POSTUP PŘI POSILOVÁNÍ RESILIENCE V SYSTÉMU KRITICKÉ INFRASTRUKTURY

Ing. Nikol KOTALOVÁ

Fakulta bezpečnostního inženýrství, Vysoká škola báňská - Technická univerzita Ostrava

Lumírova 630/13, 700 30, Ostrava - Výškovice

E-mail: nikol.kotalova@vsb.cz

Abstrakt: *Kritická infrastruktura je složitý systém prvků a vazeb, jehož narušení může mít závažný dopad na bezpečnost a ekonomiku státu. Z tohoto pohledu je resilience kritické infrastruktury důležitým faktorem. V důsledku měnícího se charakteru hrozeb je nezbytné věnovat pozornost zejména posilování této resilience. Na základě toho se článek zaměřuje na analýzu metod a nástrojů posilování resilience kritické infrastruktury. Závěr práce předkládá navržený komplexní postup posilování resilience, který sestává z pěti kroků. Aplikované nástroje vedou ke zvýšení robustnosti, obnovitelnosti anebo adaptability, čímž se posiluje celková resilience. Prvek se tak stává více odolným, resp. méně zranitelným, vůči negativním vnějším i vnitřním hrozbám a v případě výskytu nežádoucí události je schopen rychle se zotavit a přizpůsobit se opakovanému působení již proběhlé nežádoucí události.*

Klíčová slova: *kritická infrastruktura, resilience, hodnocení resilience, posilování resilience, přístupy a nástroje*

1 Úvod

Termín kritická infrastruktura byl poprvé zakotven do krizového zákona při jeho novele v roce 2010 [1]. Prvky kritické infrastruktury (KI) se určují podle odvětvových a průřezových kritérií, která jsou definována v Nařízení vlády [2]. Odvětví KI je v České republice devět. Jedná se o energetiku, vodní hospodářství, potravinářství a zemědělství, zdravotní péči, dopravu, komunikační a informační systémy, finanční trh a měnu, nouzové služby a veřejnou správu, a jejich pododvětví. Průřezovými kritérii rozumíme soubor hledisek pro posuzování závažnosti vlivu narušení funkce prvku KI vyjádřením mezních hodnot, které zahrnují kritéria obětí, ekonomického dopadu a dopadu na veřejnost.

Problematika ochrany kritické infrastruktury patří do oblasti krizového řízení. Termíny a definice používané v oblasti kritické infrastruktury sjednocuje Komplexní strategie České republiky k řešení problematiky kritické infrastruktury [3]. Cílem ochrany kritické infrastruktury je zajištění jejího fungování a zavedení opatření pro snížení rizika narušení či selhání KI. Ochrana KI je založena na managementu rizik a krizovém managementu. Při posuzování prvků KI je důležité znát a hodnotit rizika, která mohou na prvek působit a umět je zvládat. Zabezpečení ochrany prvků kritické infrastruktury je proces managementu ochrany a spočívá v posilování resilience a zvládání rizik, tedy aplikace jedné nebo více možností k minimalizaci rizik tzn. retencí rizika, transferem rizika, redukcí rizika a/nebo vyhnutí se riziku [4,5].

Resilience v kontextu kritické infrastruktury představuje schopnost subsystémů kritické infrastruktury zajistit své funkce a udržovat je i při nežádoucí události. Je to vnitřní připravenost prvků či subsystémů na negativní působení vnitřních či vnějších faktorů při těchto událostech. Resilience byla v souvislosti s kritickou infrastrukturou poprvé definována komplexně jako schopnost prvku absorbovat, adaptovat se a rychle obnovit činnost prvku z důsledků působení nežádoucí události. Jde tedy o posouzení robustnosti, obnovitelnosti (technická resilience) a adaptability, tj. organizační resilience [6]. Resiliencí a ochranou kritické infrastruktury se intenzivně zabývá Presidential Decision Directive PPD-21 [7].

Posilování resilience [8, 9] prvků kritické infrastruktury je založeno v první řadě na identifikaci jednotlivých prvků kritické infrastruktury, která je nejen v Evropské unii, ale i ve světě, prováděna rozdílnými přístupy. Tyto přístupy jsou založeny na analýze rizik [10] analýze kritičnosti pomocí rozličných kritérií [11] průřezových a odvětvových kritérií [12] nebo na základě modelování a simulací [10].

Na základě zjištěné absence metod zabývajících se posilováním resilience v kritické infrastruktuře je cílem článku předložit navrhovaný komplexní postup posilování resilience prvku kritické infrastruktury.

