojena s ostatními technologiemi.

Na příkladech práce ukazuje, že zdroje rizik v kybernetickém systémů poškozují za jistých podmínek aktiva fyzických systémů i lidi. Proto jsou uvedeny požadavky na zabezpečení kyber-fyzických systémů u železniční dopravy, která je studována podrobně. Pro zajištění bezpečí lidí potřebujeme zajistit zabezpečení adekvátní funkce složitých kyber-fyzických systémů. K formování příslušných principů pro zajištění zabezpečeného a bezpečného kybernetického systému je zapotřebí použít teorii informací a konkrétně odvodit parametry, které ovlivňují informační výkon. Informační výkon je právě ta veličina, jejíž rozměr ovlivňuje kvalitu rozhodnutí, tj. čím vyšší je informační výkon, tím je vyšší pravděpodobnost správného rozhodnutí a naopak.

Dopravní infrastruktura a drážní systémy jsou složitými systémy systémů, a svou povahou socio-kyber-fyzickými systémy, které jsou závislé na informačních technologiích, ve kterých je potencionálně řada zranitelností, které mohou vést k závažným dopravním nehodám.

Analýza dopravních nehod vlaků v ČR ukazuje, že je třeba aplikovat automatické zabezpečovací systémy pro zvýšení bezpečnosti. Obecně je pravda, že ani automatizace není bezchybná, a proto je třeba zajistit její bezpečné provedení. Proto článek ukazuje způsob ochrany automatizovaných systémů řízení bezpečnosti vůči existujícím rizikům, který se systematicky vytváří v rámci projektů EU. V oblasti letectví je řízení letového provozu unifikované předpisy IATA.

Kvalita provozu poloautomatických a automatických systémů řízení. závisí jak na hardware, tak software systémů řízení. Velkou roli hraje propojení informačních systémů a systémů, které provádí konkrétní úkony, tj. systém označovaný I&C (information and control). Bezpečný provoz dopravních systémů zajistí jen bezpečný provoz I&C systému. Při automatizaci systémů řízení pro jejich bezpečnost je třeba řešit nejen projevy a ochranu faktorů technické a lidské, ale i kybernetické povahy. Práce ukazuje výsledy studia selhání dopravních systémů kvůli kybernetickým faktorům a jejich kombinaci s ostatními faktory. Na základě současného poznání je sestaven nástroj pro posouzení rizik, jejichž zdroje odpovídají reálnému světu (All-Hazard-Approach) a model řízení bezpečnosti složitého systému, který používá automatické řízení v čase. Jelikož

drážní doprava je vysoce důležitou součástí dopravní infrastruktury a její zabezpečení patří dnes mezi priority v Evropě, a především v České republice, jsou uvedeny konkrétní výsledky právě pro ni; pozornost je zaměřena na rizika, která souvisí s rozhraním kyber-fyzickým, protože právě tato oblast má dosud z pohledu zabezpečení i bezpečnosti spoustu neznámých, a tím i rizik.

V komunikačním věku jednadvacátého století vyžaduje bezpečnost kybernetické sítě vlaku rostoucí pozornost. Vlak jakožto CPS je ovlivňován z obou podsystémů. Chování vlaku ve fyzickém prostoru je spojeno s pohybem po rozsáhlé infrastruktuře, který ztěžuje dohled nad vlakem. Komunikace s operačním centrem v kybernetickém prostoru je pak vedena skrze otevřený komunikační prostor.

MCG musí být připravena reagovat na rostoucí hrozby. To znamená garantovat nejenom lepší pasivní bezpečnost podle aktuálních technických standardů, ale i vývoj aktivní bezpečnosti. Aktivní bezpečnost MCG nemůže spoléhat na včasný zásah lidského operátora, potřebuje vlastní schopnost adaptivity na vzniklé situace.

V souvislosti s tím jsme vyvinuli MCG, která je inherentně vybavena monitorovacími systémy pro odhalení nežádoucích jevů. V současné době testujeme MCG s monitoringem několika parametrů v provozních podmínkách. Množství a kvalita monitorovaných parametrů se může do budoucna zvětšit.

Schopnost adaptovat se na nové podmínky a odhalené hrozby musí být dána MCG už při vývoji. Naše MCG zatím využívá základní nástroje jako je redundance nebo obnovení částí systému. Zabýváme se i flexibilitou v přidělování zdrojů jednotlivým procesům. Tato flexibilita ale nesmí narušit výhody v otázkách bezpečnosti přístupu MILS.

