Řízení rizik vybraných prvků kritické dopravní infrastruktury
Risk management of selected elements of critical transport infrastructure

Dana Procházková, Jan Procházka, Jana-Victorie Martincová, Tomáš Kertis

Vysoké učení technické v Brně, Ústav soudního inženýrství, prochdana7@seznam.cz, japro2am@seznam.cz, 23907@usi.vutbr.cz, kertis@sport-sky.cz

Souhrn

Pro plnění základních funkcí státu je bezpečnost kritické infrastruktury zásadní, a proto ji musí být věnována pozornost. Dopravní infrastruktura patří do kritické infrastruktury. Její prvky: mosty; tunely; nádraží; letiště; a řízení jejich provozu, jsou zásadně důležité. Článek shrnuje zásady pro řízení rizik zmíněných prvků kritické dopravní infrastruktury založený na systémovém pojetí a respektující socio-kyber-fyzickou povahu prvků a složitost systémů v dynamicky se vyvíjejícím světě.

Na základě aplikace metod inženýrských disciplín zabývajících se riziky (scénáře, případové studie, What, If, kontrolní seznamy, diagramy rybí kosti, systémy pro podporu rozhodování, matice odpovědnosti, skórování apod.) na data: 283 selhání mostů ve světě od r. 1297; 965 selhání tunelů na pozemních komunikacích a 53 případových studií ve světě od počátku 19. století; 2511 selhání kritických objektů na pozemních komunikacích (nádraží, křižovatky, obtížná místa komunikací) ve světě od roku 1815 (u železničních stanic vyhodnoceno 1125 selhání); 1917 leteckých nehod civilních letadel ve světě od roku 1909; a 31 selhání řídících systémů dopravy ve světě od roku 2006, byly zjištěny příčiny havárií i selhání sledovaných kritických prvků dopravní infrastruktury.

Analýzou příčin havárií a selhání byly stanoveny zásady, které je třeba dodržovat při projektování mostů na základě současných znalostí a požadavků novely ISO 9000 z roku 2016. Jde o aplikaci zásad platných dle současného poznání pro řízení rizik při: projektování (risk-based design) a provozu (risk based operation). Protože sledované kritické prvky dopravní infrastruktury jsou složité systémy (soubor otevřených a vzájemně propojených systémů), které mají povahu socio-kyber-fyzickou, tak byly zváženy i organizační havárie. Jelikož příčiny organizačních havárií tkví v systému řízení, tak byl zvážen systém řízení aplikovaný v EU (TQM – Total Quality Management) a princip odpovědností, který je běžný v Evropě (tj. odpovědnost za bezpečnost kritického prvku dopravní infrastruktury má vlastník (provozovatel) i veřejná správa, která má povinnost dohledu ve veřejném zájmu. Na základě požadavků strategického řízení a systému řízení v EU je sestaven generický model pro řízení bezpečnosti sledovaných prvků dopravní kritické infrastruktury. Protože jeho aplikace v praxi je ve všech aspektech náročné, tak musí být zavedeno legislativou, proto bylo provedeno srovnání nároků české legislativy na řízení bezpečnosti sledovaných prvků dopravní kritické infrastruktury s generickým modelem pro zajištění integrální bezpečnosti.

Výzkum ukázal, že příčinou rizik, která vedou k selhání sledovaných prvků kritické dopravní infrastruktury jsou: ***nedostatky v řízení objektů a jejich procesů; vnitřní zdroje rizik objektu či procesu spojené s jeho stavbou, konstrukcí, zařízeními a provozem; nedostatky v oblasti personální (nedostatečná podpora a motivace kritického personálu); nedostatečné finance na provoz, speciálně na údržbu****; vnější zdroje rizik objektu či procesu technického díla spojené s živelními pohromami či zdroji havárií v okolí; vnější zdroje rizik objektu či procesu spojené s chováním veřejné správy, konkurencí, trhem apod.; útoky na objekt či proces; kybernetické zdroje rizik spojené se sítěmi spojenými s objektem či procesem; válka; a nedostatečný dozor veřejné správy. Tučnou kurzívou vyznačené oblasti nepatří do problematiky havarijních plánů (vnitřních i vnějších), krizových plánů a plánů krizové připravenosti. Plán řízení rizik řeší všechny oblasti, protože bezpečnost je základním znakem kvality, kterou vyžaduje typ řízení TQM (Total Quality Management), který platí v Evropské unii.*

Klíčová slova: *Dopravní infrastruktura, mosty, tunely, nádraží, železniční stanice, řídící systémy dopravy, riziko, bezpečnost, zabezpečení.*

Summary

In order to fulfil the basic functions of the State, the safety of critical infrastructure is essential, and therefore, it must be paid attention to it. Transport infrastructure belongs to critical infrastructure. Its elements: bridges; tunnels; railway station; airport; and the management of their operation are essential. The article summarizes the principles for risk management of the mentioned elements of critical transport infrastructure based on a systemic concept and respecting the socio-cyber-physical nature of the elements and the complexity of systems in a dynamically evolving world.

Based on the application of the methods of engineering disciplines dealing with risks (scenarios, case studies, What, If, checklists, fishbone diagrams, decision support systems, responsibility matrix, scoring, etc.) to data: 283 bridges´ failures in the world since 1297; 965 road tunnels´ failures and 53 case studies in the world since the early 19th century; 2511 failures of critical objects on roads (railway stations, intersections, difficult road points) in the world since 1815 (1125 failures evaluated at railway stations); 1917 civil aircraft accidents in the world since 1909; and 31 failures of transport control systems in the world since 2006, the causes of accidents and failures of monitored critical elements of transport infrastructure have been identified.

By analysing the causes of accidents and failures, the principles to be followed when designing bridges based on current knowledge and requirements of the 2016 ISO 9000 amendment were established. It is an application of the principles valid according to current knowledge for risk management in: risk-based design and in risk-based operation. Since the monitored critical elements of the transport infrastructure are complex systems (a set of open and interconnected systems) that have a socio-cyber-physical nature, organizational disasters were also considered. Since the causes of organisational accidents lie in the management system, the management system applied in the EU (TQM – Total Quality Management) and the principle of responsibilities, which is common in Europe (i.e. responsibility for the safety of a critical element of transport infrastructure lies with both the owner (operator) and the public administration, which has a duty of supervision in the public interest, were considered. Based on the requirements of strategic management and management system in the EU, a generic model is developed for the safety management of monitored elements of transport critical infrastructure. Because its application in practice is demanding in all aspects, it must be introduced by legislation, which is why a comparison of the requirements of Czech legislation for the management of safety of monitored elements of transport critical infrastructure was carried out with a generic model to ensure integral safety.

Research has shown that the causes of the risks that lead to the failure of the monitored elements of critical transport infrastructure are: ***deficiencies in the management of objects and their processes; internal sources of risks of an object or process associated with its construction, structure, facilities and operation; staffing deficiencies (lack of support and motivation of critical personnel)); insufficient funds for operation, especially for maintenance; external sources of risks of the object or process of the technical work associated with natural disasters or sources of accidents in the vicinity****; external sources of risks of the object or process associated with the behaviour of public administration, competition, the market, etc.; attacks on an object or process; cyber sources of risk associated with networks associated with an object or process; war; and lack of oversight by public administration. Areas marked in bold italics do not belong to the issue of emergency plans (internal and external), crisis plans and crisis preparedness plans. The risk management plan addresses all areas, because safety is an essential sign of the quality required by the type of TQM (Total Quality Management) that applies in the European Union.*

Keywords: *Transport infrastructure, bridges, tunnels, railway stations, railway stations, traffic control systems, risk, safety, security.*

1. Úvod

Dopravu tvoří rozsáhlá síť dopravních cest, objektů, podpůrných systémů a dopravních prostředků různých druhů a typů. Dopravní síť je jednou z nejdůležitějších infrastruktur zajišťující základní funkce státu, tudíž i základní potřeby lidí pro jejich přežití. Vzhledem k historickému vývoji lidstva, států a ekonomiky se mnoho částí dopravního systémů stává kritickou infrastrukturou. Dle důležitosti a zranitelnosti

dopravních infrastruktur, nebo jejich prvků, určujeme jejich kritičnosti, které jsou posuzované z hlediska vybrané entity, tj. z hlediska větších územních celků, států, krajů či vybraných míst s návazností na jiné chráněné zájmy (aktiva), která jsou v blízkosti důležitých objektů, továren, elektráren, veřejných center a podobně.

Existuje mnoho různých oblastí řízení bezpečnosti, které se od sebe odlišují také dle druhu dopravy respektive úhlu pohledu, ze kterého se na bezpečnost sledovaného objektu díváme (na dopravní prostředek, stavbu, dopravní cesty, podpůrné systémy, řídicí systémy včetně lidského aspektu, nebo dokonce z hlediska logistických služeb, přepravy zboží a osob). Cíle jednotlivých oblastí řízení bezpečnosti a řízení rizik jsou stejné, tj. prevence ztrát, ať už se jedná o lidské životy, majetek, stav lidské společnosti, životní prostředí, kritickou infrastrukturu včetně ekonomiky a dalších. Na první pohled se zdá, že jsou jednotlivé koncepty řízení bezpečnosti v různých odvětvích jsou rozdílné, ale ve skutečnosti jsou velmi podobné. Vycházejí ze studie rizik a inženýrství založeném na řízení rizik ve prospěch bezpečnosti. V mnoha aspektech jsou totiž zastíněny nejednotností v principech.

