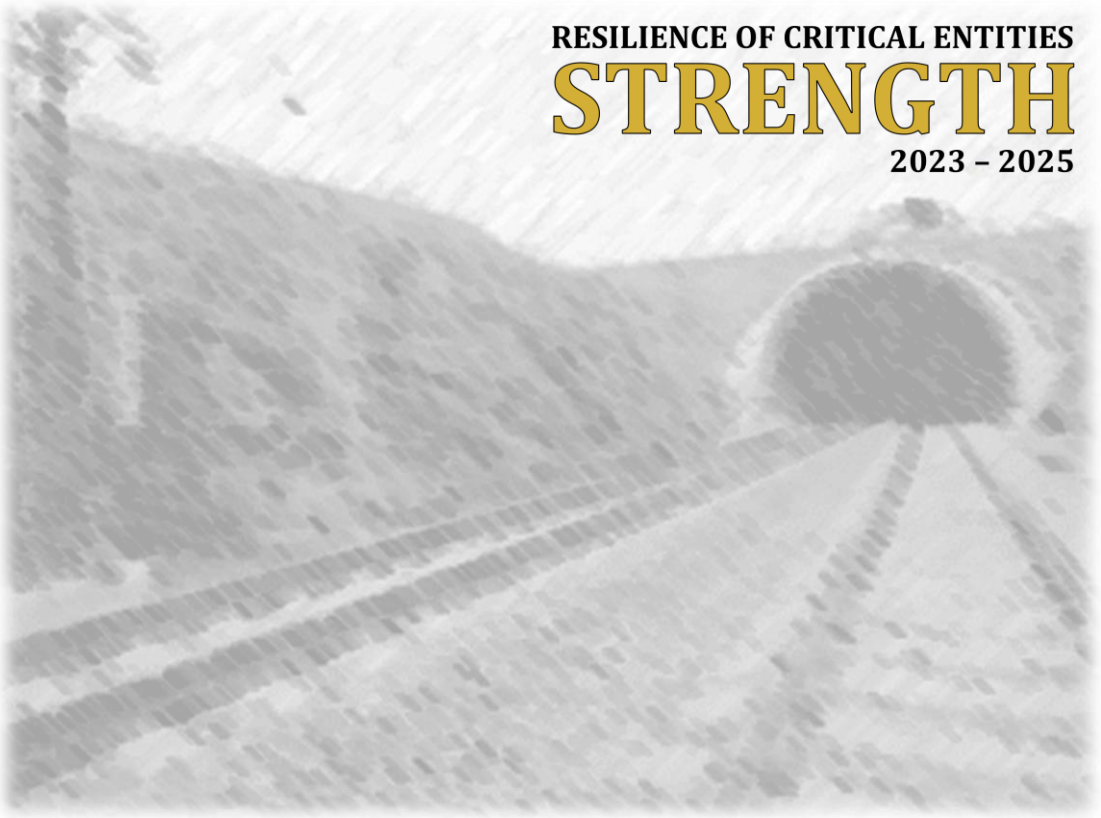
VŠB TECHNICKÁ UNIVERZITA OSTRAVA | FAKULTA BEZPEČNOSTNÍHO INŽENÝRSTVÍ

FAKULTA DOPRAVNÍ ČVUT V PRAZE



METODICKÝ POSTUP POSILOVÁNÍ RESILIENCE KRITICKÝCH SUBJEKTŮ

DAVID ŘEHÁK ET AL.
VŠB – TECHNICKÁ UNIVERZITA OSTRAVA
Fakulta bezpečnostního inženýrství

OSTRAVA 2025

ŘEHÁK, David et al. *Metodický postup posilování resilience kritických subjektů*. [Certifikovaná metodika]. Ostrava: VŠB – Technická univerzita Ostrava, 2025. 38 s.

Autorský tým

VŠB – Technická univerzita Ostrava, Fakulta bezpečnostního inženýrství

prof. Ing. David Řehák, Ph.D.
prof. Ing. Martin Hromada, Ph.D.
Ing. Alena Šplíchalová, Ph.D.
Ing. Ondřej Ryška

České vysoké učení technické v Praze, Fakulta dopravní

doc. Ing. Zdeněk Lokaj Ph.D., LL.M.
Ing. Lenka Michalcová, Ph.D.

Oponenti:

prof. Ing. Zdeněk Dvořák, PhD.
Žilinská univerzita v Žiline, Fakulta bezpečnostného inžinierstva

doc. Ing. Pavel Maňas, Ph.D.
Univerzita obrany, Fakulta vojenských technologií

Metodika byla zpracována za podpory grantového projektu VK01030014
"STRENGTH 2023: Posilování resilience subjektů pozemní dopravní kritické infrastruktury",
podpořeného Ministerstvem vnitra České republiky v letech 2023-2025.

RESILIENCE OF CRITICAL ENTITIES
STRENGTH
2023 – 2025

Certifikační orgán

Ministerstvo dopravy, Odbor kosmických aktivit a nových technologií a inovací v dopravě
JUDr. Václav Kobera
ředitel

Č. j.: MD-7176/2025-730/46
Datum schválení: 31. 7. 2025

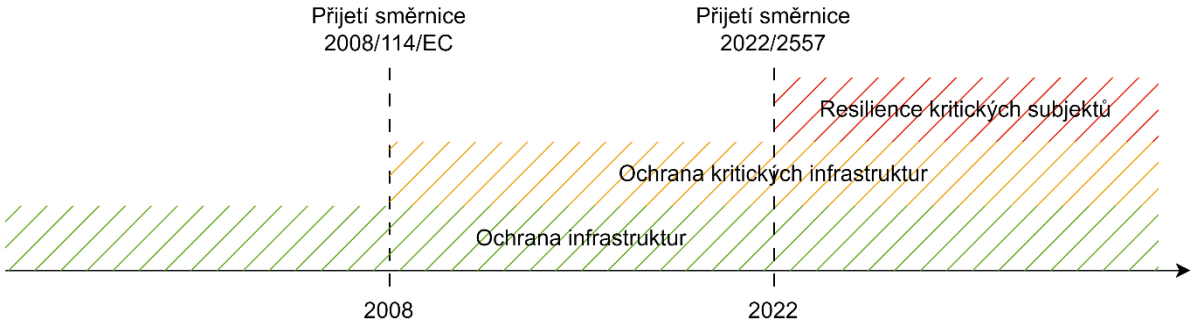
Obsah

1 Obecná ustanovení

Obecná ustanovení prezentují vstupní informace o metodickém postupu posilování resilience kritických subjektů. Vymezují základní parametry metodiky, včetně jejího předmětu, cílové skupiny, omezujících podmínek a používané terminologie.

1.1 Předmět metodiky

Přijetím Směrnice o resilienci kritických subjektů (Směrnice 2557, 2022) dochází v Evropské unii k zásadní změně ve vnímání bezpečnostního přístupu v systému kritické infrastruktury (viz Obrázek 1). Dosavadní přístup založený na ochraně kritických infrastruktur je nahrazen novým přístupem založeným na resilienci kritických subjektů, které jsou vlastníky nebo provozovateli těchto infrastruktur.



Obrázek 1: Vývoj bezpečnostního přístupu k ochraně infrastruktur v Evropské unii

Aktuálně platná směrnice (Směrnice 2557, 2022) ukládá kritickým subjektům povinnost přijmout opatření ke zvýšení své resilience, avšak neposkytuje jim žádnou metodickou oporu. Z tohoto důvodu je cílem tohoto dokumentu definování metodického postupu, který umožní kritickým subjektům v sektoru dopravy posílit úroveň jejich resilience vůči incidentům.

Tento postup je klasifikován do dvou fází, které zahrnují celkem devět kroků. První fáze je zaměřena na posuzování resilience kritických subjektů vůči incidentům. Podstatou této fáze je definování scénáře incidentu, na jehož základě je následně vyhodnocena úroveň naplňování jednotlivých faktorů determinujících resilienci kritického subjektu. Druhá fáze je zaměřena na posilování resilience kritických subjektů vůči incidentům. Podstatou této fáze je identifikace nedostačujících a kritických faktorů, výběr vhodných posilujících nástrojů a jejich implementace do procesů kritického subjektu.

1.2 Cílová skupina

Metodika je určena primárně pro posilování resilience kritických subjektů dopravní kritické infrastruktury. Sekundárně však může být využita také pro kritické subjekty ostatních technicky orientovaných infrastruktur. Terciárně může být využita také pro posilování resilience kritických subjektů vlastnících či provozujících socio-ekonomické infrastruktury. Avšak v tomto případě je nutné nejprve provést revizi jednotlivých faktorů resilience a v případě potřeby provést jejich redefinování do socio-ekonomického kontextu.

1.3 Omezující podmínky

Praktické použití metodického postupu je limitováno níže uvedenými skutečnostmi:

- metodika umožňuje posuzování a posilování pouze vnitřní resilience kritických subjektů,
- metodika je založena na principu sebe-hodnocení kritických subjektů, které umožňuje parciální subjektivitu výsledků,
- metodický postup je primárně určen pro posilování resilience kritických subjektů vlastnících či provozujících dopravní kritické infrastruktury.

1.4 Vymezení pojmů

Kritická infrastruktura

Kritickou infrastrukturou se rozumí aktivum, zařízení, vybavení, síť nebo systém či část aktiva, zařízení, vybavení, sítě nebo systému, které jsou nezbytné pro poskytování základní služby. (Směrnice 2557, 2022)

Základní služba

Základní službou se rozumí služba, která je zásadní pro zachování nejdůležitějších společenských funkcí, hospodářských činností, veřejného zdraví a bezpečnosti nebo životního prostředí. (Směrnice 2557, 2022)

Incident

Incidentem se rozumí událost, která může významně narušit nebo která narušuje poskytování základní služby, včetně případů, kdy ovlivňuje vnitrostátní systémy chránící právní stát. (Směrnice 2557, 2022)

Kritický subjekt

Kritickým subjektem se rozumí veřejný nebo soukromý subjekt, který je vlastníkem nebo provozovatelem kritické infrastruktury nezbytné pro poskytování základní služby. (Směrnice 2557, 2022)

Resilience

Resiliencí se rozumí schopnost kritického subjektu předcházet incidentům, chránit se před těmito incidenty, reagovat na ně, odolávat jim, zmírňovat a absorbovat je, přizpůsobovat se jim a zotavit se z nich. Resilience kritických subjektů je determinována jejich rezistencí, robustností, obnovitelností a adaptabilitou. (Směrnice 2557, 2022)

Rezistence

Rezistencí se rozumí schopnost kritického subjektu zabránit vzniku incidentů. (Rehak et al., 2024a)

Robustnost

Robustností se rozumí schopnost kritického subjektu absorbovat dopady incidentů. (Rehak et al., 2024a)

Obnovitelnost

Obnovitelností se rozumí schopnost kritického subjektu obnovit funkci svých infrastruktur a úroveň své resilience po incidentech. (Rehak et al., 2024a)

Adaptabilita

Adaptabilitou se rozumí schopnost kritického subjektu přizpůsobit úroveň své resilience na již proběhlé incidenty. (Rehak et al., 2024a)

1.5 Seznam zkratek

CERA	Critical Entities Resilience Assessment
ETA	Event Tree Analysis (Analýza stromu událostí)
FMECA	Failure Mode, Effects & Criticality Analysis (Analýza způsobů, důsledků a kritičnosti poruch)
PDCA	Plan–Do–Check–Act (naplánuj-proveď-ověř-jednej)
TEN-T	Trans-European Transport Networks (Transevropská dopravní síť)

2 Východiska posilování resilience kritických subjektů

Podstatou této části metodiky je seznámit uživatele s řešenou problematikou. Za tímto účelem je nejprve provedena deskripce kritických subjektů a jimi poskytovaných základních služeb. Následně je věnována pozornost incidentům a jejich dopadům na kritické subjekty. V rámci poslední části jsou definovány faktory determinující resilienci kritických subjektů.

2.1 Kritické subjekty a jimi poskytované základní služby

Společnost, zejména ve vysoce urbanizovaných oblastech, je již dlouhodobě závislá na poskytování základních služeb. Tyto základní služby jsou poskytovány prostřednictvím kritických infrastruktur (De Felice et al., 2022), které jsou na strategické úrovni klasifikovány na technické (základní) a socioekonomické (Mukherjee et al., 2023). Technické infrastruktury poskytují služby nezbytné pro běžné fungování společnosti, zejména dodávky energií a pitné vody, ale také dostupnost digitálních či dopravních služeb. Oproti tomu socioekonomické infrastruktury nabývají svého významu zejména v čase působení incidentů, kdy zajišťují primárně dostupnost zdravotní péče, která je poskytována nemocnicemi, či nouzových služeb, které jsou poskytovány hasičským záchranným sborem a policií.