Na závěr je třeba poznamenat, že ve srovnání s technickými systémy chybí při projektování kyber-fyzických systémů jasně stanovené limity a podmínky s ohledem na bezpečnost ve smyslu safety, která znamená i ochranu okolí. Autoři vidí problém v tom, že IT specialisté:

- se stále zabývají zabezpečením (používají pojem security)a mluví o bezpečnosti, a nezvažují bezpečnost ve smyslu safety, která znamená ohled i na okolí,
- nezvažuji dynamický vývoj světa a jeho vliv na limity a podmínky, které formují chování systémů; náhlé velké změny podmínek znamenají překročení limitů odolnosti systémů, což vede k selháním a haváriím.

LITERATURA

[1] PROCHÁZKOVÁ, D. *Zásady řízení rizik složitých technologických zařízení.* ISBN:78-80-01-06182-4. Praha: ČVUT 2017, 364 p. https://doi.org/10.14311%2FBK.9788001061824

[2] PROCHÁZKOVÁ, D. *Bezpečnost složitých technologických systémů.* ISBN 978-80-01-05771-1. Praha: ČVUT 2015, 208 p.

[3] KERTIS, T. Porovnání přístupů pro řízení bezpečnosti v dopravě. V: *Rizika podnikových a územních procesů a poznatky pro krizové řízení*. ISBN 978-80-01-06033-9. Praha: ČVUT 2016, pp. 34-59.

[4] ZAIRI, M. *Total Quality Management for Engineers*. Cambridge: Woodhead Publishing Ltd 1991.

[5] ČR. *ČSN EN 61508-1. Funkční bezpečnost elektrických/elektronických/ programovatelných elektronických systémů souvisejících s bezpečností – Část 1: Všeobecné požadavky.* Praha: ÚNMZ, 2005.

[6] ČR. *ČSN ISO/IEC 27000 (36 9790) Informační technologie – Bezpečnostní techniky – Systémy řízení bezpečnosti informací – Přehled a slovník.* Praha: ÚNMZ, 2010

[7] ISA. *ANSI/ISA–62443. Security for Industrial Automation and Control Systems: Concepts, Terminology and Models*. Washington, DC: ANSI 2007.

[8] ČR. *ČSN ISO/IEC 15408-1 Informační technologie - Bezpečnostní techniky – Kritéria pro hodnocení bezpečnosti IT - Část 1: Úvod a všeobecný model.* Praha: ČNI 2001.

[9] ČR. *Předpisy*. Letecká informační služba. Praha: Řízení letového provozu České republiky. http://lis.rlp.cz/predpisy/predpisy/index.htm

[10] ČR. *ČSN ISO/TS 16949 (01 0329) Systémy managementu jakosti - Zvláštní požadavky na používání ISO 9001:2000 v organizacích zajišťujících sériovou výrobu a výrobu náhradních dílů v automobilovém průmyslu.* Praha: ČNI 2001.

[11] VDA. *Qualitäts Management Center im Verband der Automobilindustrie e.V*. Berlín, http://vda-qmc.de

[12] ISO. *ISO 26262-1:2011 Road Vehicles -- Functional Safety -- Part 1: Vocabulary.* Berlín: ISO, 2011 https://www.iso.org/obp/ui/#iso:std:iso:26262:-1:ed-1:v1:en

[13] EU. *Directive 2002/49/EC of the European Parliament and of the Council of 25 June 2002 Relating to the Assessment and Management of Environmental Noise* - Declaration by the Commission in the Conciliation Committee on the Directive relating to the assessment and management of environmental noise. Brussels: EC 2002.

[14] EU. *Regulation 402/2013 on the CSM for Risk Assessment and Rrepealing.* Regulation 352/2009. Brussels: EC 2013.

[15] UNIFE. *IRIS Rev. 02.1. International Railway Industry Standard.* Belgie: UNIFE, 2012. http://www.iris-rail.org/

[16] ČR. *ČSN EN 50126-1 (333502). Drážní zařízení - Stanovení a prokázání bezporuchovosti, pohotovosti, udržovatelnosti a bezpečnosti (RAMS): Část 1: Základní požadavky a generický proces.* Praha: ČNI 2001.