Předložená práce je zpracována na principu řízení rizik ve prospěch integrální bezpečnosti [1,2], který zajišťuje bezpečnost objektu a jeho koexistenci s okolím po celou dobu životnosti, tj. ve sledovaném případě dopravního systému. Jelikož dopravní systému patří do kritické infrastruktury, tak jsou sledována ustanovení krizového zákona, tj. zákona č. 240/2000 Sb. ve znění pozdějších předpisů, která stanoví:

- krizovým řízením se rozumí souhrn řídících činností orgánů krizového řízení zaměřených na analýzu a vyhodnocení bezpečnostních rizik a plánování, organizování, realizaci a kontrolu činností prováděných v souvislosti s přípravou na krizové situace a jejich řešením, nebo s ***ochranou kritické infrastruktury***,
- kritickou infrastrukturou se rozumí prvek kritické infrastruktury nebo systém prvků kritické infrastruktury, narušení jehož funkce by mělo závažný dopad na bezpečnost státu (ústavní zákon č. 110/1998 Sb.), zabezpečení základních životních potřeb obyvatelstva, zdraví osob nebo ekonomiku státu,
- prvkem kritické infrastruktury se rozumí zejména stavba, zařízení, prostředek nebo veřejná infrastruktura (zákon č. 183/2006 Sb.), určené podle průřezových a odvětvových kritérií; je-li prvek kritické infrastruktury součástí evropské kritické infrastruktury, považuje se za prvek evropské kritické infrastruktury,
- ochranou kritické infrastruktury se rozumí opatření zaměřená na snížení rizika narušení funkce prvku kritické infrastruktury,
- subjektem kritické infrastruktury se rozumí provozovatel prvku kritické infrastruktury; jde-li o provozovatele prvku evropské kritické infrastruktury, považuje se tento za subjekt evropské kritické infrastruktury,
- průřezovými kritérii se rozumí soubor hledisek pro posuzování závažnosti vlivu narušení funkce prvku kritické infrastruktury s mezními hodnotami, které zahrnují rozsah ztrát na životě, dopad na zdraví osob, mimořádně vážný ekonomický dopad nebo dopad na veřejnost v důsledku rozsáhlého omezení poskytování nezbytných služeb nebo jiného závažného zásahu do každodenního života,
- odvětvovými kritérii se rozumí technické nebo provozní hodnoty k určování prvku kritické infrastruktury v odvětvích energetika, vodní hospodářství, potravinářství a zemědělství, zdravotnictví, doprava, komunikační a informační systémy, finanční trh a měna, nouzové služby a veřejná správa.

Nařízení vlády č. 462/2000 Sb. obsahuje náležitosti a způsob zpracování plánu krizové připravenosti subjektu kritické infrastruktury, který zvažuje prvky kritické infrastruktury, ohrožení jejich funkce a způsoby jejich ochrany. Nařízení vlády 432/2010 Sb. stanovuje odvětvová a průřezová kritéria pro určování prvků kritické infrastruktury. Pro oblast dopravy do kritických prvků patří mosty a tunely na dálnicích a silnicích I. třídy a na páteřních železnicích, nádraží / železniční stanice, letiště a centra řízení komunikačních a informačních systémů v dopravě.

V kapitole 2 je shrnuto současné pojetí rizik, bezpečnosti a jejich řízení ve formě pojmů. V kapitole 3 jsou popsána data a použité metody při výzkumu zacíleném na výše uvedené prvky dopravní infrastruktury. V kapitole 4 jsou uvedeny výsledky systematického studia rizik pro mosty, tunely, pozemní komunikace, nádraží / železniční stanice; a rizika spojená s řídícími systémy dopravy. Pátá kapitola popisuje generický model pro řízení bezpečnosti a šestá uvádí návrhy opatření pro zvýšení bezpečnosti sledovaných kritických prvků.

2. Současné základní poznatky inženýrských disciplín, které pracují s riziky

Lidstvo potřebuje pro život prostor, který je bezpečný a umožňuje mu rozvoj. Chápání světa a jeho vlastností se vyvíjí a s ním se mění i pojmy a jejich pojetí. Výraznou změnu v chápání bezpečnosti a cílů světa přinesly dokumenty OSN [3] a EU [4] a v řízení lidských aktivit v EU zavedení TQM (Total Quality Management) [5] v r. 1989 Maastrichtskou smlouvou.

Podle současného poznání v systémovém pojetí světa platí:

- entity jsou systémy [1,2]. Většinu reálných entit tvoří systémy systémů (SoS) [1,2,6]. Většina lidmi vytvořených systémů má povahu socio-kyber-fyzickou [2],
- chráněná aktiva lidského systému a všech jeho dílčích systémů jsou dle výzkumu shrnutého v práci [6]: životy, zdraví a bezpečí lidí; majetek a veřejné blaho; životní prostředí; a kritické infrastruktury a technologie,
- škodlivý jev je každý jev, který poškozuje aktiva lidského systému; od r. 1811 se dle legislativy nazývá pohroma; na základě analýzy ASPI [7] se vyskytuje v 501 právních předpisech. Později se zavedly pojmy další (nehoda, porucha, kalamita, katastrofa atd.), které jsou více specifické,
- ohrožení je míra velikosti škodlivého jevu [8]. Měří se ve stupních (stupnice jsou specifické) anebo fyzikálními jednotkami [9],
- riziko je míra ztrát, škod a újmy na chráněných aktivech lidského systému [8]; speciální pozornost životnímu prostředí je věnována v práci [10]. Riziko je dílčí – vztahuje se k jednotlivému aktivu; integrované – součet dílčích rizik; a integrální (celkové) – riziko celku chápaného jako systém, tj. jsou zvažovány nejen prvky, ale i jejich vazby a toky, které mezi nimi proudí [6,8]; zpravidla rozlišujeme integrální rizika procesů a integrální rizika objektů [11]. Rizika se dělí na: přijatelná; podmíněně přijatelná (ALARA/ALARP); a nepřijatelná [2,6,8],
- zabezpečení / bezpečí entity je vlastnost entity, která znamená, že entita je ochráněna proti všem vnějším škodlivým jevům a lidskému faktoru [2,8,11],
- bezpečnost entity (prvku, systému, objektu, procesu) je vlastnost entity, která je základním znakem kvality entity, která znamená, že entita je ochráněna proti všem vnějším a vnitřním škodlivým jevům a lidskému faktoru [2,8,11]. Jde o schopnost entity předcházet kritickým stavům, která je výsledkem aplikace antropogenních opatření a zahrnuje nejen opatření na ochranu, ale i na spolehlivost a funkčnost sledovanému objektu,
- bezpečnost, zabezpečení i spolehlivost entity se zajišťují řízením rizik [2,6,8,9,11],
- kritičnost je komplementární pojem k pojmu bezpečnost [2,6,8,11],
- kritická entita (prvek, vazba, tok, zařízení, systém..) je entita, která je zároveň velmi důležitá a velmi zranitelná [2,8,11]. Podle většiny současných pojetí, pojem kritický souvisí s bezpečností.

Další fakta o konceptu spojeném s riziky a bezpečností lze nalézt v pracích [2,6,8,11].

Dopravní infrastruktura je otevřený a složitý systém, který se skládá z mnoha dílčích systémů (subsystémů) a mnoha různých prvků. Dílčí systémy i prvky mohou pracovat samostatně a dohromady, kdy plní zcela jedinečný úkol, který je vzdálený od úkolů jednotlivých entit. Podle poznatků shrnutých v [1] jsou pro ně důležité dvě systémové vlastnosti, a to interaktivní složitost a těsná spojení. Složité interakce jsou neplánované, neočekávané a většinou neznámé sekvence, které nejsou bezprostředně srozumitelné. Složité interakce v systémech systémů mají za následek nejednoznačná rozhodnutí, nestabilní preference a konfliktní cíle. 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 prvky v sociotechnickém systému mohou vést 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 vlastnostmi systému. Zvažované nefunkční 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. Výsledek působení pohromy o jisté velikosti závisí na okamžitém stavu systému.

To znamená, že prvky i dílčí systémy mají povahu technickou (fyzickou), sociální a kybernetickou. Bezpečnost předmětného systému [2] proto závisí jak na dílčích položkách různé povahy, tak na jejich propojení. 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 i prostředí, ve kterém se aktiva nachází.

Charakteristiky složitých socio-kyber-technických (fyzických) systémů jsou shrnuty v práci [2]. 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 SoS je agregací bezpečností dílčích systémů; musí se totiž respektovat i průřezová rizika 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 zcela na místě u daných objektů. Proto musí být postupně nahrazována integrální bezpečností, při které se spoléhá i na řízení průřezových rizik.

3. Data a metody výzkumu

Při výzkumu sledovaných prvků dopravní kritické infrastruktury byla použita data o:

- 283 selháních mostů ve světě od r. 1297 [12],
- 965 selhání tunelů na pozemních komunikacích a 53 případových studií ve světě od počátku 19. století [13],
- 2511 selhání kritických objektů na pozemních komunikacích (nádraží / železniční stanice, křižovatky, obtížná místa komunikací) ve světě od roku 1815 (u železničních stanic vyhodnoceno 1125 selhání) [14],
- 1917 leteckých nehod civilních letadel ve světě od roku 1909 [15],
- 31 selhání řídících systémů dopravy ve světě od roku 2006 [16].

Při zpracování dat byly použity metody pro zpracování: scénářů; případových studií; hodnocení pomocí What, If; hodnocení pomocí kontrolních seznamů; diagramy rybích kosti; hodnocení pomocí systémů pro podporu rozhodování; matic odpovědností; a skórování [17].