Vlastníci a provozovatelé těchto kritických infrastruktur jsou ve všech 11 sektorech označovány jako kritické subjekty. Avšak podmínkou určení vlastníka či provozovatele jako kritického subjektu je splnění tří kritérií stanovených směrnicí (Směrnice 2557, 2022). Tato kritéria jsou následující: 1) subjekt poskytuje jednu nebo více základních služeb, 2) subjekt a jeho kritická infrastruktura se nachází na území jednoho z členských států Evropské unie, a 3) případný incident by významně narušil poskytování jedné nebo více základních služeb ve stanovených odvětvích nebo poskytování jiných či závislých základních služeb.

Zatím co druhé a třetí kritérium jsou binární, pro posouzení prvního kritéria je nezbytné definovat základní služby pro jednotlivé sektory. K tomuto účelu je nutné vycházet z definice základní služby, která je směrnicí (Směrnice 2557, 2022) definována jako *„služba, která je zásadní pro zachování nejdůležitějších společenských funkcí, hospodářských činností, veřejného zdraví a bezpečnosti nebo životního prostředí“*. Definování kritérií pro vymezení základních služeb v jednotlivých sektorech je aktuálně úkolem každého členského státu. Příklad definování základních služeb poskytovaných v sektoru pozemní dopravy je následující (Rehak and Janeckova, 2024):

- provozování infrastruktury v TEN-T;
- provozování služeb souvisejících s přepravou osob a nákladu v TEN-T;
- provozování inteligentních dopravních systémů v TEN-T.

Vlastníkům a provozovatelům infrastruktur, kteří budou od roku 2026 určováni jako kritické subjekty, vzniká následně povinnost 1) provádět vlastní posouzení rizik s cílem určit rizika, která by mohla narušit jejich schopnost poskytovat základní služby, 2) přijmout technická, bezpečnostní a organizační opatření ke zvýšení své resilience, a 3) oznámit významné incidenty vnitrostátním orgánům (Směrnice 2557, 2022).

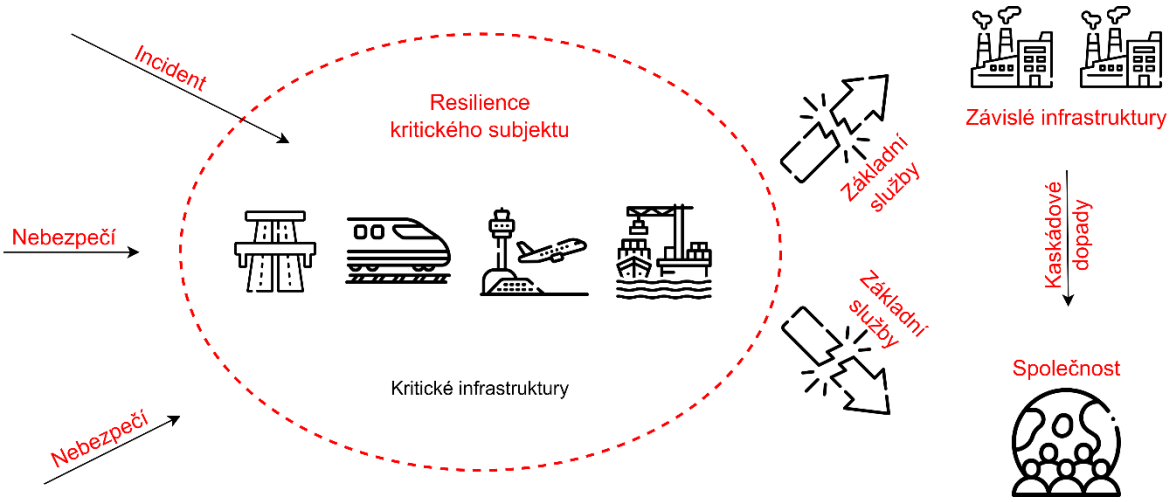
V kontextu tohoto článku je nutné věnovat pozornost zejména druhému bodu, který ukládá kritickým subjektům povinnost přijmout opatření ke zvýšení své resilience. Podstatou této povinnosti je znalost současného stavu resilience kritických subjektů vůči incidentům. Výsledky posouzení resilience následně umožní kritickým subjektům identifikovat slabá místa, na základě kterých je možné definovat adekvátní technická, bezpečnostní a organizační opatření.

2.2 Incidenty a jejich dopady na kritické subjekty

Kritické subjekty jsou po celou dobu své činnosti neustále vystavovány nebezpečí z vnějšího a vnitřního prostředí. Tato nebezpečí mohou být obecně klasifikována na naturogenní a antropogenní (UNDRR, 2015). V důsledku působení těchto nebezpečí může docházet ke vzniku incidentů, které jsou definovány jako *„události, které mohou významně narušit nebo které narušují poskytování základních služeb, včetně případů, kdy ovlivňují vnitrostátní systémy chránící právní stát“* (Směrnice 2557, 2022). Dopady incidentů dosahují většinou nízké až střední úrovně. Z tohoto důvodu je možné u kritických subjektů zajistit dostačující úroveň resilience vůči těmto událostem. Jedná se zejména o jejich připravenost, robustnost, obnovitelnost a adaptabilitu (Rehak et al., 2024b).

Obdobně jako v případě nebezpečí, také incidenty jsou klasifikovány na naturogenní a antropogenní (Shaluf, 2007). Naturogenní incidenty jsou nejčastěji důsledkem postupné změny klimatu a mezi nejvýznamnější v kontextu kritických subjektů patří zejména povodně, sesuvy půdy, bouře a lesní požáry (Fraser et al., 2020). Oproti tomu antropogenní incidenty jsou důsledkem úmyslného a/nebo neúmyslného jednání a mezi nejvýznamnější v kontextu kritických subjektů patří požáry, strukturální narušení staveb, závažné nehody, technologické katastrofy a teroristické útoky (Allen et al., 2017).

Dopady těchto incidentů působí primárně na kritické subjekty a jejich infrastruktury. V důsledku tohoto negativního působení může docházet k narušení poskytování základních služeb, což může mít za následek eskalaci kaskádních dopadů nejen na dependentní kritické infrastruktury, ale také na společnost jako celek, tj. ekonomické a společenské činnosti, životní prostředí, veřejnou bezpečnost a bezpečnost obecně nebo na zdraví obyvatelstva (Směrnice 2557, 2022). Avšak tyto dopady mohou být naopak tlumeny resiliencí kritických subjektů, a to prostřednictvím faktorů organizační a technické resilience. Vztah souvislostí uvedených v této části metodiky je prezentován na Obrázku 2.

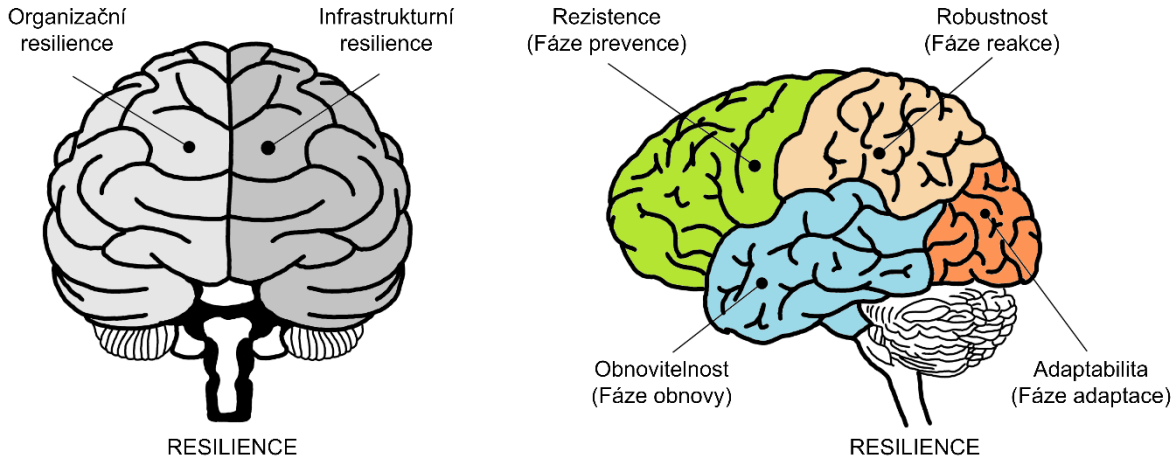


Obrázek 2: Vliv incidentů na kritické subjekty, jejich kritické infrastruktury a společnost

Z výše uvedeného je patrné, že incidenty významně narušují schopnost kritických subjektů poskytovat základní služby. Z tohoto důvodu je v navazujícím textu věnována pozornost faktorům determinujícím resilienci kritických subjektů.

2.3 Faktory determinující resilienci kritických subjektů

V kontextu kritických subjektů je resilience definována jako *„schopnost kritického subjektu předcházet incidentům, chránit se před těmito incidenty, reagovat na ně, odolávat jim, zmírňovat a absorbovat je, přizpůsobovat se jim a zotavit se z nich“* (Směrnice 2557, 2022). Na základě této definice je nutné vnímat resilienci kritických subjektů širokospektrálně, tzn. ve více rovinách. Takto vnímaná resilience může být z hlediska jednotlivých funkcí přirovnána k lidskému mozku (viz Obrázek 3).



Obrázek 3: Vnímání resilience kritických subjektů

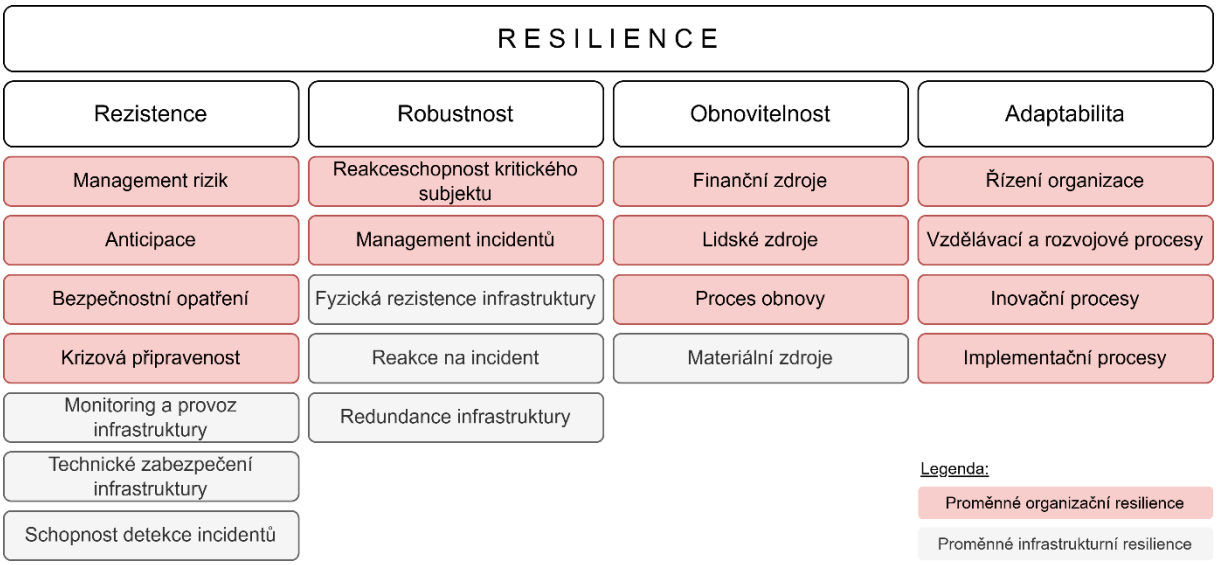
Obdobně jako je lidský mozek členěn na hemisféry a laloky, také resilienci je možné členit na sféry a komponenty. Toto přirovnání je nutné vnímat z funkčního (nikoli medicinského) hlediska. V tomto kontextu je resilience kritických subjektů determinována dvěma sférami, kdy jedna sféra je zodpovědná za organizační resilienci a druhá sféra za infrastrukturní resilienci. Současně v obou sférách je resilience kritických subjektů determinována čtyřmi komponentami (tj. rezistence, robustnost, obnovitelnost, adaptabilita), které pokrývají jednotlivé fáze krizového managementu, tj. prevence, reakce, obnova a adaptace kritických subjektů na incidenty.

Organizační resilience může být definována jako schopnost kritických subjektů předvídat, připravit se, reagovat, zotavit se a adaptovat se na vznik, působení a dopady incidentů, a to zejména v oblasti procesů a zdrojů organizace. Oproti tomu **infrastrukturní resilience** může být definována jako schopnost kritických subjektů monitorovat, detekovat a absorbovat dopady incidentů na jejich infrastruktury, jakož i schopnost kritických subjektů zotavit tyto infrastruktury z těchto dopadů.

V následující části metodiky je věnována pozornost definování faktorů determinujících jak organizační, tak infrastrukturní resilienci kritických subjektů. Na základní úrovni jsou organizační i infrastrukturní resilience determinovány čtyřmi základními komponentami (Mentges et al., 2023; Rehak et al., 2024a):

- rezistence, jejíž podstatou je zabránit vzniku incidentů;
- robustnost, jejíž podstatou je absorbovat dopady incidentů;
- obnovitelnost, jejíž podstatou je obnova funkce a resilience kritického subjektu;
- adaptabilita, jejíž podstatou je adaptace kritického subjektu na již proběhlé incidenty.