[17] ČR. *ČSN EN 50129 (34 2680). Drážní zařízení – Sdělovací a zabezpečovací systémy a systémy zpracování dat – Software pro drážní řídicí a ochranné systémy.* Praha: ÚNMZ, 2012.

[18] LEITL, R. *Spolehlivost elektrotechnických systémů*. Praha: SNTL1990.

[19] KERTIS, T. Introduction of Modern Approaches of Ensuring Safety into Business Processes in Railway Industry. V: *Vybraná rizika podnikových procesů 2015*. ISBN 978-80-01-05831-2. Praha: ČVUT 2015, pp. 26-38,

[20] ICAO. *Doc 9859 Safety Management Manual (SMM).* 3rd edition. International Civil Aviation Organization, 2013. ISBN 978-929-2492-144. http://www.icao.int /safety/SafetyManagement/Documents /Doc.9859.3rd%20Edition.alltext.en.pdf

[21] Ministerstvo dopravy ČR. L17. Ochrana mezinárodního civilního letectví před protiprávními činy. Č.j. 465/2013-220-AVS/2

[22] EU. ARTEMIS Joint Undertaking - Integrated Design and Evaluation Methodology. In: *SESAMO: Security and Safety Modelling.* http://sesamo-project.eu/sites/default/files/downloads/publications/integrated-design-and-evaluation-communication-material.pdf

[23] IEEE. *ARINC 653 An Avionics Standard for Safe, Partitioned Systems*. Wind River Inc. 2008, 30 p.

[24] MOOS, P. MALINOVSKÝ, V. *Informační systémy a technologie.* Edice monografií NNW. ISBN 80-903298-5-3. Praha: ČVUT 2006.

[25] NOVOBÍLSKÝ, P., KERTIS, T., PROCHÁZKOVÁ, D., PROCHÁZKA, J. Cyber Security of Metropolitan Railway Communication Infrastructure. In: *Risks of Business and Territorial Processes*. ISBN 978-80-7561-021-8. Ústí nad Labem: UJEP 2016, pp.78-91.

[26] KERTIS, T. Porovnání přístupů pro řízení bezpečnosti v dopravě. In: *Rizika podnikových a územních procesů a poznatky pro krizové řízení*. ISBN 978-80-01-06033-9. Praha: ČVUT 2016, pp. 34-59.

[27] KERTIS, T., PROCHAZKOVÁ, D. Railway Accidents in the Czech Republic, Causes of Risks and Their Mitigation. In: *Safety and Reliability – Theory and Applications.* ISBN 978-1-138-62937-0. London: Taylor & Francis Group 2017, pp. 1667-1673.

[28] KERTIS, T., PROCHAZKOVA, D. Information Power Supporting the Rail Systems Safety. In: *Proceedings of International European Safety and Reliability Conference, ESREL2018*. ISBN 978-0-8153-8682-7. London: Taylor & Francis Group 2018; ISBN 978-1-351-17466-4. https://www.ntnu.edu/esrel2018; pp. 2939-2947.

[29] KERTIS, T., PROCHÁZKOVÁ, D. Cyber Security of Underground Railway System Operation. In: *2017 Smart City Symposium Prague (SCSP)*, Prague, 2017, pp. 1-6. doi: 10.1109/SCSP.2017.7973839

[30] PROCHAZKA, J., NOVOBILSKY, P., PROCHAZKOVA, D. Cybersecurity of Railway Network Management and Partitioning. *Problemy kolejnictwa.* ISSN 0552-2145. 64 (2020) 189, pp. 57-64; 125-131.

[31] MOOS, P., ZELINKA, T., MALINOVSKÝ, V. *Telekomunikační služby*. ISBN 978-80-01-03598-6. Praha: ČVUT 2007, 176 p.

[32] PROCHÁZKOVÁ, D. *Základy řízení bezpečnosti kritické infrastruktury*. ISBN 978-80-01-05245-7. Praha: ČVUT 2013, 223 p.

[33] QUANTERION SOLUTIONS. https://www.quanterion.com/KnowledgeBase/ReliabilityToolkit.shtml.

[34] BARUH, H. *Applied Dynamics*. New York: CRC Press 2014.

[35] MAIXNER, L. *Navrhování automatických výrobních systémů*. Praha: NTL 1980.