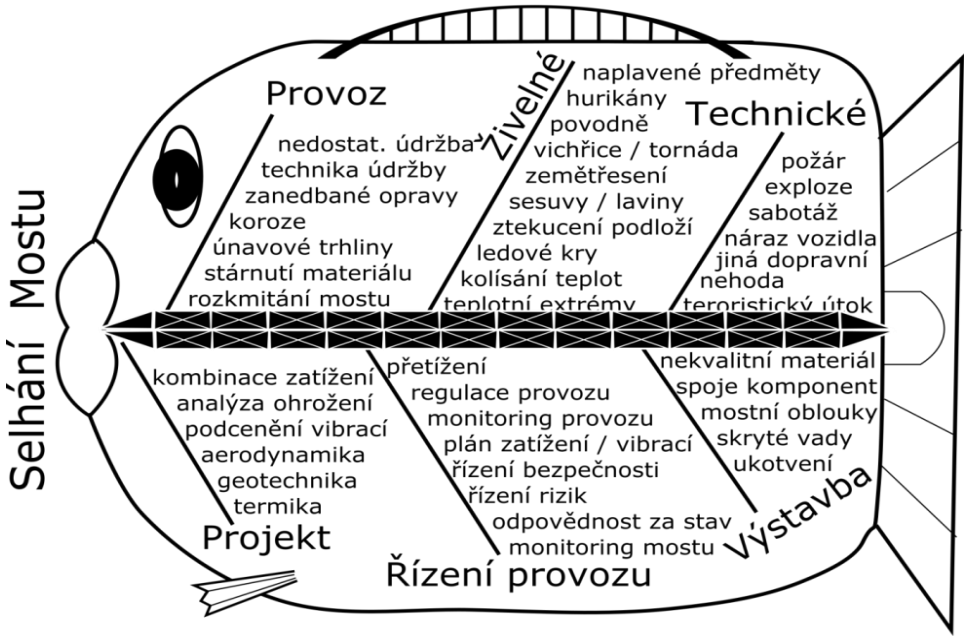
4. Poznatky pro vybrané kritické prvky

V kapitole shrneme nejdůležitější výsledky získané dosavadním výzkumem.

4.1. Rizika spojená s mosty

Rizika spojená s mosty jsou systematicky sledována v práci [12]. Na základě reálných dat o selháních mostů byla sestavena databáze příčin rizik, které byly původci selhání mostů [18]. Seznam původců selhání byl srovnán a doplněn poznatky z výzkumů dostupných v odborné literatuře. Příčiny selhání mostů jsou ukázány na obrázku 1.

Byly stanoveny zásady, které je třeba dodržovat při projektování mostů na základě současných znalostí a požadavků novely ISO 9000 z roku 2016. Jde o aplikaci zásad platných dle současného poznání pro řízení rizik při projektování (risk-based design) [19]. Dále byly určeny požadavky na bezpečný provoz (risk based operation) [20].



Obr. 1. Příčiny selhání mostů na pozemních komunikacích z pohledu rizik, které narušují bezpečnost mostů.

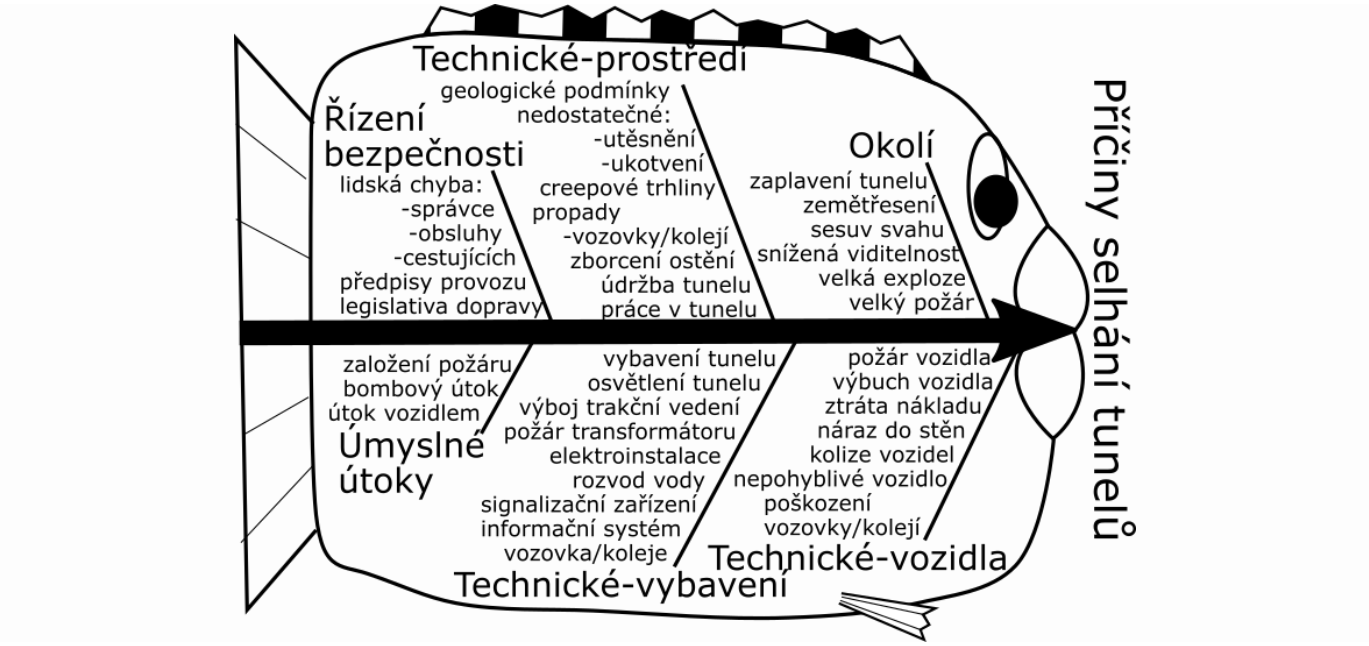
Na základě konceptu, že most je socio-kyber-fyzický systém a zvážení principu odpovědnosti, který je běžný v Evropě [21], což v daném případě znamená, že odpovědnost za bezpečnost mostu, tj. za úroveň práce s riziky spojenými s mostem, má vlastník i veřejná správa, která má povinnost dohledu ve veřejném zájmu byl v práci [12] sestaven nástroj pro rozhodování o rizicích, ve kterém byla zvážena hierarchická úroveň řízení dopravy v ČR a aspekty, které posuzují: způsob zvažování rizik a jejich zdrojů; dosaženou úroveň bezpečí při daném provedení mostu; 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 mostu, tak řízení území). Podrobné případové studie a dílčí výzkumy mostů jsou shrnuty v pracích [22-26].

4.2. Rizika spojená s tunely

Rizika spojená s tunely jsou systematicky sledována v práci [13]. Na základě reálných dat o selhání tunelů byla stanovena databáze příčin rizik, které byly původci selhání tunelů [18]. Seznam původců selhání byl srovnán a doplněn poznatky z výzkumů dostupných v odborné literatuře [13]. Diagram rybí kosti (Fishbone diagram) zobrazující základní kategorie příčin selhání tunelů je uveden na obrázku 2.

Provedená analýza selhání tunelů potvrdila výsledky již obsažené v odborné literatuře, a to účast lidského faktoru na více než 80 % selhání tunelů. Přitom se projevily tři hlavní příčiny. První příčinou jsou lidské chyby, které mají původ ve špatné komunikaci a spolupráci. Druhou příčinou je nereagování nebo nedostatečná reakce obsluhy a řídících pracovníků na situace, které mají potenciál způsobit selhání tunelu. Třetí příčinou je, že řídící pracovníci i obsluha přijímají vysoké riziko, aniž by měli dostatečné povědomí o jeho dopadech.

Analyzovaná selhání tunelů vznikla buď výskytem škodlivého jevu (pohromy), se kterým se v projektu nepočítalo, anebo se podcenila jeho velikost, anebo kumulací mnoha malých škodlivých příčin, které samy o sobě nemají významný škodlivý potenciál, v krátkém časovém intervalu. Jejich kumulace je příčinou latentních podmínek, které mohou mít dlouhou inkubační dobu, která vyplývá z faktu, že velká množství zdrojů selhání mohou být založena v systémech a projeví se, až se objeví spouštěč (trigger) ve formě lidské chyby. Proto pro prevenci selhání tunelů je třeba se vyvarovat:



Obr. 2. Zdroje rizik selhání tunelů na pozemních komunikacích.

- velkých chyb v prevenci rizik,
- a také výskytu drobných chyb, jejichž kumulace v krátkém časovém intervalu je nebezpečná, což potvrzuje např. i práce [27].

K selhání tunelů dochází, stejně jako u mostů, proto, že:

- dosud u tunelů se používají zastaralé způsoby hodnocení rizik, např. stromové modely, které nezvažují souběhy jevů,
- provozovatel či vlastník je orientován hlavně na výkon (tj. zisk) a veřejná správa mu to dovoluje,
- personál, který je s příčinami a dopady rizik v kontaktu, nemá dostatečné kompetence pro zavedení proaktivních opatření a provozních předpisů přizpůsobených momentálním podmínkám (normálním, abnormálním, kritickým),
- technická rozhodnutí jsou poplatná různým partikulárním, politickým nebo ekonomickým tlakům a nepřihlížejí ke konkrétním rizikům, která se v průběhu provozu objevují.

Základními důvody, proč provozovatelé tunelů nejsou ochotni rizika ovlivňovat, obvykle jsou:

- nedostatečné povědomí o rizicích a jejich dopadech na tunel dílo a jeho okolí,
- subjektivní pocity odpovědného subjektu, který nepovažuje riziko za aktuální,
- představa, že rizika se týkají vzdálené budoucnosti,
- kroky vedoucí k identifikaci rizika a jeho snížení jsou většinou v rozporu s okamžitými (většinou ekonomickými či politickými) zájmy provozovatele či vlastníka,
- konkrétní kompetentní pracovník většinou není tím, kdo o krocích vedoucích ke snížení rizika může přímo rozhodovat.