V rámci podrobnějšího členění je každá komponenta dále klasifikována na sekundární a terciární faktory, tj. proměnné a jejich měřitelné položky. Klasifikace sekundárních faktorů je prezentována na Obrázku 4.

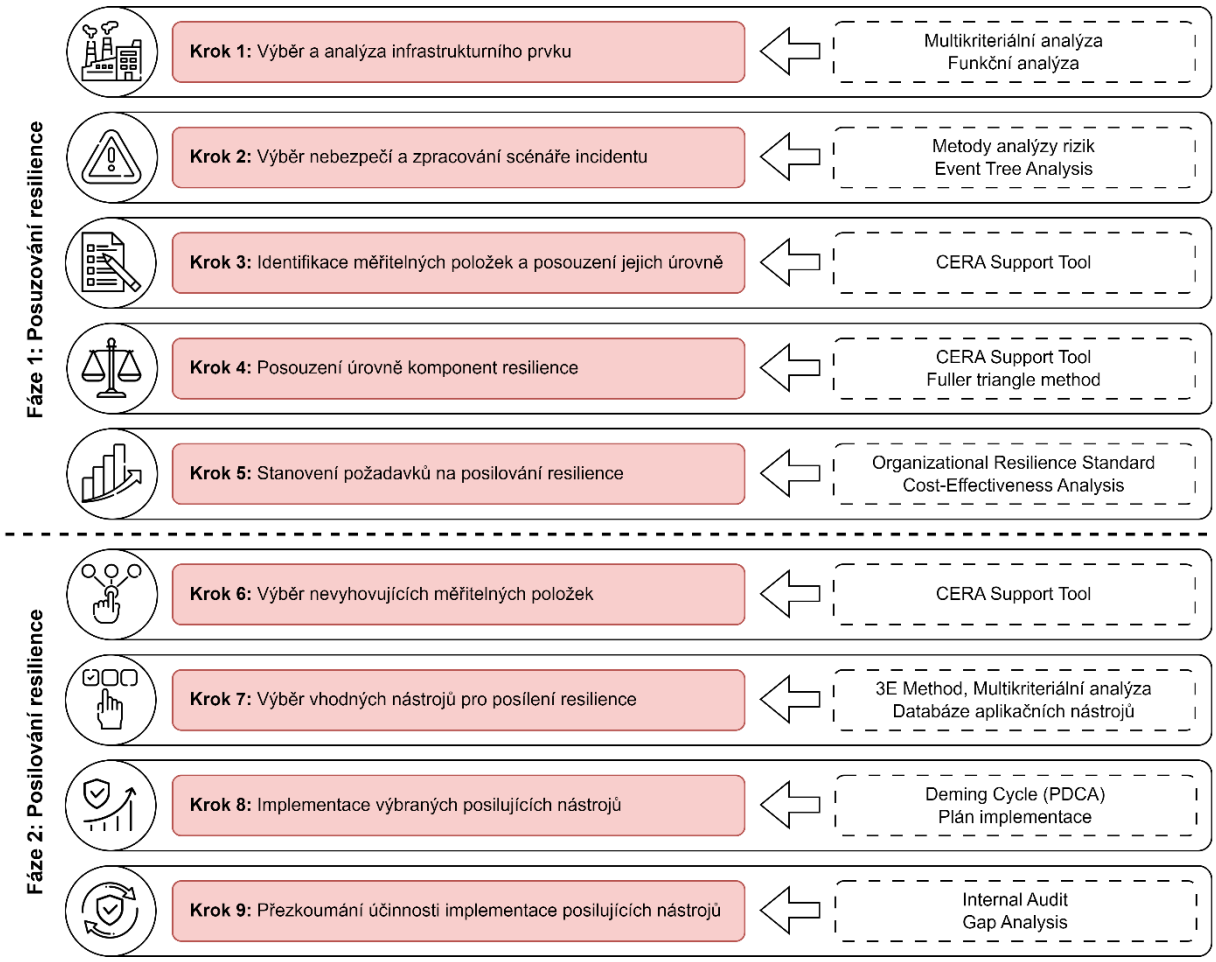


Obrázek 4: Klasifikace komponent a proměnných determinujících resilienci kritických subjektů

Podrobná deskripce sekundárních a terciárních faktorů, které jsou nezbytné pro posuzování resilience kritických subjektů vůči incidentům, je prezentována v Přílohách A-D. Koncepce těchto faktorů umožňuje posouzení resilience kritických subjektů na všech třech úrovních managementu organizace, tj. strategické, operační i taktické.

3 Postup posuzování a posilování resilience kritických subjektů vůči incidentům

Aby mohly kritické subjekty v souladu se směrnicí (Směrnice 2557, 2022) přijmout technická, bezpečnostní a organizační opatření ke zvýšení své resilience, je nezbytné nejprve u každého kritického subjektu provést posouzení této resilience a na základě výsledků provést její posílení. Za tímto účelem byl vytvořen postup posuzování a posilování resilience kritických subjektů vůči incidentům (viz Obrázek 5). Tento postup je určen výhradně pro posuzování vnitřní resilience kritických subjektů, z tohoto důvodu nezohledňuje vnější faktory ovlivňující resilienci. Jeho podstatou je semi-kvantitativní posouzení a posílení faktorů resilience, které byly definovány pro jednotlivé komponenty resilience, tj. rezistence, robustnost, obnovitelnost a adaptabilita.



Obrázek 5: Postup posuzování a posilování resilience kritických subjektů vůči incidentům

Krok 1: Výběr a analýza infrastrukturního prvku

Podstatou tohoto kroku je identifikace konkrétního infrastrukturního prvku, který je provozován kritickým subjektem, a následná analýza jeho strukturálních a topologických parametrů.

Krok 2: Výběr nebezpečí a zpracování scénáře incidentu

Podstatou tohoto kroku je analýza rizik, která umožní identifikaci konkrétního nebezpečí s vysokou mírou rizika, jež může vyústit v incident. Na základě výběru konkrétního nebezpečí je zpracován scénář předpokládaného průběhu incidentu, tj. působení vybraného nebezpečí na vybraný infrastrukturní prvek.

Krok 3: Identifikace měřitelných položek a posouzení jejich úrovně

Podstatou tohoto kroku je rozpoznání měřitelných položek, tj. faktorů resilience, které kritický subjekt aktivně využívá. U těchto položek se následně hodnotí míra jejich naplňování, tedy do jaké míry jsou dané činnosti a opatření skutečně realizovány.

Krok 4: Posouzení úrovně komponent resilience

Podstatou tohoto kroku je komplexní posouzení resilience kritického subjektu na úrovni jednotlivých komponent, které tak poskytují informaci o celkovém stavu měřitelných položek v jednotlivých oblastech resilience kritického subjektu.

Krok 5: Stanovení požadavků na posilování resilience

Podstatou tohoto kroku je formulace požadavků na posílení úrovně příslušných měřitelných položek. Jedná se o takové položky, které vykazují nízkou, nedostatečnou nebo kritickou úroveň naplňování. Tento pátý krok představuje závěrečnou fázi posuzování resilience kritických subjektů.

Krok 6: Výběr nevyhovujících měřitelných položek

Podstatou tohoto kroku je výběr měřitelných položek, které nebyly zahrnuty do posuzování nebo naplňují požadavky na posílení resilience definované v předchozím kroku.

Krok 7: Výběr vhodných nástrojů pro posílení resilience

Podstatou tohoto kroku je výběr aplikačních nástrojů, které jsou vhodné k posílení resilience dotčených měřitelných položek.

Krok 8: Implementace vybraných posilujících nástrojů

Podstatou tohoto kroku je zajištění praktického uplatnění vybraných nástrojů, tedy jejich efektivní implementace.

Krok 9: Přezkoumání účinnosti implementace posilujících nástrojů

Podstatou tohoto kroku je opětovné posouzení resilience měřitelných položek. Na základě komparace těchto výsledků s původními hodnotami resilience je možné vyhodnotit, do jaké míry byly implementované nástroje skutečně účinné.

V následující části metodiky je provedena podrobná deskripce výše uvedených kroků postupu posuzování a posilování resilience kritických subjektů vůči incidentům. Praktická aplikace tohoto postupu je demonstrována na příkladu posuzování a posilování resilience provozovatele silniční infrastruktury TEN-T vůči teroristickému útoku amonledkovou trhavinou na mostní objekt. V tomto kontextu je nutné zdůraznit, že posouzení a posilování resilience kritických subjektů musí být realizováno vždy pouze pro jeden infrastrukturní prvek (tj. infrastrukturní resilience) jednoho kritického subjektu (tj. organizační resilience) vůči jednomu konkrétnímu incidentu.

3.1 Fáze 1: Posuzování resilience kritických subjektů vůči incidentům

První fází postupu je posuzování resilience kritických subjektů vůči incidentům. Tato fáze zahrnuje pět kroků a je zakončena stanovením požadavků na posilování resilience.

3.1.1 Krok 1: Výběr a analýza infrastrukturního prvku

Podstatou tohoto kroku je výběr konkrétního infrastrukturního prvku, který je kritickým subjektem provozován. Výběr tohoto prvku je vhodné realizovat s využitím Multikriteriální analýzy (Figueira et al., 2005) nebo Funkční analýzy (Dozier et al., 2022). U takto vybraného prvku je následně nutné provést jeho kategorizaci (tj. zařazení do příslušného sektoru a subsektoru) a analýzu topologických a strukturálních parametrů.

Podstatou **topologické analýzy** je kategorizace prvku podle jeho topologické struktury (Rehak et al., 2020; Fekete, 2018):

- liniové prvky – zajišťují přenos, dodávku nebo přepravu komodit mezi dvěma fyzicky oddělenými místy (např. silniční a železniční koridory). Jsou významově základní skupinou, která se nachází ve vztahu ke všem bodovým i plošným prvkům.
- bodové prvky – představují koncentrovaný a uzavřený celek umístěný na malé ploše, který plní svou funkci pro potřeby konkrétních liniových objektů (např. mosty, tunely).
- plošné prvky – představují jeden celek nebo integrální objekty, kde se vyskytují dva a více bodových prvků nebo dvě a více klíčových technologií (např. významné dopravní uzly).

Podstatou **strukturální analýzy** je technická specifikace prvku, která je založena na jeho stavebně-technických parametrech. Příklad analýzy vybraného prvku dopravní infrastruktury je prezentován na Obrázku 6.

Sektor / Subsektor		Doprava / Silniční infrastruktura
Topologická struktura		Bodový prvek
Druh infrastrukturního prvku		Mostní objekt
Lokalizace		Dálnice I. třídy
Stavebně-technické parametry	Normální zatížitelnost: Délka přemostění: Volná šířka: Druh spodní stavby: Materiál spodní stavby: Stavební stav spodní stavby: Druh nosné konstrukce: Převažující materiál nosné konstrukce: Stavební stav nosné konstrukce:	32 t 225 m 22,5 m pilíř členěný železobeton kategorie IV (uspokojivý) trám deskový spojitý železobeton kategorie III (dobrý)

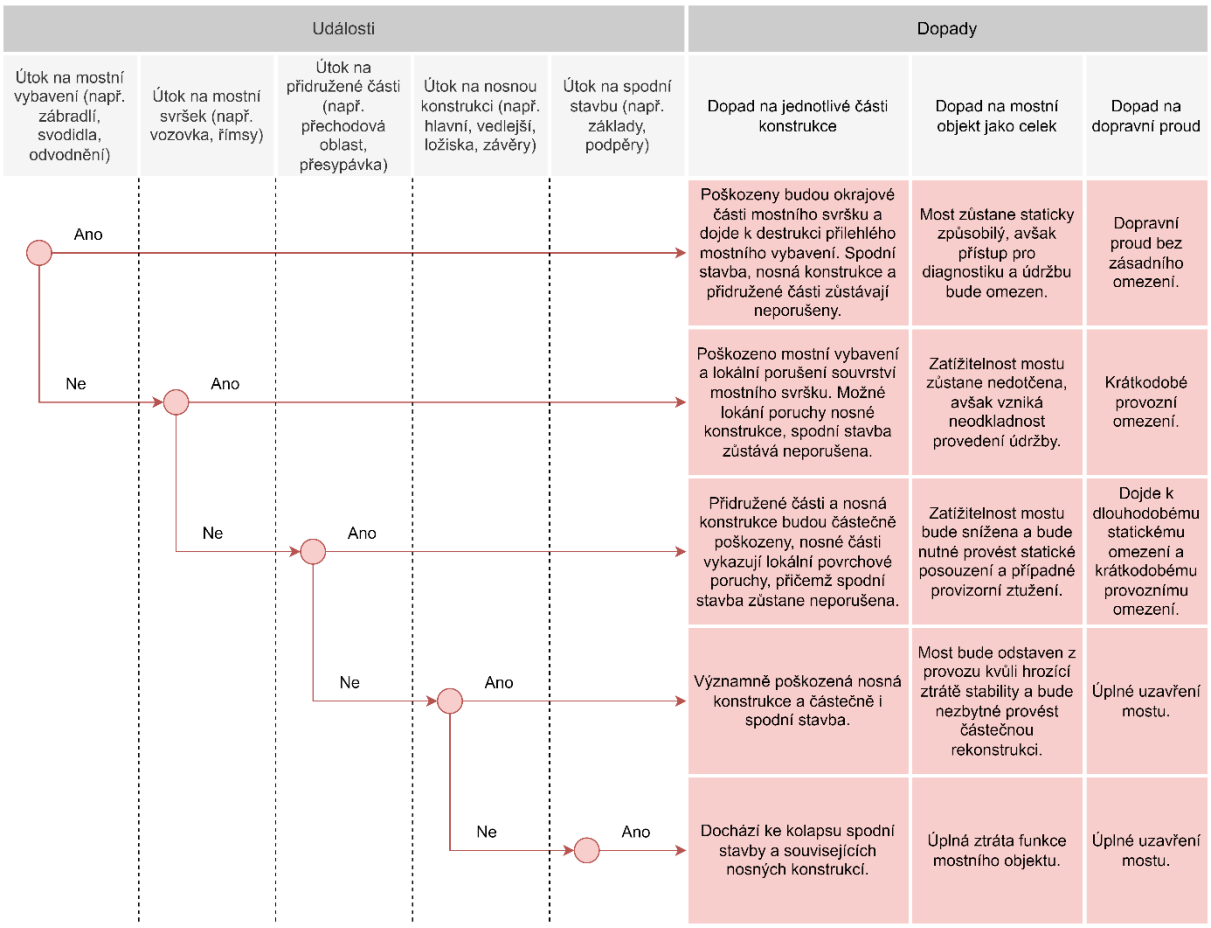
Obrázek 6: Příklad analýzy vybraného prvku dopravní infrastruktury (Zdroj: mostní list)