[36] KLAS, A. Krok za krokem k výnosné automatizaci montážních linek. *MM průmyslové spektrum*, 2004, 28 p.

[37] ZLOCHOVÁ, M. Optimalizace výrobních buněk. *Úspěch - Produktivita a inovace v souvislostech.* 1 (2012), 1.

[38] PROCHÁZKOVÁ, D., PROCHÁZKA, J., LUKAVSKÝ, J., BERAN, V., ŠINDLEROVÁ, V. *Řízení rizik procesů spojených se zhotovením a jeho uvedením do provozu*. ISBN 978-80-01-06609. Praha: ČVUT 2019, 207 p. https://doi.org/10.14311%2FBK.9788001066096

[39] PROCHÁZKOVÁ, D., PROCHÁZKA, J., LUKAVSKÝ, J., DOSTÁL, V., PROCHÁZKA, Z., OUHRABKA, L. *Řízení rizik procesů spojených s provozem technických děl během jejich životnosti.* ISBN 978-80-01-06675-1. Praha: ČVUT 2019, 465 p. https://doi.org/10.14311%2FBK.9788001066751

[40] PROCHÁZKOVÁ, D. *Bezpečnost kritické infrastruktury.* ISBN 978-80-01-05103-0. Praha: ČVUT 2012, 318 p.

[41] PROCHÁZKOVÁ, D., PROCHÁZKA, J. *Rizika spojená s pozemními komunikacemi.* ISBN 978-80-01-06843-4. Praha: ČVUT 2021, 296 p., http://hdl.handle.net/10467/9 4283

[42] PROCHÁZKOVÁ, D., PROCHÁZKA, J. *Data a metodika jejich zpracování pro potřeby inženýrských disciplín*. ISBN: 978-80-01-05792-6. Praha: ČVUT 2015, 186 p.

[43] DRÁŽNÍ INSPEKCE ČR. *Archiv.* http://www.dicr.cz

[44] LACKO, B. Analýza rizik a situační povědomí. In: *Rizika podnikových procesů 2015*. ISBN: 978-80-7414-967-2. Ústí nad Labem: UJEP 2015, pp. 27-34.

[45] ČVUT. *Archiv pohrom, havárií a selhání, jejich dopadů a postupů odezvy.* Praha: ČVUT 2022.

[46] ČR. MD. *Zpráva o výsledcích šetření příčin a okolností vzniku mimořádné události: Srážka lokomotivního vlaku Lv72461 s osobní m vlakem Os 5011 na dráze železniční celostátní v železniční stanici Moravany (trať Česká Třebová – Praha – Libeň).* http://www.dicr.cz/uploads/Zpravy/MU/MU_Moravany.pdf

[47] EU. ERA. *Advice ERA/ADV/2015-6 of the European Railway Agency for European Commission Regarding Advice Concerning the Strengths and Weaknesses of the Investigation Report on the Accident at Santiago de Cornpostela on 23 July*

2013. Brussels: European Rail Agency 2015. http://www.era.europa.eu/Document-Register/Documents/ERA-ADV-2015-6%2 0Investigation%20report-Santiago%20de%20Compstela%20%28003%29%20 %28002%29.pdf

[48] DE Eisebahn-Bundesamt. *ZwischenberichtGefaerliches Ereignis im Eisenbahnbetrieb Bad Aibling-Kolebermoor.* Bonn: DE Eisebahn-Bundesamt 2017.

[49] Railway Gazzete. *Human Error Caused Bad Aibling Collision.* http://www.railwaygazette.com/news/passenger/single-view/view/human-errpr-caused-bad-aibling-collision.com

[50] BBC NEWS. *Bad Aibling Train Crash: German Controller Jailed.* http:// www.bbc.com/news/world-europe-38206458

[51] USA NTBS. *Preliminary report Railroad Amtrak Passenger Train 501 Derailment* (*DuPont, Washington December 18, 2017 RRD18MR001)*. Washington, D.C.: National Transportation Board 2017.