Nesprávné vypořádání rizik v tunelech je způsobeno tím, že:

- rozhodovací procesy o tunelech bývají víceúrovňové. Na úrovni, kde lze reálně rozpoznat narůstající příznaky rizika a ocenit s tím související riziko, nelze rozhodnout o vynaložení vícenákladů na eliminaci tohoto rizika,
- je nedostatečné povědomí o rizicích, jejich řízení a vypořádání. Práce s riziky je chápána jako činnost, která spočívá v dodržení norem a předpisů, což není pravda, protože pravidla v nich zavedená pokrývají jen 68.4 % možných podmínek [2]; programy velké většiny vzdělávacích kurzů probíhajících v České republice tuto nedostatečnost ještě prohlubují,

- u inženýrů v provozu a jeho řízení je úzké chápání bezpečnosti; převládá orientace na technickou bezpečnost zařízení chápanou tak, že technické zařízení během životnosti nepředstavuje nebezpečí,
- je nedostatečná spolupráce profesí – stavařů, strojařů, ekonomů, chemiků, informatiků, personalistů atd. – každá profese pracuje odděleně, což neumožňuje řešit mezioborové a multioborové problémy,
- mnoho řídících pracovníků je přesvědčeno, že vše je věčné, tj. nezvažují změny technických zařízení v čase a se změnou podmínek, a tím podceňují údržbu, opravy, dovednost a dodržování režimů práce, které respektují fyzikální, chemické a biologické zákonitosti,

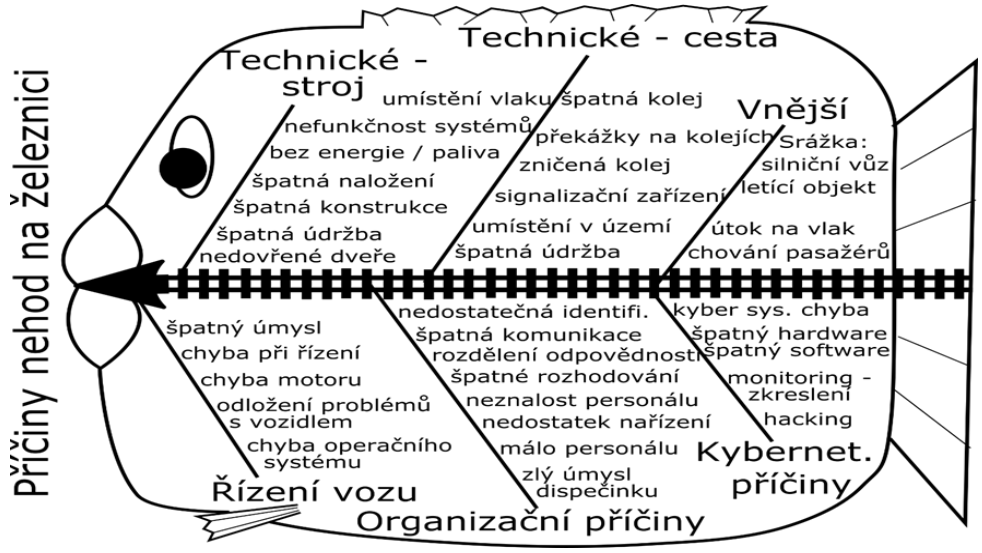
Kritická analýza selhání tunelů [13], ukázala, že některé příčiny selhání se často opakují, například dopravní nehody, nedostatečná údržba, nízká kvalita oprav a modernizace. Jejich společnou kořenovou příčinou je nedostatečná kultura bezpečnosti účastníků provozu v tunelu, jejich nedostatečný výcvik a motivace zacílená na bezpečnou práci a bezpečné chování.

Kritickou analýzou dat o dopadech selhání a postupech odezvy jsou navržena opatření pro zvýšení bezpečnosti tunelů, a to pro: účastníky postižené selháním tunelů na pozemních komunikacích; postupy pro správce tunelů; a poučení pro veřejnou správu.

Pro potřebu řízení rizik tunelů byl v práci [13] sestaven nástroj pro rozhodování o rizicích, ve kterém byla zvážena hierarchická úroveň řízení dopravy v ČR a aspekty, které posuzují: způsob zvažování rizik a jejich zdrojů; dosaženou úroveň bezpečí při daném provedení tunelu; 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 tunelu, tak řízení území). Dílčí výsledky jsou uvedeny v pracích [13,28].

4.3. Rizika spojená s pozemními komunikacemi

Rizika spojená s pozemními komunikacemi jsou systematicky sledována v pracích [29,30]. Jsou sledována z širšího pohledu než jenom jako příčiny dopravních nehod, a to proto, že selhání dopravy má závažné dopady nejen na lidi, ale i na ekonomickou prosperitu území a celého státu. Na základě zkušeností je pro ekonomickou prosperitu a zvládnutí krizových situací železniční doprava. Proto byla speciálně sledována a byla pro ni stanovena databáze dopravních nehod a selhání [18]. Její analýzou byly zjištěny jejich příčiny, které jsou zobrazeny na obrázku 3.

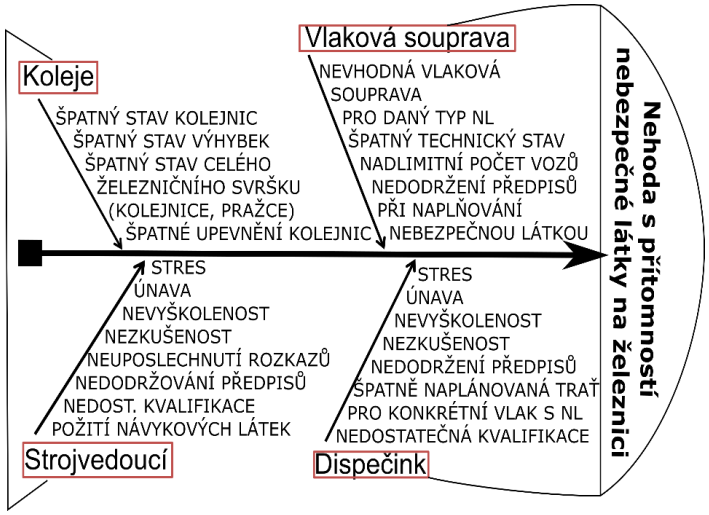


Obr. 3. Příčiny dopravních nehod na železnici.

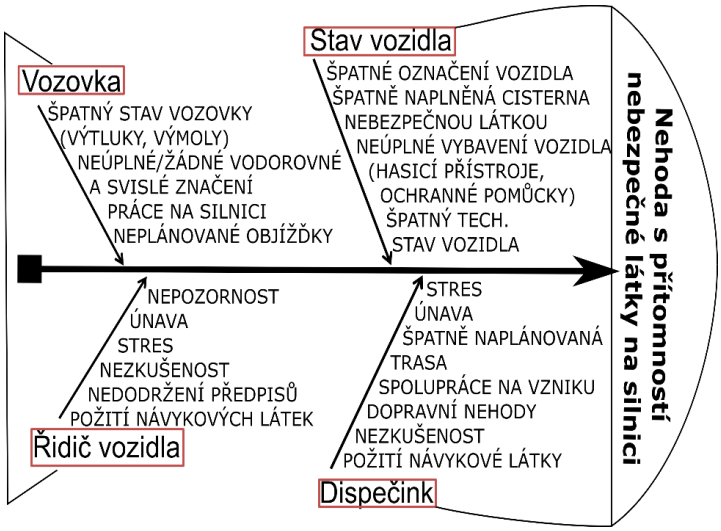
Nedílnou součástí dnešního života je používání nebezpečných látek, a s tím souvisí jejich přeprava. Dopravní nehody s přítomností nebezpečných látek jsou doprovázeny explozemi, požáry, únikem ne-

bezpečných látek do okolí či ke kombinaci dvou až tří uvedených jevů, což má dopady na chráněná aktiva v místě dopravní nehody a dále pak na kvalitu života lidí [30].

Analýza databáze dopravních nehod s nebezpečnými látkami odhalila příčiny dopravních nehod, zobrazené na obrázcích 4 a 5. Analýza prognostických scénářů dopravních nehod na pozemních komunikacích [29] ukázala, že dopady rizik, i když mají stejnou příčinu, závisí na místních podmínkách. Analýza legislativy ČR odhalila, že přeprava nebezpečných látek v České republice je řízena pouze zahraničními předpisy ADR (Evropská dohoda o mezinárodní přepravě nebezpečných věcí) [31] a Řádem pro mezinárodní přepravu nebezpečného zboží [32], které neberou v úvahu specifické podmínky území republiky a navíc jejich terminologie neodpovídá terminologii zákona č. 350/2011 Sb.. Vzhledem k výsledkům případových studií, je chybou, že hustě obydlená Česká republika nemá specifický zákon pro přepravu nebezpečných látek.



Obr. 4. Příčiny dopravních nehod na železnici v České republice.



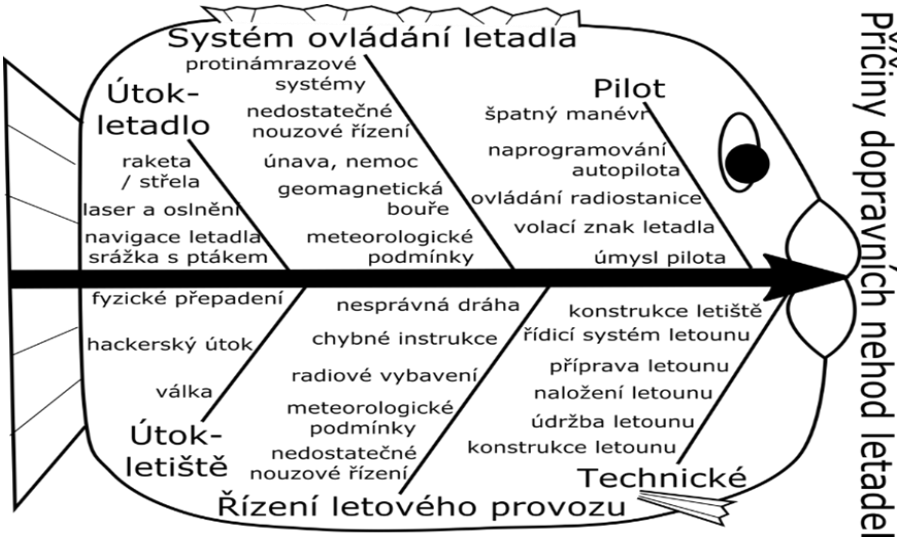
Obr. 5. Příčiny dopravních nehod na silnicích v České republice.