3.1.2 Krok 2: Výběr nebezpečí a zpracování scénáře incidentu

Jakmile je kritickým subjektem vybrán konkrétní infrastrukturní prvek, je nutné přistoupit k analýze rizik, na jejímž základě bude vybráno konkrétní nebezpečí s vysokou mírou rizika, které má potenciál zapříčinit incident. Analýzu rizik je vhodné realizovat s využitím některé z doporučovaných metod (IEC 31010, 2019). Na základě výběru konkrétního nebezpečí je možné

přistoupit ke zpracování **scénáře předpokládaného průběhu incidentu**, tj. působení vybraného nebezpečí na vybraný infrastrukturní prvek. K tomuto účelu je doporučována metoda Event Tree Analysis (IEC 62502, 2010), která umožňuje rozbor událostí a následků vedoucích ke vzniku incidentu.

Příklad zpracování scénáře incidentu za použití metody ETA je prezentován na Obrázku 7. Jedná se o teroristický útok 500 kg amonledkové trhaviny na různé části mostního objektu.



Obrázek 7: Příklad zpracování scénáře incidentu

3.1.3 Krok 3: Identifikace měřitelných položek a posouzení jejich úrovně

Podstatou tohoto kroku je identifikace měřitelných položek a posouzení úrovně jejich plnění kritickým subjektem u všech čtyř komponent resilience. K tomuto účelu je doporučován **CERA Support Tool** (viz Obrázek 8), který byl vytvořen na základě výsledků definování a klasifikace faktorů determinujících resilienci kritických subjektů (Rehak et al., 2024a). Česká verze tohoto nástroje je dostupná na webové stránce projektu STRENGTH: https://strength.vsb.cz/cera

ROBUSTNOST
KRITICKÉHO SUBJEKTU

CERA Support Tool

Roviny resilience	Proměnné	Měřitelné položky	Identifikace faktorů [ANO/NE]	Posouzení úrovně [1-5]
Subjektová resilience	Reakceschopnost kritického subjektu	Časový interval pro aktivaci ochranných opatření	Ano	3
		Stav sil a prostředků	Ano	5
	Management incidentů	Připravenost krizového managementu	Ano	4
		Komunikace a sdílení informací	Ano	2
Infrastrukturní resilience	Fyzická rezistence infrastruktury	Požární odolnost	Ano	4
		Seismická odolnost	Ano	2
		Výbuchová odolnost	Ano	3
	Reakce na incident	Redukce následků incidentu	Ano	2
		Udržení funkčnosti klíčových technologií	Ano	1
	Redundance infrastruktury	Kritérium spolehlivosti	Ano	3
		Dostupnost redundantní kapacity	Ano	4
		Dočasná substituce klíčových technologií	Ne	
Úroveň robustnosti				**53%**

Obrázek 8: Příklad identifikace měřitelných položek determinujících robustnost a posouzení jejich úrovně

Identifikace měřitelných položek spočívá ve výběru těch měřitelných položek, které jsou podle hodnotitele pro dané posouzení adekvátní, tzn. dané činnosti/opatření jsou kritickým subjektem realizovány. U těchto měřitelných položek je ve sloupci Identifikace faktorů vybrána odpověď ANO. U měřitelných položek, které nebyly hodnotitelem identifikovány je vybrána odpověď NE a v rámci posouzení úrovně získávají hodnotu nula.

U měřitelných položek, u kterých byla vybrána odpověď ANO, je následně nutné **posoudit na jaké úrovni kritický subjekt splňuje činnosti/opatření definované těmito měřitelnými položkami**. Tato úroveň je vyjádřena bodovou hodnotou od 1 do 5, kde přidělené body mají následující význam:

- **1:** Kritický subjekt nesplňuje žádné činnosti/opatření definované měřitelnou položkou.
- **2:** Kritický subjekt splňuje pouze minimální rozsah činností/opatření definovaných měřitelnou položkou (cca 25 %).
- **3:** Kritický subjekt splňuje činnosti/opatření definované měřitelnou položkou pouze částečně (cca 50 %).
- **4:** Kritický subjekt splňuje většinu činnosti/opatření definované měřitelnou položkou (cca 75 %).
- **5:** Kritický subjekt zcela splňuje činnosti/opatření definované měřitelnou položkou.

Identifikace měřitelných položek a posouzení jejich úrovně by mělo být primárně realizováno styčným bezpečnostním zaměstnancem ve spolupráci s odpovědnými manažery dotčených infrastruktur a procesů. Avšak, do procesu posuzování by měly být zapojeni také externí činitelé, kteří jsou závislí na dodávkách základních služeb od daného kritického subjektu. Tímto způsobem bude částečně potlačena subjektivita hodnocení. Současně je však nutné podotknout, že použití takových přístupů v managementu není neobvyklé (Grabinski, 2007). Takovýto způsob hodnocení umožňuje tuto subjektivitu transparentně shromáždit na jednom místě a přiznat.

3.1.4 Krok 4: Posouzení úrovně komponent resilience

V návaznosti na identifikaci měřitelných položek a posouzení jejich úrovně (viz Krok 3) je možné přistoupit k posouzení úrovně jednotlivých komponent. Za tímto účelem byly stanoveny normalizované váhy pro jednotlivé měřitelné položky (viz Příloha E-H). Tyto váhové koeficienty

reflektují nejen významnost měřitelných položek, ale také proměnných, které jsou těmito měřitelnými položkami determinovány. **Stanovení váhových koeficientů** bylo provedeno dvojfázově s využitím metod vícekriteriálního hodnocení, konkrétně Metfessel's allocation (Metfessel, 1947) a Fuller's triangle (Fishburn, 1971). Podrobný popis stanovení váhových koeficientů byl prezentován v odborné publikaci (Rehak et al., 2024a).

Posouzení úrovně resilience kritického subjektu prostřednictvím jednotlivých komponent je následně vypočteno váženým průměrem jednotlivých měřitelných položek, viz vzorec (1).

$$C_i = 20 \sum_{j=1}^{k} P_j w_j \tag{1}$$

kde C_i = i-tá komponenta resilience kritického subjektu [%]; P_j = j-tá měřitelná položka resilience kritického subjektu [počet bodů]; w_j = j-tá normalizovaná váha j-té měřitelné položky resilience kritického subjektu v intervalu $\langle 0;1 \rangle$; k = celkový počet měřitelných položek v i-té komponentě.

K výpočtu úrovně resilience pro jednotlivé komponenty je doporučován CERA Support Tool, který tuto hodnotu zobrazuje ve spodní části formuláře (viz Obrázek 8).

V závěru posouzení je nutné provést vyhodnocení dosažených úrovní jednotlivých komponent. Tyto výsledné úrovně je nutné zaškálovat do jedné z pěti **kategorií, které vyjadřují úrovně přijatelnosti resilience**. Rozdělení těchto úrovní filozoficky vychází z metody FMECA (IEC 60812, 2018), která při stanovování míry rizika pracuje s pěti bodovou škálou. Variací extrémních hodnot této škály (tj. největší a nejmenší hodnoty souboru, tj. 1 a 5 bodů) jsou stanoveny kategorie úrovní přijatelnosti komponent resilience (viz Obrázek 9).

Obrázek 9: Kategorie úrovní přijatelnosti komponent resilience

U komponent, které byly kategorizovány jako úroveň nízká, nedostačující či kritická, je nutné provést zpětný rozbor jejich měřitelných položek a stanovit požadavky na posilování resilience.

3.1.5 Krok 5: Stanovení požadavků na posilování resilience

Po výběru komponent s nízkou, nedostačující či kritickou úrovní resilience je nutné přejít ke stanovení požadavků na posilování resilience měřitelných položek determinujících tyto komponenty. Požadavky na posilování resilience měřitelných položek vyplývají z výsledků posouzení jejich stávajícího stavu a jsou definovány v kontextu Organizational Resilience Standard (ASIS, 2009):

- **u měřitelných položek s hodnotou 1 nebo 2** je nutné provést posílení resilience prostřednictvím vhodných nástrojů. Tyto nástroje jsou definovány v databázi aplikačních nástrojů pro posilování resilience kritických subjektů, která je dostupná na webové stránce projektu STRENGTH: https://strength.vsb.cz/databaze
- **u měřitelných položek s hodnotou 3 nebo 4** je vhodné provést posílení resilience prostřednictvím vhodných nástrojů, avšak na základě výsledků analýzy efektivnosti nákladů (Levin and McEwan, 2000).
- **u měřitelných položek s hodnotou 5** v současné době není nutné posilovat jejich resilienci.

Pátým krokem je ukončen postup posuzování resilience kritických subjektů vůči incidentům. Tento postup je vhodné opakovat v případě, že došlo k posílení resilience některých měřitelných položek nebo uplynula doba vyžadující cyklické posouzení resilience, tj. jeden rok.

3.2 Fáze 2: Posilování resilience kritických subjektů vůči incidentům

Druhou fází postupu je posilování resilience kritických subjektů vůči incidentům. Tato fáze zahrnuje čtyři kroky a je zakončena přezkoumáním účinnosti implementace posilujících nástrojů.

3.2.1 Krok 6: Výběr nevyhovujících měřitelných položek

Výběr nevyhovujících měřitelných položek by měl být realizován v kontextu požadavků na posilování resilience (viz Krok 5). Na základě těchto požadavků by měla být věnována pozornost všem **měřitelným položkám, které nebyly v rámci identifikace měřitelných položek a posouzení jejich úrovně (viz Krok 3) zahrnuty do posuzování**. U těchto měřitelných položek by měla být zjištěna příčina jejich nezahrnutí a je-li možné provést nápravné opatření implementací některého z posilujících nástrojů, pak je možné přejít k následujícímu kroku (viz Krok 7). Obdobný postup by měl být aplikován také v případě **měřitelných položek, jejichž úroveň resilience byla posouzena hodnotou 1 nebo 2**.

K tomuto účelu je doporučováno využít výsledky identifikace měřitelných položek a posouzení jejich úrovně (viz Obrázek 8), kterých bylo dosaženo v rámci Kroku 3 prostřednictvím CERA Support Tool: https://strength.vsb.cz/cera

3.2.2 Krok 7: Výběr vhodných nástrojů pro posílení resilience

V okamžiku, kdy jsou hodnotitelem vybrány konkrétní měřitelné položky, u kterých je požadováno posílení jejich resilience, je možné přejít k výběru vhodných aplikačních nástrojů. Podrobná deskripce všech nástrojů byla prezentována v odborné publikaci (Rehak et al., 2025). Komplexní **databáze aplikačních nástrojů** pro posilování resilience kritických subjektů je dostupná na webové stránce projektu STRENGTH: https://strength.vsb.cz/databaze

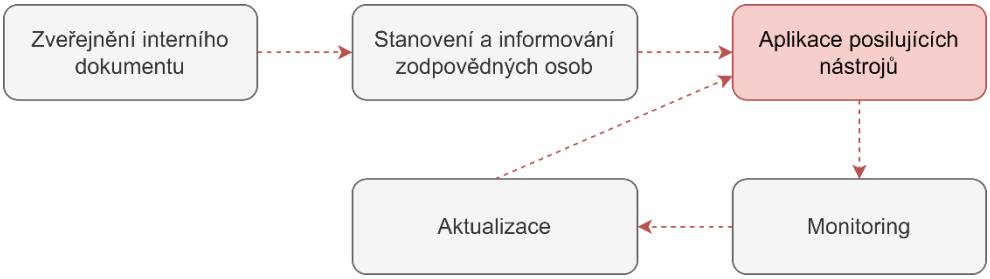
K výběru vhodných nástrojů z této databáze je doporučována primárně metoda 3E (Liu et al., 2010), kde jsou jednoznačně **stanovena kritéria, tj. hospodárnost, efektivnost, účelnost**. Pokud hodnotiteli tato kritéria nevyhovují, může použít Multikriteriální analýzu (Figueira et al., 2005), kde si stanoví vlastní kritéria.