[52] WALMSLEY, R., ANDERSON, T., BRENDISH, C., MCDERMID, J., ROLFE, M., SULTANA, J., SWAN, M., TOMS, M. *NATS System Failure 12 December 2014*. http://www.caa.co.uk/docs/2942/Independent%20Enquiry%20Final%20Report %202.0.pdf

[53] BUREAU D'ENQUÊTES ET D'ANALYSES POUR LA SÉCURITÉ DE L'AVIATION CIVILE (BEA). *Final Report On the Accident on 1. June 2009 to the Airbus A330-203 Registered F-GZCP Operated by Air France Flight AF 447 Rio de Janiero – Paris*. 5. červenec 2012. 223 p.

[54] WIKIPEDIE. *Let Air France 447*. https://cs.wikipedia.org/wiki/Let_Air_France _447

[55] WIKIPEDIE. *EgyptAir Flight 804*. https://en.wikipedia.org/wiki/EgyptAir_Flight _804

[56] BEA Press Release: *Review of Situation on 6 July 2018, Safety Investigation into Airbus A320 Accident, Registred SU-GCC and Operated by EgyptAir, on 19.05.2016 off the Egyptian Coast*. https://www.bea.aero/en/investigation-reports/notified-events/detail/accident-to-the-airbus-a320-registere dsu-gcc-and-operated-by-egyptair-on-05-19-2016-in-cruise-off-the-egyptian-coast-investigation-led-by-aib---egypt/

[57] LE MONDE. *"L'Airbus A320 d'Egypt Air qui s'est écrasé en 2016 n'était pas en état de voler"* [The EgyptAir Airbus A320 that Crashed in 2016 Was not Able to Fly]. Agence France-Presse. 2 April 2019.

[58] BBC. *EgyptAir Crash: Forensics Chief Denies Explosion Claim". BBC News. 24 May 2016.*

[59] KOMITE NASIONAL KESELAMATAN TRANSPORTASI. Aircraft Accident Investigation Report. KNKT.14.12.29.04. Jakarta: 2015, 206 p.

[60] KOMITE NASIONAL KESELAMATAN TRANSPORTASI. Aircraft Accident Investigation Report. KNKT.18.10.35.04. Jakarta: 2018, 76 p.

[61] https://idnes.cz

[62] PROCHÁZKOVÁ, D., PROCHÁZKA, J. Rizika spojená s leteckou dopravou. In: *Řízení rizik procesů, zařízení a bezpečnost složitých technických děl.* ISBN 978-

80-01-06906-6. Praha: ČVUT 2021, pp. 70-136. DSPACE. http://hdl.handle.net/10467/98461. doi.org/10.14311/ BK.97880 01069066.

[63] KOPŘIVA, J. Kybernetické hrozby pro regionální bezpečnost a obranná opatření proti nim. In: *Rizika podnikových a územních procesů a poznatky pro krizové řízení.* ISBN: 978-80-01-06033-9. Praha: ČVUT 2016, pp. 76-82.

[64] MURPHY, S. *BGP Security Vulnerabilities Analysis*. Tech. rep. RFC 4272. Jan. 2006. http://www.rfc-editor.org/rfc/rfc4272.txt.

[65] NEC Press Release: NEC Technology Uses Artificial Intelligence to Automatically Detect Unknown Cyber-Attacks. December 2015.

[66] TAGATO H. et al. Automated Security Intelligence (ASI) with Auto Detection of Unknown Cyber-Attacks. *NEC Technical Journal*. 11(2016), 1.

[67] US. *NIST SP 800-53.* Security and Privacy Controls for Federal Information Systems and Organizations.

[68] VINAY, M. I., LAUGHTER, S. A., WILLIAMS, R. D. Security Issues in SCADA Networks. *Computers & Security*, 25 (2006), pp. 498-506.

[69] KERTIS, T., PROCHAZKOVA, D. Impacts of Lacks in Design of Control Systems in Rail Transportation. In: *Smart Cities Symposium Prague 2018,* pp. 1-6. **e**ISBN 978-1-5386-5017-2, ISBN 978-1-5386-5018-9. doi:10.1109/SCSP.2018.8402668.

[70] ISO. ISO/IEC 27001. *Information technology—Security Techniques—Information Security Management Systems—Requirements*. Geneva: ISO 2013.

[71] EU. ARTEMIS 2014. *Project SESAMO: Security and Safety Modelling*. Brussels 2011-2014. http://sesamo-project.eu

[72] CEN-CENELEC. *Rail Sector Forum: Railway in Future*. Brussels: EU (JRC) 2017.