Pro potřebu řízení rizik ve prospěch bezpečnosti na pozemních komunikacích byl v práci [30] sestaven nástroj pro rozhodování o rizicích, ve kterém byla zvážena hierarchická úroveň řízení dopravy v ČR a aspekty, které posuzují: způsob zvažování rizik a jejich zdrojů; dosaženou úroveň bezpečí při daném provedení pozemní komunikace; 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 pozemní komunikace, tak řízení území). Dílčí výsledky jsou uvedeny v práci [33].

4.4. Rizika spojená s leteckou dopravou

Rizika spojená s leteckou dopravou jsou systematicky sledována v práci [15]. Analýza databáze leteckých nehod [18] odhalila příčiny leteckých nehod civilních letadel s 15 a více pasažéry, které jsou zobrazeny na obrázku 6. Pro potřebu řízení rizik ve prospěch bezpečnosti letecké dopravy byl v práci [15] sestaven nástroj pro rozhodování o rizicích, ve kterém byla zvážena hierarchická úroveň řízení letecké dopravy v ČR a aspekty, které posuzují: způsob zvažování rizik a jejich zdrojů; dosaženou úroveň bezpečí při daném provedení letiště; 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 letiště, tak řízení území).



Obr. 6. Roztřídění příčin dopravních nehod civilních letadel.

Na základě šetření velkých leteckých nehod [15] lze konstatovat, že řada primárních (kauzálních) a sekundárních příčin se u nehod opakuje, ačkoliv existuje poměrně dost znalostí potřebných k prevenci nejen skoro nehod, ale i závažných havárií, ke zmírnění jejich dopadů, a tím ke zmenšení ztrát a škod s nimi spojených. Příčinou daného stavu, kromě lidského činitele, jsou nedostatky jak v zavedení funkčního systému řízení bezpečnosti, tak i neznalost závěrů z již vyšetřovaných nehod a havárií [1,2].

Práce [15] rovněž obsahuje opatření pro snížení počtu a závažnosti havárií a selhání v leteckém provozu, a to především v oblasti prevence závažných havárií a v letovém provozu. Obsahuje postupy: pro zvládání očekávaných nouzových situací na letišti; opatření pro zvýšení kvality personálu; a plán řízení rizik. Plán řízení rizik je sestaven jak pro letadlo, tak pro letiště, jehož modelem je letiště Václava Havla v Praze.

Pro zajištění bezpečnosti letišť, letadel i letového provozu je nutno velmi podrobně řešit otázky technické, organizační, ekonomické, personální, finanční atd. příklad řešení vybraného technického problému lze nalézt v práci [34].

4.5. Rizika spojená s řídícími systémy

V současné době automatizace proniká do života všech technických děl. Na jednu stranu přináší obrovské výhody a úspory práce lidí a na straně druhé 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 daném kontextu je řízení členěno na automatické a ruční. V praxi se odlišují ovládání, regulace a vyšší formy řízení (optimální a adaptivní řízení, učení a umělá inteligence).

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 je velmi stručná nebo v mnoha případech nejasná [35]. V průmyslu se pro řízení bezpečnosti uplatňují především systémy řízení kvality založené na procesním a projektovém řízení TQM [5], s implementovaným procesem analýzy rizik, respektive standardu ISO 9001 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. 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 zahrnutých do kategorie subjekt kritické infrastruktury je podřízena krizovému zákonu č. 240/2010 Sb., což znamená, že zavádí alespoň základní principy krizového řízení, tj. má povinnost vypracovat plán krizové připravenosti na základě krizového plánu dotčené oblasti, který je pravidelně přezkoumáván, a je odpovědná za veškerou součinnost s dalšími subjekty uvedenými v zákoně.

Dle [35] oblasti řízení bezpečnosti zahrnují také systémy řízení bezpečnosti informací (ISMS) a kybernetické bezpečnosti (cyber security). Zde je nutné poznamenat, že se ve skutečnosti jedná o zabezpečení informací a zabezpečení kyberprostoru (od anglického slova security), ale v českých podmínkách se ujal nepřesný pojem bezpečnost informací. Účelem uvedeného systému 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. Celkově lze říci, že současné dopravní systémy jsou zabezpečené z hlediska funkční bezpečnosti, ale nepřipouští, že se mohou vyskytnout i jiné nepředvídatelné události. Například kybernetický útok a další pohromy (i živelní) mohou uvažovaný systém uvést do abnormálních a kritických podmínek, které výrazným způsobem ohrožující své okolí.

Na základě databáze 31 selhání řídících systémů dopravy ve světě od roku 2006 [18] a výsledků výzkumu řídících systémů z dalších oblastí shrnuté v pracích [2,16], příčiny selhání kybernetických systému entit byly:

- překročení (přetížení) přenosové kapacity vlastní telekomunikační sítě,
- havárie technologických celků,
- cílené poškození informační a komunikační infrastruktury (sabotáž, hackerství, terorismus, kriminální činnost apod.),
- ztráta integrity dat v informačním systému,
- živelní pohromy velkého rozsahu jako rozsáhlé požáry, vichřice, sesuvy půdy, povodně apod. s následným poškozením nebo výpadkem informačních a komunikačních systémů (IKS),
- radiační havárie s následným poškozením nebo výpadkem řídicího systému objektu,
- havárie velkého rozsahu způsobené vybranými nebezpečnými chemickými látkami a chemickými přípravky s následným poškozením nebo výpadkem řídicího systému objektu,
- jiné technické a technologické havárie velkého rozsahu – požáry, exploze, destrukce nadzemních a pozemních částí staveb s následným poškozením nebo výpadkem IKS,
- destrukce hrází vodohospodářských děl se vznikem povodňové vlny s následným poškozením nebo výpadkem řídicího systému objektu,
- narušení dodávek elektrické energie velkého rozsahu,
- narušení zákonnosti velkého rozsahu s následným poškozením nebo výpadkem řídicího systému objektu,
- výpadky veřejných telekomunikačních sítí,
- disfunkční chování řídících a informačních systémů při zabezpečování základních funkcí státu,
- výpadek kritických informačních systémů nebo procesů.

Společné kybernetické příčiny se vyskytují především na rozhraních systémů, které jsou navrženy,

implementovány i provozovány různými subjekty s ne vždy stanovenou mírou odpovědnosti [16], 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. Analýzy provedené v pracích [16,36] odhalily příčiny:

- ***zkreslení dat z monitorování***, ke kterému dojde v systému pro sběr provozních dat, což 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 řídícím pracovníkům, 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.

Z výše uvedených důvodů významný problém nastává v dopravě u řídících systémů, a to hlavně ve spojení se zaváděním poloautomatických a automatických systémů řízení do praxe je spojeno mnoho problémů, které jsou spojené s propojeními mezi technikou, informacemi a lidským faktorem, který vytváří software pro zajištění propojení. Jde o oblast dosud, která je ve stavu zrodu, a proto nemá ustálená pravidla jako technika.

V oblasti kritické dopravní infrastruktury jde především o zajištění zvládnutí: slabin v zabezpečení vůči vnějším vlivům; výskytu vnitřních náhodných poruch systému; výskytu vnitřních systémových poruch zařízení; poruch v procesech, lidských chyb, nedostatku zdrojů; konfliktů mezi požadavky na bezpečnost a zabezpečení; chybné nebo nedostatečné identifikace ovlivňujících činitelů; chybné práce s riziky, volba metody, definice stupnic, ohodnocení rizika neodpovědnosti, nekompetence, závislosti a nedůvěryhodnosti řešitelských subjektů.

V oblastech, kde jsou nadřazené systémy propojeny toky či vazbami s podřízenými či vedlejšími systémy jde především o zabránění: přenosu chybných a matoucích informací, tj. chyby na vstupu nebo na výstupu systémů; přerušení informačních a materiálových toků; vykonávání navzájem se ovlivňujících funkcí; a poruchám okolních systémů a realizaci relevantních pohrom.

V oblastech propojení mezi jednotlivými vrstvami systému řízení bezpečnosti jde především o zabránění: aplikaci chybných metodik pro identifikace ohrožení a analýzy rizik z vyšších úrovní systému řízení bezpečnosti (SMS); neporozumění požadavkům a informacím z jiné vrstvy SMS; přenosu poruchových stavů v případě jejich výskytů z jedné vrstvy do druhé; a nedodání vstupní informace. Na rozhraní infrastruktury s okolním prostředím jde o zabránění nepředvídatelným událostem a útokům: změna podmínek pro provoz ze strany státu; úmyslná poškození; a cílené útoky.

5. Řízení rizik sledovaných kritických prvků ve prospěch bezpečnosti

Kritické prvky dopravní infrastruktury jsou složité systémy typu systémy systémů, tj. jsou to otevřené vzájemně propojené systémy, jejichž povaha je socio-kyber-fyzická [2]. V Evropě k jejich řízení používáme způsob Total Quality Management (TQM) [5,37], který je základem ISO norem třídy 9000, 14000 a dalších. Přístup TQM spočívá v tom, že na procesu zlepšování kvality se musí podílet všichni zaměstnanci, od řadových zaměstnanců až po nejvyšší řídící pracovníky. Proces zlepšování jakosti vychází z impulsu podle potřeb od zákazníka / občana. TQM vychází z toho, že trvalá kvalita výrobků a služeb se nedá zajistit příkazy, kontrolou, dílčími programy, organizačními nebo ekonomickými opatřeními, ale

cíleným hledáním, měřením a hodnocením příčin toho, proč se produktivita a kvalita nezvyšuje [37]. Je to způsob, při kterém se pozornost zaměřuje na procesy probíhající v instituci. Při implementaci TQM se přihlíží na specifika instituce, protože z důvodu účinnosti musí odpovídat struktuře instituce. TQM se využívá v řízení podniků (technických děl), obcí a regionů.

Z pohledu zajištění bezpečnosti sledovaných kritických prvků a jejich koexistence s okolím po celou dobu životnosti jde o určení velikosti příslušných rizik a jejich roztřídění do kategorií: přijatelné riziko; podmíněně přijatelné riziko, u kterého se navrhnou nutná opatření preventivní, zmírňující, reaktivní a obnovovací; a nepřijatelné riziko, u kterého se navrhne buď vyhnutí dané činnosti, je-li to možné, anebo další opatření v rámci krizového řízení, která vyžadují vyšší znalosti, vyšší technické vybavení, vyšší náklady, vyšší připravenost lidských zdrojů [8]. Proto musíme riziko selhání kritického prvku dopravní infrastruktury nejprve určit správnými nástroji.