V případě aplikace metody 3E jsou nástroje pro posilování resilience vybraných měřitelných položek posuzovány z hlediska jejich hospodárnosti, efektivnosti a účelnosti. Hospodárnost zohledňuje minimalizaci nákladů na zdroje kritického subjektu (tj. finanční, lidské, věcné) při dodržení požadované kvality zdrojů a očekávaného výsledku, tj. posílení resilience měřitelné

položky na požadovanou úroveň. Efektivnost zohledňuje optimalizaci využití zdrojů k dosažení očekávaného výsledku. Oproti tomu účelnost zohledňuje maximalizaci úrovně dosaženého výsledku při alokaci zdrojů shodné kvantity a kvality.

3.2.3 Krok 8: Implementace vybraných posilujících nástrojů

Jakmile jsou vybrány vhodné nástroje pro posílení resilience měřitelných položek, je nutné provést jejich implementaci. Proces implementace by měl v obecné rovině naplňovat podstatu Demingova cyklu (Swamidass, 2000). Za tímto účelem je vhodné zpracovat **plán implementace**, který by měl zahrnovat soubor činností, jejichž cílem je efektivně a systematicky aplikovat vybrané nástroje v požadované době (viz Obrázek 10).



Obrázek 10: Proces implementace nástrojů pro posílení resilience měřitelných položek (vytvořeno podle Blumenthal and Stoddard, 1999)

Prvním krokem procesu implementace posilujících nástrojů je zveřejnění interního dokumentu (zásada, předpis, nařízení), který bude obsahovat veškeré informace nezbytné k implementaci nástrojů do procesů a zdrojů kritického subjektu. Dále je nutné stanovit a informovat kompetentní osoby o změnách, které budou provedeny. Následně může být zahájena fáze samotné aplikace posilujících nástrojů, která bude průběžně monitorována a v případě zjištění nedostatků bude přizpůsobena aktuálním podmínkám. Pokud v průběhu implementačního procesu dojde k aktualizaci podmínek, je nutné revidovat a opětovně realizovat fázi aplikace posilujících nástrojů.

3.2.4 Krok 9: Přezkoumání účinnosti implementace posilujících nástrojů

Posledním krokem postupu posilování resilience je přezkoumání účinnosti implementace posilujících nástrojů. Vyhodnocení jejich účinnosti může být provedeno na základě výsledků interního auditu (ISO 22301:2019) kritického subjektu. Pro detailnější přezkoumání účinnosti je vhodné na základě výsledků interního auditu následně provést aplikaci metody Gap Analysis (Blokdyk, 2017). Podstatou této metody je **komparace požadované/plánované úrovně resilience kritického subjektu se skutečným stavem**.

Výsledkem přezkoumání účinnosti implementace posilujících nástrojů může být např. komparační tabulka, která poskytuje celkový obraz o naplnění očekávaného přínosu. Jestliže tato očekávání nejsou naplněna, stává se postup posilování resilience kritického subjektu nedostačujícím. V takovémto případě je vhodné opětovně provést posouzení úrovně komponent resilience (viz Krok 4), identifikovat měřitelné položky s nedostačující úrovní resilience (viz Krok 5) a opakovat postup posilování resilience kritického subjektu (viz Kroky 6-9). Tímto krokem se celý postup posilování resilience kritického subjektu vůči incidentu uzavírá.

4 Závěr

Metodický postup prezentovaný v tomto dokumentu umožňuje kritickým subjektům v sektoru dopravy posuzování a posilování jejich vnitřní resilience vůči incidentům. Sekundárně může být tento postup využit také pro kritické subjekty ostatních technicky orientovaných infrastruktur. Terciárně může být využit také pro kritické subjekty vlastnící či provozující socio-ekonomické infrastruktury, avšak v tomto případě je nutné nejprve provést revizi jednotlivých faktorů resilience a v případě potřeby provést jejich redefinování do socio-ekonomického kontextu.

Novost tohoto postupu spočívá zejména v jeho schopnosti posoudit aktuální stav vnitřní resilience kritického subjektu a na základě výsledků posouzení doporučit vhodné nástroje k posílení této resilience. Stávající postupy jsou totiž orientovány primárně na posuzování resilience kritických infrastruktur a nezohledňují procesy a zdroje organizace. V současné době neexistuje ucelený postup ani aplikační nástroje pro posilování resilience subjektů pozemní dopravní kritické infrastruktury.

Metodický postup poskytuje kritickým subjektům informace vedoucí k posílení jejich resilience vůči nežádoucím incidentům. Jedná se o opatření preventivního charakteru, která zabraňují vzniku těchto incidentů a v případě jejich vzniku minimalizují negativní dopady na funkci kritického subjektu, tj. poskytování základních služeb. V důsledku těchto opatření dochází k minimalizaci nákladů na odstraňování následků způsobených případným vznikem potenciálně negativních incidentů.

Přílohy

Příloha A: Faktory determinující rezistenci kritických subjektů

Sféry resilience	Proměnné	Deskripce proměnných	Měřitelné položky
Organizační resilience	Management rizik	Soubor procesů pro včasné posouzení a zvládání rizik, včetně specifikace scénářů incidentů.	Úroveň managementu rizik
			Metodologie posuzování rizik
			Implementace bezpečnostních norem
			Modelování incidentů
	Anticipace	Soubor organizačních opatření a postupů pro predikci vzniku incidentu v důsledku působení nebezpečí.	Preventivní kontrola
			Indikování narušení resilience kritického subjektu
	Bezpečnostní opatření	Soubor organizačních a režimových opatření pro monitoring a fyzickou/kybernetickou ochranu infrastruktury.	Fyzická ostraha
			Režimová opatření
	Krizová připravenost	Soubor analyticko-plánovacích podkladů ke zvýšení připravenosti kritického subjektu na incidenty a plnění navazujících bezpečnostních opatření.	Odpovědnosti, povinnosti a pravomoci
			Školení a výcvik pracovníků
			Bezpečnostní plánování a dokumentování
			Plánování kontinuity
Infrastrukturní resilience	Monitoring a provoz infrastruktury	Soubor technických opatření pro monitoring technického stavu zařízení, jeho údržby, servisu a testování.	Technický stav infrastruktury
			Údržba, servis a testování zařízení
	Technické zabezpečení infrastruktury	Soubor technických opatření pro monitoring a fyzickou/kybernetickou ochranu infrastruktury.	Mechanické zábranné prostředky
			Elektronické sledovací a poplachové prostředky
			Kybernetická bezpečnost
	Schopnost detekce incidentů	Soubor technických opatření pro monitoring infrastruktury za účelem včasné detekce poruch a detekce vzniku incidentu.	Monitoring prostředí
			Detekce vzniku incidentu

Úroveň managementu rizik spočívá v posouzení úrovně koordinovanosti činností pro vedení a řízení rizik s cílem zvýšit resilienci organizace (ISO/TS 31050, 2023). Pozornost je věnována zejména úrovni implementace a realizace strategie managementu rizik, analýzy rizik, zvládání rizik, monitorování rizik a optimalizace managementu rizik.

Metodologie posuzování rizik spočívá v posouzení úrovně aplikované metodologie posuzování rizik (IEC 31010, 2019). Vzhledem k tomu, že existuje řada metodologií umožňujících realizovat analýzu rizika s různými cíli, je posuzování metodologie z velká části založeno na základním cíli analýzy (pro účely tohoto hodnocení), tj. hodnocení toho, nakolik použitá metodologie umožňuje chápat rizika vedoucí k výraznému omezení nebo přerušení poskytování služeb aktiva.

Implementace bezpečnostních norem spočívá v posouzení úrovně zavedení bezpečnostních norem v organizaci. Mezi stěžejní oblasti patří management rizik (ISO 31000, 2018), bezpečnost

informací (ISO/IEC 27001, 2022) a bezpečnost a ochrana zdraví (ISO 45001, 2018). Vedle stěžejních bezpečnostních norem mohou být implementovány také normy z dalších specifických bezpečnostně orientovaných oblastí, např. bezpečnost strojních zařízení (ISO 12100, 2010).

Modelování incidentů spočívá v posouzení úrovně zpracování scénářů incidentů pro identifikovaná rizika. Tyto scénáře mohou být zpracovány buď na úrovni základní nebo detailní. Podstatou základní úrovně zpracovaných scénářů je kvalitativní nebo semikvantitativní posouzení vývoje incidentu. Tyto scénáře jsou zpracovávány s použitím jednodušších metod (Iturriza et al., 2018) a určeny např. jako vstup do dalších analýz nebo jako podklad pro porozumění problému. Podstatou detailní úrovně zpracovaných scénářů je vícevariantní kvantitativní posouzení pravděpodobnosti a závažnosti dopadů incidentu. Tyto scénáře jsou zpracovány s použitím složitějších metod hodnocení, jsou založeny na kvantitativních datech a jsou zpětně testovány. V současné době jsou k tomuto účelu stále více využívána tzv. digitální dvojčata (Brucherseifer et al., 2021).

Preventivní kontrola by měla být prováděna manažery kritického subjektu na všech úrovních řízení. Podstatou preventivní kontroly je získání zpětné vazby o aktuálním stavu infrastruktur, výrobních a bezpečnostních procesů a znalostí a dovedností zaměstnanců (Denyer, 2017).

Indikování narušení resilience kritického subjektu spočívá ve využívání metod a nástrojů zaměřených na prediktivní indikaci potenciálního narušení organizační i infrastrukturní resilience (Yang et al., 2023; Splichalova et al., 2020).

Fyzická ostraha je soubor bezpečnostních služeb vykonávaných bezpečnostními pracovníky za účelem ochrany infrastruktury (EN 15602, 2022). *Režimová opatření* je možné členit na fyzická a kybernetická. V oblasti fyzické ochrany se jedná o soubor bezpečnostních opatření, která zabezpečují převážně vstup a vjezd do prostoru infrastruktury, jakož i pohyb osob a prostředků v těchto prostorách (Lovecek and Reitspis, 2011). V oblasti kybernetické ochrany se jedná o soubor bezpečnostních opatření pro systematickou ochranu elektronických či tištěných dat kritického subjektu, např. systémy managementu bezpečnosti informací (ISO/IEC 27001, 2022).

Odpovědnosti, povinnosti a pravomoci spočívají v posouzení míry definování odpovědností, povinností, pravomocí a rolí při řešení incidentů a krizových situací (ISO 9001, 2015).

Školení a výcvik pracovníků spočívá v posouzení rozsahu školení, úrovně výcviku a udržování praktických dovedností pracovníků k řešení incidentů a krizových situací. Za tímto účelem by měly být managementem kritického subjektu realizovány činnosti v oblasti bezpečnosti a ochrany zdraví při práci, požární ochrany, informačních technologií a u technického personálu praktický nácvik zvládání incidentů a krizových situací (ISO 9001, 2015).

Bezpečnostní plánování a dokumentování spočívá v posouzení úrovně zpracování bezpečnostní dokumentace, zejména havarijního plánu a plánu krizové připravenosti kritického subjektu (Philpott, 2016).

Plánování kontinuity spočívá v posouzení způsobilosti organizace pokračovat v poskytování základní služby, v přijatelném časovém rámci a v předdefinovaném objemu, během incidentu. Jedná se především o nastavení politiky kontinuity, stanovení cílů kontinuity na relevantních funkcích a úrovních, plánování, implementování a řízení procesů zajišťujících základní službu či stanovení pokynů a informací pro reakci na incident (ISO 22301, 2019).

Technický stav infrastruktury spočívá v posouzení způsobilosti zařízení k bezpečnému provozu z pohledu jeho technického stavu (ISO 12100, 2010). Jedná se zejména o ověřování aktuálního technického stavu zařízení podle průvodní dokumentace, popřípadě místního provozního

bezpečnostního předpisu, zda je zařízení stále schopno plnit svůj účel a zda jeho stav, popřípadě provoz neohrožuje bezpečnost práce a provozu.

Údržba, servis a testování zařízení spočívá v realizaci kontrol technického stavu infrastruktury, její funkce a poskytovaných služeb (Tracht et al., 2013). Na základě výsledků technické kontroly zařízení je vhodné provádět požadovanou údržbu a servis. Rovněž je vhodné provádět testování zařízení formou pravidelných funkčních a zátěžových testů.

Mechanické zábranné prostředky zahrnují zejména oplocení (tj. ochrana perimetru prvku), mříže, rolety nebo zámky (tj. ochrana pláště prvku) v takovém rozsahu a s takovými technickými parametry, aby vytvořily systém zábran, které budou svou konstrukcí a mechanickou odolností splňovat bezpečnostní funkce stanovené technickými normami (Vidrikova et al., 2017).