[73] EU. *Project CertMILS: Compositional Security Certification for Medium to High-Assurance COTS-Based Systems In Environments With Emerging threats*. https://certmils.eu

[74] EU. *Project CITADEL: Critical Infrastructure Protection Using Adaptive MILS*. https: hhtt:cyberwatching.eu

[75] INSAG. Defence in Depth in Nuclear Safety. *INSAG-10.* ISBN 92-0-103295-1. Vienna: IAEA 1996.

[76] PROCHÁZKOVÁ, D., PROCHÁZKA, J., ŘÍHA, J., BERAN, V., PROCHÁZKA, Z. *Řízení rizik procesů spojených se specifikací a umístěním technických děl do území*. ISBN 978-80-01-06467-2. Praha: ČVUT 2018, 134 p., https://doi.org/10.14311%2FBK.9788001064672

[77] PROCHÁZKOVÁ, D. *Analýza, řízení a vypořádání rizik spojených s technickými díly.* ISBN 978-80-01-06480-1. Praha: ČVUT 2018, 222 p. https://doi.org/10.14311%2FBK.9788001064801

[78] KEENEY, R. L, RAIFFA, H. *Decision with Multiple Objectives*. Cambridge: Cambridge University Press 1976, 1993, 569 p.

[79] FEMA. *Guide for All-Hazard Emergency Operations Planning*. State and Local Guide (SLG) 101. Washinton: FEMA 1996.

[80] EU. *FOCUS Project*. Brussels: EU 2012, http://www.focusproject.eu/documents /14976/-5d7 63378-1198-4dc9-86ff-c46959712f8a

[81] IEEE. IEEE Std 1474 Series, Communications Based Train Control (CBTC). https://standareds.ieee.org.

[82] PINKAS, P. Řízení a zabezpečení železniční dopravy. *AUTOMA 1 (2014).*52955. pdf. http://automa.cz

[83] IEC. *IEC 62290-1. Railway Applications – Urban Guided Transport Management and Command/Control Systems – Part 1: System Principles and Fundamental Concepts* 2014

[84] FAROOQ, J., SOLER, J. Radio Communication for Communications-Based Train Control (CBTC): A Tutorial and Survey", *IEEE Commun. Surveys Tuts.* 19 (2017), 3, pp. 1377-1402.

[85] Oh, S., Yoon, Y., Kim, Y. Automatic Train Protection Simulation for Radio-Based Train Control Systém. In: *Proc. Int. Conf. Inf. Sci. Appl.*, pp. 1-4, 2012.

[86] EU. *Směrnice 96/48. Interoperabilita evropských vysokorychlostních železničních systém*ů. https://eur-lex.europa.eu

[87] MD ČR. *ETCS (European Train Control System).* https://mdcr.cz

[88] EU. *Směrnice 2001/16/ES, o interoperabilitě transevropského konvenčního železničního systému*. https: //eur-lex.europa.eu

[89] EU. *Směrnice 2016/797 o interoperabilitě železničního systému v Evropské unii*. https://eur-lex.europa.eu

[90] ERA. *Technical Standards for Interoperability (TSI).* https://www.era.europa.eu

[91] EU. *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*. https://eur-lex.europa.eu

[92] EU. *Regulation of the European Parliament and of the Council on ENISA and on Information and Technological Cybersecurity Certification*. https://eur-lex.europa.eu

[93] ISO. *ISO 27005. Information Technology — Security Techniques — Information Security Risk Management* . Geneve: ISO 2018.

[94] CENELEC. *TS 50701. Railway Applications.* ENISA 2021. https://www.enisa. europa.eu

[95] OECD. *Guidance on Safety Performance Indicators. Guidance for Industry, Public Authorities and Communities for Developing SPI Programmes Related to Chemical Accident Prevention, Preparedness and Response*. Paris: OECD 2002, 191 p.

[96] BOSS, J. Railway Signalling and Cyber Security. *Doctor´ Thesis*. Delft: Technical University Delft 2020, 100 p.

[97] EU. 92 EN 51029 EUR-Lex - *71978L0144DNK_51029* https://eur-lex.europa.eu

[98] NIST. 93 *NIST SP800-82. Guide to Industrial Control Systems (ICS) Security*. http://dx.doi.org /10.6028/NIST.SP.800-82r2

[99] BS. *EN ISO/IEC 27002:201794 ISO 27002. Information Technology. Security Techniques. Code of Practice for Information Security Controls.* Praha: ČNI 2014.