Abychom zajistili bezpečnost technických zařízení i technických děl, řešíme problém bezpečnosti systému systémů [2,11], protože soubor propojených bezpečných systémů není ještě nutně bezpečný systém, protože bezpečnost systému systémů závisí také na charakteru vzájemných propojení mezi systémy. Důsledkem vzájemných závislostí je to, že defekt v jedné části technického díla způsobí selhání dalších částí technického díla a kaskádu dalších dopadů. To znamená, že když chceme zajistit bezpečnost systému systémů, tak kromě bezpečnosti dílčích částí technického díla musíme ještě zvlášť sledovat soubor systémů jako celek. Musíme zjišťovat: typy selhání systému systémů; provozní podmínky systému systémů; vnitřní vazby a jejich projevy; a charakteristiky kritických stavů systému systémů.

Zvládání rizik v případě, že riziko není přijatelné, spočívá dle [1,2,6,8,11] ve výběru některé z dále uvedených alternativ: vyhnutí se riziku, tj. nezahájit nebo nepokračovat v činnostech, které jsou zdrojem rizika, když to jde (lidská společnost se může bez technického díla obejít); odstranění zdrojů rizik, tj. zabránění vzniku pohrom, když to jde (zvolit alternativu technického díla, která bude mít méně zdrojů rizik, anebo menší rizika); snížení pravděpodobnosti výskytu rizika, tj. výskytu větších pohrom, když to jde (aplikace zásad kultury bezpečnosti); snížení závažnosti dopadů rizika, tj. příprava zmírňujících opatření jako jsou varovací systémy, systémy odezvy a obnovy; sdílení rizika, tj. rozdělení rizika mezi zúčastněné a pojišťovny; a retence rizika.

Vyjednávání s riziky vychází ze současných možností lidské společnosti a spočívá dle [1,2,6,8,11] v rozdělení rizik do kategorií, ve kterých se část rizika: sníží, tj. preventivními opatřeními se odvrátí realizace rizika; zmírní, tj. preventivními opatřeními a připraveností (varovné systémy a jiná opatření nouzového a krizového řízení) se sníží nebo odvrátí nepřijatelné dopady; pojistí; zajistí opatřeními odezvy a obnovy, pro které se připraví rezervy všeho druhu; a pro část, která je neřiditelná nebo příliš nákladná nebo málo častá se připraví plán pro nepředvídané situace (Contingency plan).

Ačkoliv koncept integrální (celkové) bezpečnosti se rozšiřuje v praxi pomalu z důvodů uvedených v práci [38], je třeba ho prosazovat, protože do pojetí integrální bezpečnosti patří i život podporující funkce, jejichž rizika s ohledem na zdraví člověka, ekosystémy a bezpečnost systému se minimalizují. Generický model pro řízení bezpečnosti kritických prvků dopravní infrastruktury ukazuje způsob řízení rizik, aby se předešlo, anebo alespoň zmírnilo možným nežádoucím a nepřijatelným dopadům. Jde především o zajištění zvládnutí: slabin v zabezpečení vůči vnějším vlivům; výskytu vnitřních náhodných poruch systému; výskytu vnitřních systémových poruch zařízení; poruch v procesech, lidských chyb, nedostatku zdrojů; konfliktů mezi požadavky na bezpečnost a zabezpečení; chybné nebo nedostatečné identifikace ovlivňujících činitelů; chybné práce s riziky, volba metody, definice stupnic, ohodnocení rizika neodpovědnosti, nekompetence, závislosti a nedůvěryhodnosti řešitelských subjektů. V oblastech, kde jsou nadřazené systémy propojeny toky či vazbami s podřízenými či vedlejšími systémy jde především o zabránění: přenosu chybných a matoucích informací, tj. chyby na vstupu nebo na výstupu systémů; přerušení informačních a materiálových toků; vykonávání navzájem se ovlivňujících funkcí; a poruchám okolních systémů a realizaci relevantních pohrom.

V oblastech propojení mezi jednotlivými vrstvami systému řízení bezpečnosti jde především o zabránění: aplikaci chybných metodik pro identifikace ohrožení a analýzy rizik z vyšších úrovní systému řízení bezpečnosti (SMS); neporozumění požadavkům a informacím z jiné vrstvy SMS; přenosu poruchových stavů v případě jejich výskytů z jedné vrstvy do druhé; a nedodání vstupní informace. Na rozhraní infra-

struktury s okolním prostředím jde o zabránění nepředvídatelným událostem a útokům: změna podmínek pro provoz ze strany státu; úmyslná poškození; a cílené útoky.

Generický model pro řízení bezpečnosti sledovaných kritických prvků dopravní infrastruktury založený na typu řízení TQM je sestaven v práci [39]. Opírá se o systematický monitoring významných rizik a jejich soustavné řízení. Jde o řízení nejen významných dílčích rizik, ale především o řízení integrálního rizika pomocí specifických systémů pro podporu rozhodování, které byly sestaveny pro jednotlivé sledované kritické prvku [11-16,30], protože 80% selhání a havárií vzniká v důsledku kombinace několika příčin, které samy o sobě by k selhání či havárii nevedly [1,2,11-16,30]. Velká pozornost je věnována původcům tzv. organizačních havárií, tj. havárií nebo selhání entit, které jsou způsobené špatným rozhodováním a řízením lidí odpovědných za entitu [8].

6. Návrhy opatření

Ve sdělení [39] jsme uvedli výsledky srovnání nároků české legislativy na řízení bezpečnosti a na řízení rizik ve prospěch bezpečnosti vybraných prvků dopravní kritické infrastruktury se současným odborným poznáním, reprezentovaným generickým modelem pro zajištění integrální bezpečnosti. Srovnání ukázalo, že při aplikaci pětistupňové stupnice (tabulka 1), je míra nedostatků legislativy z hlediska úplnosti požadavků na:

- integrální bezpečnost je 4 (86.3 %), tj. je velmi vysoká,
- práci s riziky je 4 (85.8 %), tj. je velmi vysoká.

Tabulka 1. Míra nedostatků legislativy pro zajištění integrální bezpečnosti / kvalitu práce s riziky.

Míra nedostatků	**Hodnoty v % N**
Extrémně vysoká – 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 prvním případě jde především o oblast organizace veřejné správy, ve které chybí:

- orgán dozoru nad bezpečností vybavený dostatečnými pravomocemi,
- odborný systém řízení bezpečnosti jak celého dopravního systému, tak vybraných prvků dopravní kritické infrastruktury.

Ministerstvo dopravy je sice statutárním orgánem státu pro dopravní stavby, ale nemá specifické nástroje, zakotvené v legislativě pro zajištění kvality staveb. Na úseku dozoru nad kvalitou provozu dopravní infrastruktury, tj. i kritických prvků infrastruktury, nemá síť orgánů dozoru ve struktuře veřejné správy.

Specifické zákony o dopravě (zákon č. 111/ 1994 Sb., o silniční dopravě; zákon č. 266/1994 Sb., o drahách; zákon č. 12/1997 Sb., o bezpečnosti a plynulosti provozu na pozemních komunikacích; zákon č. 13/1997 Sb. o pozemních komunikacích; zákon č. 49/1997 o civilním letectví; zákon č. 361/2000 Sb., o provozu na pozemních komunikacích; zákon č. 56/2001 Sb., o podmínkách provozu vozidel na pozemních komunikacích) ***nerozlišují v systému správy celkovou bezpečnost objektů a sítí a bezpečnost procesů spojených s provozem***. V zákoně č. 266/1994 Sb. není jasně stanovena pravomoc a odpovědnost Drážního úřadu.

U sledovaných kritických prvků dopravní infrastruktury se řešení událostí jako je pád letadla či teroristických útok specificky neřeší, ačkoliv mohou být vážně poškozeny zájmy státu (zákon č. 110/1998 Sb.). Požadavky na sledované prvky kritické dopravní infrastruktury spojené: se zákonem č. 240/2000 Sb. a

souvisejícími předpisy; se zákony č. 22/1997 Sb. a 250/2021 Sb. ; zákonem č. 181/2014 Sb., o kybernetické bezpečnosti, jsou sledovány pouze v obecné rovině.

V druhém případě jde především o zabezpečený systém řízení bezpečnosti jednotlivých kritických prvků dopravní infrastruktury, který je založen na kontinuálním řízení rizik ve prospěch bezpečnosti ve všech fázích životnosti předmětných prvků. ***Legislativa*** neukládá zajišťovat celkovou bezpečnost sledovaných kritických prvků dopravní infrastruktury; obvykle ***se zaměřuje jen na bezpečnost procesů spojených s provozem***. Pro řízení rizik v drážní dopravě jsou široce používány postupy RAM a RAMS, kterými se zajišťuje v prvním případě spolehlivost, dostupnost a udržitelnost a v druhém ještě bezpečnost [40] ve smyslu zabezpečení, protože nezvažuje ochranu okolí; pro sledované prvky kritické dopravní infrastruktury však nejsou upraveny. Ochrana okolí je legislativou systematicky vyžadována jen u letišť. Legislativa speciálně neukládá odstraňovat příčiny organizačních havárií a sledovat skoro nehody u sledovaných prvků kritické dopravní infrastruktury. Pro případy požárů jsou požadovány poplachové směrnice. Je také fakt, že legislativa neukládá správcům mít vlastní plány odezvy na nouzové situace; obvykle se spoléhá na IZS (zákon č. 239/2000 Sb.).