Elektronické sledovací a poplachové prostředky zahrnují zejména kamerové a přístupové systémy, elektrickou požární signalizaci, poplachové zabezpečovací a tísňové systémy, zařízení pro detekci nebezpečných plynů a par, zařízení omezující rozsah úniku nebezpečných látek, zvláštní technická opatření proti neoprávněné manipulaci nebo systém rychlé odstávky objektu nebo zařízení v takovém rozsahu, aby byla vytvořena ochrana osob a infrastruktury, která umožní včasný a účinný zákrok v narušeném objektu nebo zařízení (např. EN 50398-1, 2017).

Kybernetická bezpečnost představuje soubor opatření k ochraně počítačových systémů a sítí kritického subjektu před neoprávněným přístupem a před počítačovou kriminalitou, tj. narušením, krádeží či zneužitím poskytovaných služeb nebo poškozením hardwaru, softwaru nebo elektronických údajů (Regulation 881, 2019).

Monitoring prostředí představuje soubor metod, měření a nástrojů (aktivní/pasivní monitoring), včetně vizuálního sledování, který zjišťuje aktuální stav událostí v blízkosti jednotlivých infrastruktur, tj. určení stavu jejich systémů, procesů a činností (Novotny et al., 2021). Zároveň zajišťují systematický sběr informací v určitém čase, a to za účelem předcházení incidentů, získávání obecného přehledu a tvorbě statistik o aktuálním stavu jednotlivých infrastruktur a jejich prostředí.

Detekce vzniku incidentu zahrnuje soubor technických opatření a nástrojů pro včasné rozpoznání nadcházejícího incidentu (např. ElSahly and Abdelfatah, 2022). Jedná se např. o senzory, detektory, alarmy, softwarové nástroje, varovné systémy, ale také vhodné nástroje pro analýzu nežádoucích stavů.

Příloha B: Faktory determinující robustnost kritických subjektů

Sféry resilience	Proměnné	Deskripce proměnných	Měřitelné položky
Organizační resilience	Reakceschopnost kritického subjektu	Soubor organizačních opatření a postupů pro hlášení a zvládání incidentů.	Časový interval pro aktivaci ochranných opatření
			Stav sil a prostředků
	Management incidentů	Soubor schopností a dovedností krizového managementu a způsobů komunikace a sdílení informací při zvládání incidentů.	Připravenost krizového managementu
			Komunikace a sdílení informací
Infrastrukturní resilience	Fyzická rezistence infrastruktury	Schopnost infrastruktury odolávat negativním účinkům naturogenních, antropogenních a technogenních nebezpečí, a to prostřednictvím materiálové a konstrukční rezistence těchto staveb.	Požární odolnost
			Seismická odolnost
			Výbuchová odolnost
	Reakce na incident	Schopnost zařízení zabránit šíření následků incidentů a zajištění opravitelnosti klíčových technologií.	Redukce následků incidentu
			Udržení funkčnosti klíčových technologií
	Redundance infrastruktury	Schopnost okamžité substituce výkonu narušené části infrastruktury nebo posílení její kapacity.	Kritérium spolehlivosti
			Dostupnost redundantní kapacity
			Dočasná substituce klíčových technologií

Časový interval pro aktivaci ochranných opatření slouží k posouzení reakčního času systému pro aktivaci klíčových (primárních) ochranných opatření, které zajistí minimalizaci ztrát při vzniku incidentu (Rehak et al., 2019).

Stav sil a prostředků spočívá v posouzení dostupnosti sil a prostředků, které má kritický subjekt k dispozici pro minimalizaci dopadů incidentu (Rehak et al., 2019). Síly a prostředky jsou nezbytné k přerušení příčin a řešení dopadů incidentu ve výrobním procesu.

Připravenost krizového managementu slouží k posouzení úrovně schopností a dovedností krizového managementu kritického subjektu řešit incidenty a krizové situace (Carmeli and Schaubroeck, 2008).

Komunikace a sdílení informací slouží k posouzení postupů, metod a způsobů/kanálů pro výměnu informací mezi interními a externími zainteresovanými stranami v průběhu incidentu, a to prostřednictvím hlasového a datového přenosu informací prostřednictvím veřejných i neveřejných telekomunikačních sítí (Savolainen, 2017). Při krizové komunikaci je klíčové, zda vnímání lidí odpovídá reálnému stavu a jakou mají schopnost asimilovat informace v průběhu incidentu.

Požární odolnost spočívá v posouzení schopnosti stavebních konstrukcí odolávat účinku plně rozvinutého požáru, aniž by došlo zejména k narušení jejich únosnosti a stability, celistvosti a izolační schopnosti (Chaturvedi et al., 2023).

Seismická odolnost spočívá v posouzení schopnosti stavebních konstrukcí odolávat účinkům zemětřesní prostřednictvím dostatečné tažnosti neboli duktility (Rasulo et al., 2021).

Výbuchová odolnost spočívá v posouzení schopnosti staveb svou dispozicí a opatřeními předcházet výbuchům (tj. aktivní výbuchová ochrana) anebo eliminovat účinky výbuchu (tj. pasivní výbuchová ochrana) (Bangash and Bangash, 2006).

Redukce následků incidentu spočívá v posouzení schopnosti technologie zabránit šíření následků incidentu. V případě kritických infrastruktur se jedná např. o automatické systémy hašení požárů nebo automatic incident detection for bridges and tunnels (Bosch, 2020).

Udržení funkčnosti klíčových technologií spočívá v posouzení možností realizace oprav klíčových technologií v průběhu působení incidentu či krizové situace, např. formou Public-Private Partnerships (Marana et al., 2017).

Kritérium spolehlivosti spočívá v posouzení, zda prvek splňuje tzv. kritérium spolehlivosti. Platí, že čím je toto kritérium vyšší, tím lze očekávat vyšší bezpečnost. Systém o N prvcích splňující kritérium N-1 pak při vyřazení jakéhokoliv jednoho prvku soustavy (z této N-tice) je schopen pracovat bez narušení funkce, tzn. s každou kombinací N-1 prvků (Ovaere and Proost, 2016).

Dostupnost redundantní kapacity spočívá v posouzení dostatečnosti kapacity a rychlosti zpohotovení záložních systému a opatření pro zajištění požadovaného výkonu/kapacity infrastruktury (Daidone et al., 2008). Mezi základní způsoby zvýšení spolehlivosti patří zvýšení bezporuchovosti systémů volbou co nejnižšího počtu sériového spolehlivostního modelu, zálohováním klíčových technologií, pojistky apod.

Dočasná substituce klíčových technologií spočívá v posouzení možností okamžité substituce klíčových technologií bez narušení výkonu infrastruktury, např. přesměrováním výroby na záložní systém (Steinhauser, 2021).

Příloha C: Faktory determinující obnovitelnost kritických subjektů

Sféry resilience	Proměnné	Deskripce proměnných	Měřitelné položky
Organizační resilience	Finanční zdroje	Dostupnost finančních zdrojů, popř. rezerv, umožňujících financování rychlé obnovy infrastruktury.	Alokace finančních zdrojů na obnovu
			Časová připravenost finančních zdrojů
	Lidské zdroje	Dostupnost lidských zdrojů s potřebnou kvalifikací.	Kapacita lidských zdrojů
			Odbornost lidských zdrojů
			Časová dostupnost lidských zdrojů
	Proces obnovy	Procesy podporující rychlou obnovu požadovaného výkonu infrastruktury.	Disaster připravenost procesů obnovy
			Obnova funkce infrastruktury
Infrastrukturní resilience	Materiální zdroje	Dostupnost potřebných komponent k realizaci opravy nebo náhrady poškozených nebo zničených částí infrastruktury.	Schopnost zotavení funkce infrastruktury
			Opravitelnost klíčových technologií infrastruktury
			Nahraditelnost klíčových technologií infrastruktury
			Časová dostupnost náhradních dílů a horizont oprav

Alokace finančních zdrojů na obnovu spočívá v posouzení míry a zdrojů finančních prostředků alokovaných na rychlou obnovu požadovaného výkonu infrastruktury (Zhang et al., 2018). S alokací finančních zdrojů úzce souvisí také *časová připravenost finančních zdrojů*, která spočívá v posouzení, jak rychle a jakým způsobem jsou vyčleňovány finanční zdroje na obnovu výkonu infrastruktury. Finanční prostředky mohou, ale také nemusí být předem průběžně (dobrovolně či na základě zákona atd.) vyčleňovány a/nebo akumulovány a/nebo pro daný (kalendářní) rok účelově vázány (při nevyčerpání se vrací).

Kapacita lidských zdrojů spočívá v posouzení množství personálu, který je možné vyčlenit pro obnovu infrastruktury, a posouzení jeho dislokace v rámci dané infrastruktury (Proag, 2021). S kapacitou lidských zdrojů souvisí také *odbornost lidských zdrojů*, která spočívá v posouzení kvalifikace personálu ve vztahu k požadavkům na obnovu výkonu infrastruktury, a *časová dostupnost lidských zdrojů*, která spočívá v posouzení časového hlediska dostupnosti potřebného personálu.

Disaster připravenost procesů obnovy spočívá v posouzení úrovně procesů, které ovládají nebo se zabývají materiálními zdroji, finančními zdroji/rezervami a lidskými zdroji. Jedná se o hodnocení procesu zajištění těchto zdrojů pro obnovu funkce infrastruktury z pohledu krizové připravenosti a přípravy na opakované působení small-scale disasters (Mohan, 2023).

Obnova funkce infrastruktury spočívá v posouzení úrovně plánování a obnovy funkce infrastruktury v důsledku působení small-scale disasters (Zorn and Shamseldin, 2015). Jedná se o čas a průběh obnovy výkonu infrastruktury po ukončení působení incidentu. Čím je čas obnovy výkonu kratší a nárůst výkonu rychlejší, tím dochází rychleji k obnově výkonu infrastruktury na požadovanou úroveň.

Schopnost zotavení funkce infrastruktury spočívá v posouzení úrovně zotavení funkce infrastruktury bez nutnosti realizace zásadních oprav. Jedná se zejména o obnovu nastavení či resetování elektronických částí systému. Pokud není zotavení funkce infrastruktury možné, je nutné disponovat informacemi o *opravitelnosti klíčových technologií infrastruktury*, která spočívá v posouzení, zda lze provést opravu klíčové technologie infrastruktury a jaké úrovně výkonu lze po této opravě dosáhnout (Ciapessoni et al., 2020).

Nahraditelnost klíčových technologií infrastruktury spočívá v posouzení, zda lze každou klíčovou technologii infrastruktury či její část nahradit (Hartmann and Maseberg, 2001). To znamená, zda již na trhu existuje nebo ji lze vyrobit a zda její náhradu či náhradní díl k opravě lze vůbec nainstalovat (zejména jde o fyzické překážky bránící instalaci). Náhradou se míní odstranění poškozené části či celé technologie a její výměna za díl s identickou funkcí. Výkon je ve smyslu (maximální) hodnoty, pro kterou je infrastruktura zařazena do systému kritické infrastruktury (např. transportní kapacita či propustnost komunikací nebo maximální průtok distribučního potrubí).

Časová dostupnost náhradních dílů a horizont oprav spočívá v posouzení, jak rychle je možné opravit nebo vyměnit poškozenou klíčovou technologii a obnovit výkon infrastruktury na požadovanou úroveň (Lamghari-Idrissi et al., 2020). Rovněž je nutné posouzení rychlosti dodání náhradních dílů či částí technologií, ale také specializovaných přístrojů, nástrojů a montážních pomůcek.

Příloha D: Faktory determinující adaptabilitu kritických subjektů

Sféry resilience	Proměnné	Deskripce proměnných	Měřitelné položky
Organizační resilience	Řízení organizace	Procesy související zejména s nastavením celého systému řízení, hodnot a pravidel organizace, nastavení organizační struktury, řízení zdrojů, procesů a výkonnosti.	Analýza organizačních procesů
			Řízení organizačních procesů
	Vzdělávací a rozvojové procesy	Procesy podporující znalosti, dovednosti a postoje zaměstnanců subjektu kritické infrastruktury.	Rozsah odborného vzdělávání
			Kvalita odborného vzdělávání
			Výcvik k řešení incidentů
			Hodnocení efektivnosti výcviku
	Inovační procesy	Procesy podporující invenci, vědu a výzkum a realizaci bezpečnostních opatření.	Inovace procesů řízení
			Inovace opatření a technologií
			Investice do inovací
	Implementační procesy	Procesy přípravy zavedení teoreticky naplánovaných myšlenek, projektů, procesů, systémů nebo řešení za účelem jejich dalšího použití.	Implementace nových procesů
			Implementace systémů řízení
			Implementace software
			Implementace bezpečnostních opatření
Infrastrukturní resilience	V infrastrukturní sféře resilience nebyly definovány žádné faktory determinující adaptabilitu kritických subjektů.		