2 Posuzování a posilování resilience kritické infrastruktury

Resilience v kontextu kritické infrastruktury představuje schopnost prvků kritické infrastruktury zajistit a udržovat své funkce provozuschopné při působení nežádoucí události. Je to vnitřní připravenost prvků či subsystémů na negativních faktorů působících při těchto událostech. Resilienci lze rozdělit do dvou oblastí. Na oblast technickou a organizační. Mezi technickou resilienci lze zařadit robustnost a obnovitelnost. Posilování technické resilience je realizováno výhradně jen ve vztahu ke konkrétnímu prvku. Další oblastí je organizační resilience, která je determinována úrovní vnitřních procesů, do kterých patří management rizik, inovační procesy, vzdělávací a rozvojové procesy (adaptace). [6]

Posilovat resilienci je možné prostřednictvím managementu rizik [13] a technik posuzování rizik [14]. Dostupná literatura, články, metodiky a další příspěvky poskytují nepřeberné množství metod, které se dají využít pro identifikaci slabých míst kritické infrastruktury. Tyto metody můžou být následně modifikovány či navzájem kombinovány pro konkrétní případy jejich užití a mohou rovněž sloužit jako podpůrný nástroj při stanovení, implementaci a rozhodování o bezpečnostních opatřeních posilujících resilienci prvku. Metody posuzování rizik jsou v kontextu hodnocení resilience kritické infrastruktury považovány za metody obecné. Doposud uvedené metody obecného charakteru, které jsou používány v oblasti posuzování rizik a dají se využít nejen v rámci měření a hodnocení resilience. Rešerše literatury a dostupných zdrojů poskytuje i speciální metody, které jsou používány pouze pro měření a stanovení úrovně resilience. Právě pomocí těchto metod je zjištěna úroveň resilience prvku a jsou nalezena slabá místa přispívající k vyšší zranitelnosti prvku. Výsledky a zjištění vyplývající z provedení těchto metod, jsou považovány za stěžejní informace, které jsou základem pro rozhodnutí a následnou aplikaci vhodných protiopatření, na základě čehož je resilience prvku posílena. Na základě výše uvedeného následující text popisuje vybrané metody a metodiky, zabývající se posuzováním resilience systémů, subsystémů, prvků, objektů či zařízení.

Metodika **CIERA** definuje postupy a kritéria pro hodnocení resilience prvků kritické infrastruktury, především v technických odvětvích. To spočívá ve vyhodnocování úrovně robustnosti prvků kritické infrastruktury, schopnosti obnovit svou funkci z následků působení nežádoucí události a schopnosti přizpůsobit se na již proběhlé nežádoucí události. Úroveň resilience je tedy vyhodnocována na třech úrovních – na úrovni prvku, komponenty a proměnné. Závěrečným krokem metodiky je pak vyhodnocení úrovně resilience prvku kritické infrastruktury, identifikace slabých míst a návrh opatření určených k posílení resilience prvku. Resilience musí být posilována vždy na nejnižší úrovni, tedy na úrovni měřitelných položek. [15]

Metodika obsahující **Resilience Measurement Index (RMI)** byla vyvinuta roku 2013 v Argone National Laboratory v USA a navazuje na Index resilience (RI), který byl představen touto společností již v roce 2010. RMI komplexně posuzuje systém od hrozby až k následkům, podporuje rozhodování o rizicích, reakci na katastrofy a zajišťuje kontinuitu systému. Hlavním účelem RMI je měření schopnosti kritické infrastruktury snížit velikost nebo trvání dopadů rušivých událostí [16]. Metoda využívající RMI třídí informace do šesti úrovní, aby se zvýšila specifičnost jednotlivých kategorií. Resilience Measurement Index tedy vnímá resilienci jako schopnost entity např. prvku, organizace, společnosti, regionu předvídat, odolávat, absorbovat, reagovat, adaptovat se a obnovit se z působení nežádoucí události [17]. Na základě používání této metody RMI, lze posléze navrhnout opatření přispívající ke zvýšení připravenosti na incident, implementace redundance ke zmírnění účinků incidentu a posílení nouzových opatření, plánování a implementace kontinuity podnikání za účelem zvýšení účinnost postupů reakce a obnovy. Informace a výstupy vyplývající z metody RMI vlastníci/provozovatelé zařízení používají ke srovnání jejich zařízení a podobnými sektory/subsektory a pomáhat jim provádět rozhodnutí v oblasti řízení rizik. Tyto informace lze také použít ke snížení rizika a zlepšení odolnosti na regionální úrovni.

Critical Infrastructure Resilience Index (CIRI) představuje holistickou, snadno použitelnou a potenciálně kompatibilní metodiku pro hodnocení odolnosti kritické infrastruktury, použitelnou pro prvky všech odvětví kritické infrastruktury. Metodika je nejvhodnější pro hodnocení organizační a technologické resilience prvků. Metodika se skládá ze čtyř hierarchicky uspořádaných ukazatelů. První úroveň představuje všechny fáze krizového managementu (posouzení rizik, prevence, připravenost, varování, odezva, obnova, zlepšování). Tyto ukazatele jsou jasně dané. Naopak ukazatelé 2. úrovně jsou flexibilní a dají se přizpůsobit dle potřeby. Třetí úroveň se skládá z podmnožin každého ukazatele 2. stupně a jsou rovněž přizpůsobitelné. Ukazatelé 4. úrovně se skládají z ukazatelů specifických pro každého provozovatele, který tuto metodiku používá. Na základě výstupů aplikace metodiky na konkrétní prvek lze následně navrhnout potřebná opatření pro zlepšení ochrany prvku. [18]