Lze říci, že česká legislativa v řadě případů ustrnula na poznání z 80. let minulého století a dosud nezavedla, anebo jen v omezené míře zavedla současné poznatky o řízení bezpečnosti a o práci s riziky ve prospěch bezpečnosti. Přestože česká republika je člen EU, nezavedla důsledně typ řízení TQM, ve kterém jsou jasně stanoveny odpovědnosti a jasná pravidla pro práci s riziky. V řadě případů spojených s dopravními systémy, dopravní infrastrukturou a sledovanými kritickými prvky dopravní infrastruktury sice legislativa požaduje bezpečnost, ale pojem samotný nedefinuje a normy i metodiky jsou obvykle příliš obecné, anebo je zřejmé, že se vztahují ke spolehlivosti a ne bezpečnosti. Pro dosažení úrovně ve vyspělých zemích světa je nutné zajistit nejen úpravu legislativy, ale také potřebnou vzdělanost.

Přitom jsme zjistili řadu dílčích nedostatků, např.:

- zákon č. 266/ 1994 Sb.: se stále odkazuje na již neplané předpisy EU 2004/49/ES a 2008/57/ES; není provázán s krizovou legislativou v oblasti určení prvků, které musí mít plán krizové připravenosti,
- směrnice EU 2016/797 z 11. května 2016, o interoperabilitě železničního systému v Evropské unii se dosud nepromítla do české legislativy,¨
- koncept Defence-in-Depth [41] je aplikován jen v omezené míře,
- v železniční dopravě se v souvislosti s riziky často používají normy, např. norma EN 50126, která nemá oporu v českých zákonech,
- stavební zákon je příliš obecný, neobsahuje ani požadavky na zadávací podmínky stavby, a tím dochází k tomu, že např. příčinou selhání mostů jsou externí zdroje rizik (sesuvy, povodně, vítr, poklesy podloží) atd.

Proto, v prvé řadě je nutné do legislativy zavést důsledně principy TQM [5,37], což mimo jiné znamená, že stát v rámci péče o veřejná aktiva zajistí dohled a dozor nad sledovanými kritickými prvky dopravní kritické infrastruktury. To znamená, že tímto způsobem se začne vyžadovat důsledná aplikace principů řízení rizik u sledovaných prvků dopravní kritické infrastruktury zacílená na integrální bezpečnost. Zároveň se tím nastaví jistá úroveň kultury bezpečnosti při tvorbě a provozu sledovaných prvků dopravní kritické infrastruktury, která souvisí s organizační kulturou a je souborem dohodnutých pravidel uplatňovaných v řízení nejen sledovaných prvků, ale i organizačních jednotek státu dohlížejících na tvorbu a provoz sledovaných entit, tj. na vytváření norem institucionálního chování.

Kultura bezpečnosti znamená správné aplikování znalostí, přemýšlení a správné reakce na reálné situace. Nejde totiž jenom o dodržování norem a předpisů zacílených na spolehlivost sledovaných entit, protože tím můžeme přehlédnout jevy, které normy a předpisy nevidí. Z hlediska veřejného zájmu sledované entity musí být bezpečné, tj. zajišťovat požadované úkoly na úseku obslužnosti a ani při svých kritických podmínkách neohrožovat sebe a své okolí.

Z porovnání nároků na zajištění bezpečnosti kritických prvků entit, které mají socio-kyber-fyzickou strukturu (tvoří systémy systémů), shrnutých v práci [39] a požadavků uvedených v české legislativě vyplývá, že pro zajištění bezpečnosti kritických prvků dopravní infrastruktury je třeba do české legislativy doplnit:

- jasné úkoly a odpovědnosti, jak pro veřejnou správu, tak pro management kritických prvků,
- jasné pokyny pro práci s riziky, tj. používat propojení norem a výsledků řízení rizik, moderní přístupy: All-Hazard Approach [42,43]; Defence-in-Depth [41]; a risk-based design, risk-based operation, risk-based inspection, risk-based maintenance [11,19,20].

Předmětné nároky jsou ve vyspělých zemích již zohledněny.

V dalším kroku je nutné u sledovaných kritických prvků dopravní kritické infrastruktury zavést:

- povinnost zpracovávat bezpečnostní dokumentaci ve formě bezpečnostní zprávy v rozsahu běžném ve vyspělých zemích, ve které bude upřednostněna integrální bezpečnost,
- zřídit orgán, který bude vykonávat státní dozor nad bezpečností,
- jasnou organizační strukturu systému řízení bezpečnosti (SMS) kritických prvků dopravní infrastruktury a odpovědnosti: vrcholový management; vyšší management; střední management; technický management; a personál (kritický a podpůrný). Na jednotlivých úrovních jasně stanovit úkoly, odpovědnosti a požadavky na spolupráci na horizontálních i vertikálních úrovních,
- jasnou organizační strukturu dozoru nad bezpečností kritických prvků dopravní infrastruktury a odpovědnosti na úrovni organizačního řízení státu,
- pro zajištění bezpečnosti monitoring kritických prvků dopravní infrastruktury a provádět pravidelně hodnocení rizik, anebo po každé havárii či selhání kritického prvků dopravní infrastruktury,
- metodu hodnocení rizik z pohledu složitosti entity a časového intervalu, ke kterému se hodnocení vztahuje,
- povinnost investorů i provozovatelů entity a orgánů státní správy realizovat odborná doporučení pro zlepšení bezpečnosti kritických prvků dopravní infrastruktury – risk based design; risk-based inspections; risk-based maintenance a risk-based operation. Jde o propojení norem a výsledků analýzy rizik jak doporučují ISO 31 000 a ISO 31 010 a další ISO normy pro konkrétní položky,
- povinnost zpracovávat plán řízení rizik, kterým se zvládnou havárie a selhání kritických prvků dopravní infrastruktury a předem se vyřeší konflikty mezi zájmy zúčastněných, které během životnosti entity mohou nastat.

Systém řízení bezpečnosti (SMS) musí mít jasný program na udržování a stálého zvyšování bezpečnosti, a to včetně kultury bezpečnosti. V případě automatizace musí být řádně zabezpečen proti útokům všeho druhu [5,16]. Pro jeho správnou funkčnost správce kritického prvku dopravní infrastruktury (entity) pro zajištění bezpečnosti musí mít legislativou uloženy povinnosti:

- monitoroval situaci a provoz dopravy v entitě a jejím okolí s použitím kamer a senzorů a komunikačního zařízení s cílem zajistit normální provoz,
- mít připravenu odezvu pro případ selhání entity,
- mít účinný varovací systém a schopnost rychlé a správné detekce jakéhokoliv jevu, který může vést k selhání entity a její funkce,
- mít zařízení pro uzavření entity,
- mít zařízení pro kontakt se záchrannými službami,
- mít zařízení pro kontakt s uživateli entity,
- mít vycvičený personál pro řízení tunelu za možných situací – normální, nouzové i kritické,
- mít plán údržby,
- mít plán kontrol – nutná pravidelná kontrola kritických prvků entity a podmínek okolí, a nouzových opatření včetně jejich zajištění,
- mít plán pro řízení rizik.

Bezpečnostní dokumentace i plán řízení rizik entity musí z hlediska veřejného zájmu zohlednit:

- dopady: možných živelních pohrom na entitu a četnost výskytu extrémních pohrom; klimatických a meteorologických podmínek na entitu a četnost výskytu extrémních podmínek; provozních poruch a nehod na entitu a četnost jejich výskytu; možných požárů na entitu a četnost jejich výskytu; možných explozí na entitu a četnost jejich výskytu; možných mechanických poškození entity a četnost jejich výskytu; možných dopravních nehod v entitě a četnost jejich výskytu; dopady chyb v projektu entity jako: špatné kombinace zatížení; podcenění velikostí možných pohrom; nezvážení resonancí v konstrukci; podcenění vibrací; nezvážení aerodynamických sil; nezvážení geotechnických

zranitelností v podloží apod.; možných chyb při výstavbě a konstrukci entity jako: nekvalitní materiál (často ochuzený beton); skryté vady v materiálu; špatné ukotvení; chyby ve spojích komponent; špatné provedení kritických prvků (např. mostních oblouků ostění tunelů) apod.; možných chyb v provozu entity jako: nedostatečná údržba; zanedbané opravy; neprovádění včasných oprav; častá přetížení; koroze; únavové trhliny v materiálu; podcenění stárnutí materiálu apod.; možných změn způsobených stárnutím jako: koroze např. u ocelových výztuží u mostů a tunelů; rozvrstvení betonových desek; velká šířka trhlin v betonových strukturách entity; únava ocelových struktur; velké napjatostí v ocelových strukturách apod.); možných sabotáží v entitě a četnost jejich výskytu; a možných teroristických útoků na entitu a četnost jejich výskytu,
- nároky na obslužnost, kterou zajišťuje entita z pohledu: území; obrany; průmyslu; IZS (Integrovaný záchranný systém); a sociálních potřeb občanů,
- ekonomické ztráty způsobené nefunkčností entity po dobu delší než 14 dnů,
- úroveň fyzické ochrany entity,
- úroveň promyšleného rozmístění záloh prioritních komponent entity,
- úroveň zajištění náhradních řešení v případě selhání entity,
- úroveň řízení bezpečnosti entity (kultura bezpečnosti, systém řízení bezpečnosti mostu – fáze: prevence, připravenost, odezva, obnova).

Orgán veřejné správy pověřený dohledem a dozorem nad bezpečností musí mít legislativou uloženy povinnosti mít plán inspekcí a jejich základní rozsah s ohledem na rizika spojená s entitou a jejím okolím.

7. Závěr

Dnešní společnost je závislá na technických a kybernetických systémech, které přispívají k uspokojení základních potřeb lidí, tak se 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. Pro zajištění bezpečí lidí potřebujeme zajistit zabezpečení a v mnoha případech také bezpečnostní kyber-fyzické systémy.

Řízení každé entity dělíme dle rozsahu odpovědnosti, rozhodování a délky plánovacího horizontu. Každá entita plánuje a řídí své aktivity a procesy celkem 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. V obecném smyslu rozumíme řízením usměrňování procesů nebo činností, které probíhají v určitém dynamickém systému. Řízení socio-kyber-fyzických děl znamená propojit procesy řízení lidí a řízení technických procesů ve smyslu jejich ovládání. Řízení ve smyslu ovládání techniky lze provádět manuálně (ručně), poloautomaticky a automaticky.