[100] NIST. *NIST SP800-30. Guide for Conducting Risk Assessments.* https://csrc.nist.gov

[101] ISO. *ISO/IEC 27005:2018. Information Technology — Security Techniques — Information Security Risk Management.*

[102] DELONGU, B. *Risk Analysis and Governance in EU Policy Making and Regulation.* ISBN 978-3-319-30822-1. Springer 2016, 288 p.

[103] VEBER, J. a kol. *Management*. ISBN 807261-029-5. Praha: Management Press 2001. 700 p.

[104] BĚLOHLÁVEK, F, KOŠŤAN, P., ŠULEŘ, O. *Management.* ISBN 80-251-0396-X. Brno: Computer Press 2006. 724 p.

[105] DĚDINA, J. *Management a organizační chování*. Praha: Grada 2005.

[106] PROCHÁZKA, J., NOVOBILSKÝ, P., PROCHÁZKOVÁ, D. Segmentace řídících systémů vlaku. In: *Řízení rizik procesů a bezpečnost složitých technických děl*. ISBN 978-80-01-06786-4. Praha: ČVUT 2020, pp. 98-106. http://hdl.handle.net/10467/91988; https://doi.org/10.14311/BK.9788001067864

[107]PROCHÁZKA, J., NOVOBILSKÝ, P. PROCHÁZKOVÁ, D. Standardizace bezpečnosti komunikace vlak – řídící centrum. In: *Criscon 2020 – Krizové řízení a řešení krizovcvh situací.* ISBN 978-80-7454-957-1. Zlín: UTB 2020, pp. 152-161. http://hdl.handle.net/10563/45944

[108] EU. IEC 61375-2-6. *Electronic Railway Equipment - Train Communication Network: On-board to Ground Communication*. International Electrotechnical Commission. https://www.en-standard.eu

[109] EU. *Project certMILS, 2017. Compositional Security Certification for Medium- to High-Assurance COTS-Based Systems in Environments with Emerging Threats.* Horizon 2020, no 731456, EU.

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

[111] PikeOS. *PikeOS® 4.2 Certified Hypervisor*, SYSGO – version 2019. https://www.sysgo.com/products/pikeos-hypervisor

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

[113] PROCHAZKA J., NOVOBILSKY P., PROCHAZKOVA D. Certification Cycles of Train Cyber Gateway. In: *Proceedings of the 30th European Safety and Reliability Conference and 15th Probabilistic Safety Assessment and Management Conference (ESREL2020 PSAM15).* No. 3728. ISBN 978-981-14-8593-0. Singapore: ESRA 2020, Research Publishing Singapore 2020. e:enquiries@rpsonline.com.sg

[114] PROCHAZKA J., NOVOBILSKY P., PROCHAZKOVA D. Cyber Security of Urban Guided Transport Management according MILS Principles. In: *Proceedings of the 29th European Safety and Reliability Conference (ESREL).* ISBN 978-981-11-2724-3. Singapore: ESRA 2019, Research Publishing 2019, pp. 4107 - 4413, doi:10.3850/978-981-11-2724-3_0220-cd, e:enquiries@rpsonline.com.sg,

[115] MQTT. *The Standard for IoT Messaging*. 2020. Online on https:/mqtt.org.

[116] CORBETTA S., ZONI D., FORNACIARI W. A Temperature and Reliability Oriented Simulation Frame-work for Multi-Core Architectures. In: *2012 IEEE Computer Society Annual Symposium on VLSI.* 51 p. IEEE.

[117] COSMOS. *DevOps for Complex Cyber-Physical Systems*. EU, Horizon 2020, no 957254. Brussles: EU 2021.

Titul:	Řízení rizik systémů pro řízení dopravy
Autorský kolektiv:	RNDr. Jan Procházka, Ph.D. Doc. RNDr. Dana Procházková, DrSc.
Recenzenti:	Doc. Ing. Branislav Lacko, CSc. Doc. Ing. Petr Šrytr, CSc.
Vydavatel:	ČVUT v Praze - DSPACE
Počet kopií:	Open Access
Počet stránek:	129
Rok vydání:	2022

ISBN 978-80-01-06995-0