Analýza organizačních procesů spočívá v posouzení pružnosti organizační struktury kritického subjektu (Chmielarz, 2013). Moderní formy organizační struktury činí společnosti více přizpůsobivé a schopné splnit očekávání vnitřních i vnějších zákazníků. V návaznosti na analýze organizačních procesů je rovněž nutné analyzovat *řízení organizačních procesů*, které spočívá v posouzení způsobu řízení organizačních procesů. Každá organizace nebo její část je řízena určitým způsobem, který lze hodnotit (Sincora et al., 2023).

Rozsah odborného vzdělávání spočívá v posouzení rozsahu odborného vzdělávání v rámci kritického subjektu umožňující získání specifické odbornosti nutné pro reakceschopnost a obnovu funkce infrastruktury. Hodnocení se zaměřuje především na počet vyškolených pracovníků a cílovou skupinu, tj. komu jsou školení určena (Yamoah, 2014). V souvislosti s rozsahem odborného vzdělávání je nutné posoudit také jeho kvalitu. *Kvalita odborného vzdělávání* spočívá v posouzení úrovně vzdělání, které je poskytováno či umožňováno pracovníkům kritického subjektu.

Výcvik k řešení incidentů spočívá v posouzení úrovně výcviku a udržování praktických dovedností pracovníků organizace k řešení small-scale disasters (Rodriguez and Walters, 2017). S výcvikem k řešení incidentů rovněž velmi úzce souvisí *hodnocení efektivnosti výcviku*, které spočívá v posouzení způsobu hodnocení efektivnosti výcviku pracovníků kritického subjektu.

Inovace procesů řízení spočívá v posouzení úrovně inovace procesů řízení v kritickém subjektu. Inovace mohou být realizovány v různých časových hlediscích, z čehož vyplývají dva způsoby realizace. Prvním způsobem je Business Process Reengineering, které předpokládá, že jednorázová změna je nezbytná pro takzvané „narovnání" procesů, které způsobí dramatickou změnu výkonnosti v organizaci (Fetais et al., 2022). Jedná se o radikální zásah do struktury procesu a měl by přinést okamžitou změnu. Druhým způsobem je Business Process Improvement, které předpokládá, že jednorázová změna v organizaci je nejen neefektivní, ale i nedostatečná, a dokonce i škodlivá. Proto usiluje pouze o postupnou změnu podnikových procesů, která je pro organizaci lépe přijatelná (Syed Ibrahim et al., 2019).

Inovace opatření a technologií spočívá v posouzení rozsahu realizace opatření a technologických inovací (Fayomi et al., 2019), které mohou být zaměřeny např. do oblasti inovace produktů (které se orientují na tvorbu nebo modifikaci poskytovaných služeb), inovace technologií (tj. zařízení, která dané produkty vytvářejí) nebo inovace technologických postupů (tj. způsobů, jak jsou produkty vytvářeny).

Investice do inovací spočívá v posouzení úrovně investic kritického subjektu do jednotlivých inovací (tj. procesů řízení, technologií a bezpečnostních opatření) a výzkumu a vývoje (Lazonick, 2023). Základním ukazatelem je nejen výše těchto prostředků, ale také jejich přiměřenost, účelnost a včasnost vynaložení.

Významnou roli v organizační resilienci sehrávají implementační procesy (Duchek, 2020), které zahrnují implementaci nových procesů, systémů řízení, software a bezpečnostních opatření. *Implementace nových procesů* spočívá v komplexním posouzení implementačních postupů a využívání implementačních nástrojů. *Implementace systémů řízení* spočívá v posouzení úrovně implementace systémů řízení v kritickém subjektu. Jedná se o komplexní celek propojených požadavků norem na kvalitu, ochranu životního prostředí a bezpečnost a ochranu zdraví při práci, který je zakomponován do celkového firemního systému řízení. *Implementace software* spočívá v posouzení úrovně zavedení nového či upgrade stávajícího software (naprogramování) vycházející z analýzy incidentů, požadavků a potřeb kritického subjektu. Jedná se také o zavedení úkonů, jejichž cílem je zajištění bezpečnosti v kybernetickém prostoru, jako je např.: zajištění informací v informačních systémech, dostupnost a spolehlivost služeb a sítí elektronických komunikací. *Implementace bezpečnostních opatření* spočívá v posouzení úrovně/stavu zavádění řešení a bezpečnostních opatření pro zajištění základní služby, které byly navrženy na základě získaných informací o vzniklém incidentu.

Podstatou adaptability kritických subjektů je posilování procesů organizace vůči proběhlým incidentům. Z tohoto důvodu nebyly v infrastrukturní sféře resilience definovány žádné determinující faktory.

Příloha E: Normalizované váhy měřitelných položek determinujících rezistenci kritických subjektů

Proměnné	**Měřitelné položky**	**Normalizované váhy**
Management rizik	Úroveň managementu rizik	0,05
	Metodologie posuzování rizik	0,05
	Implementace bezpečnostních norem	0,04
	Modelování incidentů	0,05
Anticipace	Preventivní kontrola	0,06
	Indikování narušení resilience kritického subjektu	0,04
Bezpečnostní opatření	Fyzická ostraha	0,06
	Režimová opatření	0,05
Krizová připravenost	Odpovědnosti, povinnosti a pravomoci	0,04
	Školení a výcvik pracovníků	0,04
	Bezpečnostní plánování a dokumentování	0,05
	Plánování kontinuity	0,05
Monitoring a provoz infrastruktury	Technický stav infrastruktury	0,06
	Údržba, servis a testování zařízení	0,04
Technické zabezpečení infrastruktury	Mechanické zábranné prostředky	0,06
	Elektronické sledovací a poplachové prostředky	0,06
	Kybernetická bezpečnost	0,05
Schopnost detekce incidentů	Monitoring prostředí	0,07
	Detekce vzniku incidentu	0,08
Σ		**1,00**

Příloha F: Normalizované váhy měřitelných položek determinujících robustnost kritických subjektů

Proměnné	**Měřitelné položky**	**Normalizované váhy**
Reakceschopnost kritického subjektu	Časový interval pro aktivaci ochranných opatření	0,09
	Stav sil a prostředků	0,08
Management incidentů	Připravenost krizového managementu	0,06
	Komunikace a sdílení informací	0,06
Fyzická rezistence infrastruktury	Požární odolnost	0,08
	Seismická odolnost	0,08
	Výbuchová odolnost	0,08
Reakce na incident	Redukce následků incidentu	0,11
	Udržení funkčnosti klíčových technologií	0,12
Redundance infrastruktury	Kritérium spolehlivosti	0,07
	Dostupnost redundantní kapacity	0,09
	Dočasná substituce klíčových technologií	0,08
Σ		**1,00**

Příloha G: Normalizované váhy měřitelných položek determinujících obnovitelnost kritických subjektů

Proměnné	**Měřitelné položky**	**Normalizované váhy**
Finanční zdroje	Alokace finančních zdrojů na obnovu	0,12
	Časová připravenost finančních zdrojů	0,10
Lidské zdroje	Kapacita lidských zdrojů	0,09
	Odbornost lidských zdrojů	0,09
	Časová dostupnost lidských zdrojů	0,08
Proces obnovy	Disaster připravenost procesů obnovy	0,09
	Obnova funkce infrastruktury	0,08
Materiální zdroje	Schopnost zotavení funkce infrastruktury	0,08
	Opravitelnost klíčových technologií infrastruktury	0,10
	Nahraditelnost klíčových technologií infrastruktury	0,09
	Časová dostupnost náhradních dílů a horizont oprav	0,08
Σ		**1,00**

Příloha H: Normalizované váhy měřitelných položek determinujících adaptabilitu kritických subjektů

Proměnné	**Měřitelné položky**	**Normalizované váhy**
Řízení organizace	Analýza organizačních procesů	0,08
	Řízení organizačních procesů	0,10
Vzdělávací a rozvojové procesy	Rozsah odborného vzdělávání	0,08
	Kvalita odborného vzdělávání	0,08
	Výcvik k řešení incidentů	0,10
	Hodnocení efektivnosti výcviku	0,06
Inovační procesy	Inovace procesů řízení	0,06
	Inovace opatření a technologií	0,08
	Investice do inovací	0,07
Implementační procesy	Implementace nových procesů	0,07
	Implementace systémů řízení	0,07
	Implementace software	0,07
	Implementace bezpečnostních opatření	0,08
Σ		**1,00**

Reference

Allen, A., Zilbert Soto, L., Wesely, J., Belkow, T., Ferro, V., Lambert, R., Langdown, I., Samanamu, A. (2017). From State Agencies to Ordinary Citizens: Reframing Risk-Mitigation Investments and Their Impact to Disrupt Urban Risk Traps in Lima, Peru. *Environment and Urbanization*, 29(2): 477-502. https://doi.org/10.1177/0956247817706061

ASIS. (2009). *Organizational Resilience: Security, Preparedness, and Continuity Management Systems – Requirements with Guidance for Use*. American National Standards Institute, Washington, DC.

Bangash, M.Y.H., Bangash, T. (2006). *Explosion-Resistant Buildings: Design, Analysis, and Case Studies*. Springer, Berlin, Heidelberg. https://doi.org/10.1007/3-540-31289-7

Blokdyk, G. (2017). *Gap Analysis: The Definitive Handbook*. Createspace Independent Publishing Platform, Scotts Valley, CA.

Blumenthal, D., Stoddard, R. (1999). Implementation Planning: The Critical Step. *PM Network*, 13(10): 80-86.

Bosch. (2020). *Automatic Incident Detection for Bridges and Tunnels*. Bosch Security Systems, Fairport, NY. Available at: https://media.boschsecurity.com/fs/media/pb/images/industries_2/transportation/APP-NOTE_Automatic_Incident_Detection.pdf (accessed 2024-04-24)

Brucherseifer, E., Winter, H., Mentges, A., Mühlhäuser, M., Hellmann, M. (2021). Digital Twin Conceptual Framework for Improving Critical Infrastructure Resilience. *Automatisierungstechnik*, 69(12): 1062-1080. https://doi.org/10.1515/auto-2021-0104

Carmeli, A., Schaubroeck, J. (2008). Organisational Crisis-Preparedness: The Importance of Learning from Failures. *Long Range Planning*, 41(2): 177-196. https://doi.org/10.1016/j.lrp.2008.01.001

Ciapessoni, E., Cirio, D., Pitto, A., Sforna, M. (2020). A Quantitative Methodology to Assess the Process of Service and Infrastructure Recovery in Power Systems. *Electric Power Systems Research*, 189: 106735. https://doi.org/10.1016/j.epsr.2020.106735

Daidone, A., Chiaradonna, S., Bondavalli, A., Veríssimo, P. (2008). Analysis of a Redundant Architecture for Critical Infrastructure Protection. In de Lemos, R., Di Giandomenico, F., Gacek, C., Muccini, H., Vieira, M. (Eds.), *Architecting Dependable Systems V. Lecture Notes in Computer Science*, Vol. 5135, Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-540-85571-2_4

De Felice, F., Baffo, I., Petrillo, A. (2022). Critical Infrastructures Overview: Past, Present and Future. *Sustainability*, 14: 2233. https://doi.org/10.3390/su14042233

Denyer, D. (2017). *Organizational Resilience: A summary of academic evidence, business insights and new thinking*. BSI and Cranfield School of Management, Cranfield.

Dozier, C.L., Briggs, A.M., Holehan, K.M., Kanaman, N.A., Juanico, J.F. (2022). Functional Analysis Methodology: Best Practices and Considerations. In Leaf, J.B., Cihon, J.H., Ferguson, J.L., Weiss, M.J. (Eds.), *Handbook of Applied Behavior Analysis Interventions for Autism. Autism and Child Psychopathology Series*. Springer, Cham. https://doi.org/10.1007/978-3-030-96478-8_22

Duchek, S. (2020). Organizational Resilience: A Capability-Based Conceptualization. *Business Research*, 13: 215-246. https://doi.org/10.1007/s40685-019-0085-7

ElSahly, O., Abdelfatah, A. (2022). A Systematic Review of Traffic Incident Detection Algorithms. *Sustainability*, 14(22): 14859. https://doi.org/10.3390/su142214859

EN 15602. (2022). *Private Security Services*. European Committee for Standardization, Brussels.

EN 50398-1. (2017). *Alarm Systems – Combined and Integrated Alarm Systems*. European Committee for Electrotechnical Standardization, Brussels.

Fayomi, O.S.I., Adelakun, J.O., Babaremu, K.O. (2019). The Impact of Technological Innovation on Production. *Journal of Physics: Conference Series*, 1378: 022014. https://doi.org/10.1088/1742-6596/1378/2/022014

Fekete, A. (2018). *Urban Disaster Resilience and Critical Infrastructure*. Julius-Maximilians-Universität Würzburg, Würzburg.