Práce shrnuje výsledky řízení rizik pro mosty, tunely, pozemní komunikace, nádraží / železniční stanice, letiště, a řídící systémy dopravy. Společným jmenovatelem zjištěných výsledků je nedostatečná práce s riziky ve prospěch bezpečnosti a nestanovení odpovědností v oblasti řízení prvků. Pro uvedené prvky sestavuje nástroje pro stanovení rizik [12-16] tak, aby o nich bylo možno správně rozhodovat ve prospěch bezpečnosti. Protože svět se dynamicky mění, tak se mění i podmínky. Tím vznikají situace, kdy podmínky jsou takové, že se překročí limity, na které sledované prvky vyprojektované, což pochopitelně vede k selháním a haváriím. Významným faktorem je i stárnutí materiálů a jejich propojení a zastarávání technologií [11].

Literatura

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

[2] PROCHÁZKOVÁ, D. *Zásady řízení rizik složitých technologických zařízení*. ISBN 978-80-01-06180-0, e-ISBN:78-80-01-06182-4. Praha: ČVUT 2017, 364 p. doi.org/10.14311%2 FBK.978 80010 61824

[3] UN. *Human Development Report*. New York 1994, www.un.org

[4] EU. The Safe Community Concept. *PASR project*. Brussels: EU 2004.

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

[6] PROCHÁZKOVÁ, D. *Strategické řízení bezpečnosti území a organizace*. ISBN 978-80-01-04844-3. Praha: ČVUT 2011, 483 p.

[7] PROCHÁZKOVÁ, D., ŠESTÁK, B. *Řízení bezpečnosti a krizové řízení*. ISBN 80-7251-212-9. Praha: Policejní akademie ČR 2005, 242 p.

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

[9] PROCHÁZKOVÁ, D. *Rizika spojená s pohromami a inženýrské postupy pro jejich zvládání*. ISBN 978-80-01-05479-6. Praha: ČVUT 2014, 234 p.

[10] PROCHÁZKOVÁ, D., PROCHÁZKA, J. *Integrální bezpečnost zajišťuje optimální rozvoj životního prostředí*. ISBN 978-80-01-05480-2. ČVUT, Praha 2014, 224 p.

[11] PROCHÁZKOVÁ, D., PROCHÁZKA, J., LUKAVSKÝ, J., DOSTÁL, V., PROCHÁZKA, Z., OU-HRABKA, L. Řízení rizik procesů spojených s provozem technického díla během jeho životnosti. ISBN 978-80-01-06675-1. Praha: ČVUT 2019, 465 p. doi.org/10.14311%2FBK.9788001066751

[12] PROCHÁZKA, J., PROCHÁZKOVÁ, D. Rizika a bezpečnost mostů. In: Řízení rizik procesů a bezpečnost složitých technických děl. ISBN 978-80-01-06786-4. Praha: ČVUT 2020, pp. 107-179; doi: 10.14311/BK. 9788001067864

[13] PROCHÁZKOVÁ, D., PROCHÁZKA, J. Rizika a bezpečnost tunelů na pozemních komunikacích. In: Řízení rizik procesů a bezpečnost složitých technických děl. ISBN 978-80-01-06786-4. Praha: ČVUT 2020, pp. 268-318; doi.org/10.14311/BK.9788001067864

[14] PROCHÁZKOVÁ, D., PROCHÁZKA, J. Rizika spojená s kritickými vlakovými a autobusovými nádražími. *Soudní inženýrství*. ISSN 1211-443X. 32 (2021), 3, pp. 33-46.

[15] 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; doi.org/10.1 4311/ BK.97880 01069066

[16] PROCHÁZKA, J., PROCHÁZKOVÁ, D. *Řízení rizik systémů pro řízení dopravy*. ISBN 978-80-01-06995-0. Praha: ČVUT 2022, 129 p.; doi:10.14311/BK.9788001069950.

[17] PROCHÁZKOVÁ, D. *Metody, nástroje a techniky pro rizikové inženýrství*. ISBN 978-80-01-04842-9. Praha: ČVUT 2011, 369 p.

[18] ČVUT. Databáze pohrom, selhání a havárií, rizik, způsobů odezvy a získaných poučení. *Archiv.* Praha: ČVUT 2022.

[19] PROCHÁZKOVÁ, D. Risk-based Design of Technical Facilities. In: *JUFOS 2021*. ISBN 978-80-214-5963-2. Brno: VUT 2021, pp. 40-51.

[20] PROCHAZKOVA, D., PROCHAZKA, J. Risk Management Plan for Technical Facility Operation. In: *Proceedinggs the 31st ESREL Conference.* ISBN 978-981-18-2016-8, p. 1502-1509, Singapore:

Research Publishing(s) Pte Ltd. editorial@rpsonline.com.sg 2021. doi:10.3850/978-981-18-2016-8_124-cd

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

[22] PROCHÁZKA, J., PROCHÁZKOVÁ, D., VESELÍK, P. Mosty – jejich rizika a nástroje pro řízení bezpečnosti. In: *Criscon 2020 – Krizové řízení a řešení krizových situací*. ISBN 978-80-7454-957-1. Zlín: UTB 2020, pp. 335-346. http://hdl.handle.net/10563/45944

[23] PROCHÁZKA, J., PROCHÁZKOVÁ, D. Řízení rizik mostů. In: *Globálné existenciálné rizika*. ISBN 978-80-973460-4-1. Bratislava: SSŽP 2021, pp. 185-194.

[24] PROCHÁZKA, J., PROCHÁZKOVÁ, D. Příklad selhání mostní konstrukce. In: *JUFOS 2021*. ISBN 978-80-214-5963-2. Brno: VUT 2021, pp. 153-159.

[25] HÝZL, P., MATUSZKOVA, R., PROCHÁZKOVÁ, D. Příklad selhání mostu na D1. *Soudní inženýrství*. ISSN 1211-443X. 32 (2021), 2, pp. 28-34. DOI http://dx.doi.org./10.13164/SI.2021.2.28

[26] PROCHÁZKA, J., PROCHÁZKOVÁ, D. Prognostická případová studie - selhání železničního mostu Výtoň – Smíchov. *Soudní inženýrství*. ISSN 1211-443X. 32 (2021), 4, pp. 17-21. DOI http://dx.doi.org./10.13164/SI.2021.4.17

[27] GEYSEN, W. The Acceptance of Systemic Thinking in Various Fields of Technology and Consequences on Respective Safety Phylosophies. In: *Safety of Modern Systems. Congress Documentaion Saarbruecken 2001*. ISBN 3-8249-0659-7. Cologne: TŰV- Verlag GmbH, 2001, pp. 19-27.

[28] PROCHÁZKOVÁ D., PROCHÁZKA, J., MARTINCOVÁ, J. V., KERTIS, T. Measures for Tunnel safety Management. In: ESREL 2022 Proceedings. Singapore: Research Publishing(s) Pte Ltd. editorial@rpsonline.com.sg 2021; *v tisku*.

[29] PROCHÁZKOVÁ, D., PROCHÁZKA, J., PATÁKOVÁ, H., PROCHÁZKA, Z., STRYMPLOVÁ, V. *Kritické vyhodnocení přepravy nebezpečných látek po pozemních komunikacích v ČR*. ISBN 978-80-01-05599-1. Praha: ČVUT 2014, 150 p.

[30] 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

[31] UN. *ADR*. http://www.unece.org/trans/danger/publi/adr/adr2019/19contentse.html

[32] OTIF. RID –- Regulations concerning the International Carriage of Dangerous Goods by Rail. In: *Convention concerning International Carriage by Rail (COTIF)* - Appendix C.

[33] PLÁŠEK, O., HRUZÍKOVÁ, M., PROCHÁZKOVÁ, D. Vykolejení drážních vozidel v důsledku lomu jazyka výhybek. *Soudní inženýrství*. ISSN 1211-443X. 31 (2020), 4, pp. 17-21. http://dx.doi.org./10.13164/SI.2020.4.17

[34] PROCHÁZKOVÁ, D., PROCHÁZKA, J. Causes of Accidents in Civilian Aircraft Operation and Tools for Management of Selected Risks. In: *Safety and Reliability – Theory and Applications*. ISBN 978-1-138-62937-0. London: Taylor & Francis Group 2017, pp. 3057-3066.

[35] 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.

[36] 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.

[37] NENADÁL, J. *TQM. Role ekonomiky jakosti v koncepci TQM*. 1999, www: http://fmmi10.vsb.cz/639/qmag/mj03-cz.htm.

[38] PROCHÁZKOVÁ, D. Integral Safety. In: *Motivation – Education – Trust – Environment – Safety*. ISBN 978-80-973460-7-2. Bratislava: SSŽP et STRIX 2021, pp. 69-73.

[39] PROCHÁZKOVÁ D., PROCHÁZKA, J., MARTINCOVÁ, J. V., KERTIS, T. Návrhy opatření pro zvýšení bezpečnosti vybraných prvků dopravní kritické infrastruktury. In: *ExFoS 2022*. ISBN 978-80-214-6033-1. Brno: VUT 2022, pp. 343-386.

[40] MAHOOB, Q., ZIO, E. *Handbook of RAMS in Railway Systems. Theory and Practice*. ISBN 978-113 803-512-6. London: CRC Press 2018, 765 p.

[41] INSAG. Defence in Depth in Nuclear Safety. INSAG-10. ISBN 92-0-103295-1 IAEA, 1996.

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

[43] EU. *FOCUS Project*. Brussels: EU 2012, http://www.focusproject.eu/documents/14976/-5d73378-1198-4dc9-86ff-c46959712f8a

Poděkování: Článek byl vypracován v rámci projektu TAČR CK01000095 Plán řízení rizik pro vybrané kritické objekty dopravní infrastruktury.