Fetais, A., Abdella, G.M., Al-Khalifa, K.N., Hamouda, A.M. (2022). Business Process Re-Engineering: A Literature Review-Based Analysis of Implementation Measures. *Information*, 13: 185. https://doi.org/10.3390/info13040185

Figueira, J., Greco, S., Ehrogott, M. (2005). Multiple Criteria Decision Analysis: State of the Art Surveys. Springer, New York, NY. https://doi.org/10.1007/b100605

Fishburn, P.C. (1971). A Comparative Analysis of Group Decision Methods. *Behavioral Science*, 16(6): 538-544. https://doi.org/10.1002/bs.3830160604

Fraser, A., Pelling, M., Scolobig, A., Mavrogenis, S. (2020). Relating Root Causes to Local Risk Conditions: A Comparative Study of the Institutional Pathways to Small-Scale Disasters in Three Urban Flood Contexts. *Global Environmental Change*, 63: 102102. https://doi.org/10.1016/j.gloenvcha.2020.102102

Grabinski, M. (2007). *Management Methods and Tools*. Gabler Verlag, Wiesbaden. https://doi.org/10.1007/978-3-8349-9295-6

Hartmann, M., Maseberg, S. (2001). Replacement of Components in Public Key Infrastructures. In *27th Annual Conference of the IEEE Industrial Electronics Society (IECON'01)*, Vol. 3, Denver, CO, pp. 2012-2016. https://doi.org/10.1109/IECON.2001.975600

Chaturvedi, S., Vedrtnam, A., Youssef, M.A., Palou, M.T., Barluenga, G., Kalauni, K. (2023). Fire-Resistance Testing Procedures for Construction Elements – A Review. *Fire*, 6(1): 5. https://doi.org/10.3390/fire6010005

Chmielarz, W., Zborowski, M., Biernikowicz, A. (2013). Analysis of the Importance of Business Process Management Depending on the Organization Structure and Culture. In *2013 Federated Conference on Computer Science and Information Systems*. Krakow, Poland, pp. 1079-1086.

IEC 31010. (2019). *Risk Management – Risk Assessment Techniques*. International Electrotechnical Commission, Geneva.

IEC 60812. (2018). *Failure Modes and Effects Analysis (FMEA and FMECA)*. International Electrotechnical Commission, Geneva.

IEC 62502. (2010). *Analysis Techniques for Dependability – Event Tree Analysis (ETA)*. International Electrotechnical Commission, Geneva.

ISO 9001. (2015). *Quality Management Systems*. International Organization for Standardization, Geneva.

ISO 12100. (2010). *Safety of Machinery – General Principles for Design – Risk Assessment and Risk Reduction*. International Organization for Standardization, Geneva.

ISO 22301. (2019). *Security and Resilience – Business Continuity Management Systems*. International Organization for Standardization, Geneva.

ISO/IEC 27001. (2022). *Information Security, Cybersecurity, and Privacy Protection – Information Security Management Systems – Requirements*. International Organization for Standardization, Geneva.

ISO 31000. (2018). *Risk Management*. International Organization for Standardization, Geneva.

ISO/TS 31050. (2023). *Risk Management – Guidelines for Managing an Emerging Risk to Enhance Resilience*. International Organization for Standardization, Geneva.

ISO 45001. (2018). *Occupational Health and Safety Management Systems – Requirements with Guidance for Use*. International Organization for Standardization, Geneva.

Iturriza, M., Labaka, L., Sarriegi, J.M., Hernantes, J. (2018). Modelling Methodologies for Analysing Critical Infrastructures. *Journal of Simulation*, 12(2): 128–143. https://doi.org/10.1080/17477778.2017.1418640

Lamghari-Idrissi, D., Basten, R., van Houtum, G.J. (2020). Spare Parts Inventory Control under a Fixed-Term Contract with a Long-Down Constraint. *International Journal of Production Economics*, 219: 123-137. https://doi.org/10.1016/j.ijpe.2019.05.023

Lazonick, W. (2023). *Investing in Innovation: Confronting Predatory Value Extraction in the U.S. Corporation*. Cambridge University Press, Cambridge. https://doi.org/10.1017/9781009410700

Levin, H.M., McEwan, P.J. (2000). *Cost-Effectiveness Analysis: Methods and Applications*. 2nd edit. SAGE Publications, Washington, DC.

Liu, W.B., Cheng, Z.L., Mingers, J., Qi, L., Meng, W. (2010). The 3E Methodology for Developing Performance Indicators for Public Sector Organizations. *Public Money & Management*, 30(5): 305-312. https://doi.org/10.1080/09540962.2010.509180

Lovecek, T., Reitspis, J. (2011). *Designing and Evaluation of Object Protection Systems*. University of Zilina, Zilina.

Marana, P., Labaka, L., Sarriegi, J.M. (2017). Maintenance in Critical Infrastructures: The Need for Public-Private Partnerships. In Carnero, M., González-Prida, V. (Eds.), *Optimum Decision Making in Asset Management*, IGI Global, pp. 62-82. https://doi.org/10.4018/978-1-5225-0651-5.ch003

Mentges, A., Halekotte, L., Schneider, M., Demmer, T., Lichte, D. (2023). A Resilience Glossary Shaped by Context: Reviewing Resilience-Related Terms for Critical Infrastructures. *International Journal of Disaster Risk Reduction*, 96: 103893. https://doi.org/10.1016/j.ijdrr.2023.103893

Metfessel, M. (1947). A Proposal for Quantitative Reporting of Comparative Judgments. *The Journal of Psychology: Interdisciplinary and Applied*, 24(2): 229-235. https://doi.org/10.1080/00223980.1947.9917350

Mohan, P.S. (2023). Disasters, Disaster Preparedness and Post Disaster Recovery: Evidence from Caribbean firms. *International Journal of Disaster Risk Reduction*, 92: 103731. https://doi.org/10.1016/j.ijdrr.2023.103731

Mukherjee, M., Abhinay, K., Rahman, M.M., Yangdhen, S., Sen, S., Adhikari, B.R., Nianthi, R., Sachdev, S., Shaw, R. (2023). Extent and Evaluation of Critical Infrastructure, the Status of Resilience and its Future Dimensions in South Asia. *Progress in Disaster Science*, 17: 100275. https://doi.org/10.1016/j.pdisas.2023.100275

Novotny, V., Sysel, P., Prinosil, J., Mekyska, J., Slavicek, K., Lattenberg, I. (2021). Critical Infrastructure Monitoring System. In *IEEE 17th International Colloquium on Signal Processing & Its Applications (CSPA)*, Langkawi, Malaysia, 2021, pp. 165-170. https://doi.org/10.1109/CSPA52141.2021.9377303

Ovaere, M., Proost, S.V. (2016). *Electricity Transmission Reliability: The Impact of Reliability Criteria*. Katholieke Universiteit, Leuven. https://doi.org/10.2139/ssrn.2874192

Philpott, D. (2016). *Emergency Preparedness: A Safety Planning Guide for People, Property and Business Continuity*. 2nd ed. Bernan Press, Lanham, MD.

Proag, V. (2021). Human Resources Management for Infrastructure. In *Infrastructure Planning and Management: An Integrated Approach*. Springer, Cham, pp. 563-593. https://doi.org/10.1007/978-3-030-48559-7_20

Rasulo, A., Pelle, A., Briseghella, B., Nuti, C. (2021). A Resilience-Based Model for the Seismic Assessment of the Functionality of Road Networks Affected by Bridge Damage and Restoration. *Infrastructures*, 6(8): 112. https://doi.org/10.3390/infrastructures6080112

Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act).

Rehak, D., Janeckova, H. (2024). Perceiving the Resilience of Land Transport Critical Entities. In: Prentkovskis, O., Yatskiv (Jackiva), I., Skackauskas, P., Karpenko, M., Stosiak, M. (Eds.), *TRANSBALTICA XIV: Transportation Science and Technology. TRANSBALTICA 2023. Lecture Notes in Intelligent Transportation and Infrastructure*, pp. 553-561. Springer, Cham. https://doi.org/10.1007/978-3-031-52652-7_55

Rehak, D., Senovsky, P., Hromada, M., Lovecek, T. (2019). Complex Approach to Assessing Resilience of Critical Infrastructure Elements. *International Journal of Critical Infrastructure Protection*, 25: 125-138. https://doi.org/10.1016/j.ijcip.2019.03.003

Rehak, D., Slivkova, S., Pittner, R., Dvorak, Z. (2020). Integral Approach to Assessing the Criticality of Railway Infrastructure Elements. *International Journal of Critical Infrastructures*, 16(2): 107-129. https://doi.org/10.1504/IJCIS.2020.107256

Rehak, D., Splichalova, A., Janeckova, H., Ooulehlova, A., Hromada, M., Kontogeorgos, M., Ristvej, J. (2024a). Critical Entities Resilience Assessment (CERA) to Small-Scale Disasters. *International Journal of Disaster Risk Reduction*, 111: 104748. https://doi.org/10.1016/j.ijdrr.2024.104748

Rehak, D., Splichalova, A., Hromada, M., Walker, N., Janeckova, H., Ristvej, J. (2024b). Critical Entities Resilience Failure Indication. *Safety Science*, 170: 106371. https://doi.org/10.1016/j.ssci.2023.106371

Rehak, D., Splichalova, A., Janeckova, H., Ryska, O., Oulehlova, A., Michalcova, L., Hromada, M., Kontogeorgos, M., Ristvej, J. (2025). Critical Entities Resilience Strengthening Tools to Small-scale Disasters. *International Journal of Critical Infrastructure Protection*, 49: 100766. https://doi.org/10.1016/j.ijcip.2025.100766

Rodriguez, J., Walters, K. (2017). The Importance of Training and Development in Employee Performance and Evaluation. *World Wide Journal of Multidisciplinary Research and Development*, 3(10): 206-212.

Savolainen, R. (2017). Information Sharing and Knowledge Sharing as Communicative Activities. *Information Research*, 22(3): 9.

Shaluf, I.M. (2007). Disaster types. *Disaster Prevention and Management*, 16(5): 704-717. https://doi.org/10.1108/09653560710837019

Sincora, L.A., Oliveira, M.P.V.d., Zanquetto-Filho, H., Alvarenga, M.Z. (2023). Developing Organizational Resilience from Business Process Management Maturity. *Innovation & Management Review*, 20(2): 147-161. https://doi.org/10.1108/INMR-11-2021-0219

Směrnice Evropského parlamentu a Rady (EU) 2022/2557 ze dne 14. prosince 2022 o odolnosti kritických subjektů a o zrušení směrnice Rady 2008/114/ES.

Splichalova, A., Patrman, D., Kotalova, N., Hromada, M. (2020). Managerial Decision Making in Indicating a Disruption of Critical Infrastructure Element Resilience. *Administrative Sciences*, 10(3): 75. https://doi.org/10.3390/admsci10030075

Steinhauser, F. (2021). Redundancy for Power Utility Communication Networks. In *26th International Conference and Exhibition on Electricity Distribution (CIRED 2021)*, pp. 1742-1746. https://doi.org/10.1049/icp.2021.1917

Swamidass, P.M. (2000). Deming Cycle (PDCA). In: *Encyclopedia of Production and Manufacturing Management*. Springer, Boston, MA. https://doi.org/10.1007/1-4020-0612-8_229

Syed Ibrahim, M., Hanif, A., Jamal, F.Q., Ahsan, A. (2019). Towards Successful Business Process Improvement – An Extension of Change Acceleration Process Model. *PLoS ONE*, 14(11): e0225669. https://doi.org/10.1371/journal.pone.0225669

Tracht, K., Goch, G., Schuh, P., Sorg, M., Westerkamp, J.F. (2013). Failure Probability Prediction Based on Condition Monitoring Data of Wind Energy Systems for Spare Parts Supply. *CIRP Annals*, 62: 127-130. https://doi.org/10.1016/j.cirp.2013.03.130

UNDRR. (2015). *Sendai Framework for Disaster Risk Reduction 2015-2030*. United Nations Office for Disaster Risk Reduction, Geneva.

Vidrikova, D., Boc, K., Dvorak, Z., Rehak, D. (2017). *Critical Infrastructure and Integrated Protection*. The Association of Fire and Safety Engineering, Ostrava.

Yamoah, E.E. (2014). The Link Between Human Resource Capacity Building and Job Performance. *International Journal of Human Resource Studies*, 4(3): 139-146. http://dx.doi.org/10.5296/ijhrs.v4i3.5938

Yang, Z., Barroca, B., Weppe, A., Bony-Dandrieux, A., Laffr´echine, K., Daclin, N., November, V., Omrane, K., Kamissoko, D., Benaben, F., Dolidon, H., Tixier, J., Chapurlat, V. (2023). Indicator-Based Resilience Assessment for Critical Infrastructures – A Review. *Safety Science*, 160: 106049. https://doi.org/10.1016/j.ssci.2022.106049

Zhang, Ch., Kong, J.J., Simonovic, S.P. (2018). Restoration Resource Allocation Model for Enhancing Resilience of Interdependent Infrastructure Systems. *Safety Science*, 102: 169-177. https://doi.org/10.1016/j.ssci.2017.10.014

Zorn, C.R., Shamseldin, A.Y. (2015). Post-disaster Infrastructure Restoration: A Comparison of Events for Future Planning. *International Journal of Disaster Risk Reduction*, 13: 158-166. https://doi.org/10.1016/j.ijdrr.2015.04.004