Guidelines for Critical Infrastructure Resilience Evaluation (CIRE) představují východisko a kombinaci definice, oblastí, schopností, modelů a prvků resilience s cílem vytvořit jednotné chápání a následné hodnocení resilience přizpůsobitelné konkrétnímu sektoru kritické infrastruktury [19]. Přístup je založen na hodnocení jednotlivých indikátorů utvářejících resilienci, přičemž výsledný kompozitní indikátor je funkcí indikátorů v dané oblasti. Metoda CIRE se zabývá zkoumáním čtyř oblastí systému resilience, oblastí fyzické

a logické, personální, organizační a kooperační. Podstatou fyzické a logické resilience je používání nejlepších dostupných technologií používaných pro specifické potřeby daných odvětví. Personální resilience zahrnuje popis profilů vedoucích zaměstnanců prvků kritické infrastruktury a tréninkové programy na vyškolení expertů. v rámci organizační resilience se zmiňuje definování a implementace organizační úrovně systému managementu resilience a také stanovení odpovědností osob na různých úrovních. Náplní kooperační resilience je poté zavedení spolupráce mezi rozdílnými odvětvími kritické infrastruktury, zahrnující soukromý i veřejný sektor. Dále je potřeba posoudit současný stav a příklady z praxe.

Další metodou použitelnou pro měření a hodnocení je **Resilience Framework For Measuring Development,** který využívá soubor indikátorů měřící pružnou povahu resilience a rozvoj prvků. v rámci této metody je resilience chápána jako identifikovatelný stav, který ztělesňuje základní soubor zásad. Řešení resilience mohou vytvářet kapacity v různých kontextech, systémech a geografických oblastech při dodržení společných zásad odolnosti. Některé klíčové vlastnosti řešení odolnosti jsou ty, které vytvářejí následující kapacity [20]: podporu flexibility a redundance zajišťují fungování základních systémů na více místech, budování místního a regionálního sebevědomí, posilování jednotlivců a kontrola proměnné důležité pro jejich osobní sociální, kulturní, ekologický a ekonomický blahobyt, vytvoření rozmanité a dostupné formy živobytí a místní vlastnictví majetku, vytváření cenného důvěryhodného partnerství a flexibilní sítě lidí a zdrojů, které se mohou připojit a časem se znovu připojovat, usnadnění průběžného učení, adaptaci, sdílení znalostí a inovací.

Walker et al. [21] zkoumali faktory, které tvoří adaptivní resilienci, dynamickou schopnost reagovat na události. Organizační resilienci dělí v a **Guide to Building Adaptive Resilience** do dvou úrovní, a to resilienci organizace a jednotlivých zaměstnanců. Tyto dvě úrovně jsou vzájemně propojené. Zatímco odolnost jednotlivce záleží na jejich osobních vlastnostech a pracovním prostředí, určuje ji také kultura organizace, pracovní postupy a způsob vedení. Individuální resilience jednotlivých zaměstnanců závisí na jejich vlastnostech, pracovním prostředí, kultuře organizace i stylu k vedení práce z řad nadřízených. Když mohou pracovat v podpůrném prostředí, spolupracují a manažeři je povzbuzují k učení, přispívá to k resilienci celé organizace.

3 Návrh postupu posilování resilience v systému kritické infrastruktury

Aby bylo možné resilienci posilovat, je nutné vybrat konkrétní nežádoucí událost, která na konkrétní vybraný prvek působí. Pomocí analýzy rizik se vyberou slabá místa v resilienci, která budou následně posilována. Posilování resilience je založeno na zvyšování úrovně faktorů, kterými je determinována. Může se tak jednat o změny v organizaci a implementaci nových vnitřních předpisů, bezpečnostní opatření prvku, zlepšení strukturálních a výkonových parametrů prvků nebo zlepšení jedné z oblastí technické resilience. Komplexní přístup k posilování resilience kritické infrastruktury se skládá z pěti základních bodů:

Krok 1: Výběr zájmových prvků

Výběr prvku závisí na tom, jakou má pro společnost hodnotu. Návrhy na posilování resilience se mohou lišit podle sektoru a prvků, na které budou metody aplikovány. Prvky mohou být vybrány např. pomocí SWOT analýzy [22]. Tato analýza analyzuje slabé a silné stránky (poskytuje rozbor a hodnocení vnitřního prostředí organizace) a současné situace v jejím vnějším prostředí (příležitosti a hrozby). Cílem analýzy je omezovat slabé stránky a podporovat silné stránky, hledat nové příležitosti zlepšování a posilování, které může organizace využít k předcházení hrozbám nebo snížení počtu slabých stránek. Silné stránky naopak využije k odvrácení hrozeb a při hledání příležitostí. SWOT analýzu aplikuje při analýze aktuálního úrovně ochrany kritické infrastruktury v ČR i Skalická [23]. Inspiruje se přitom v Koncepci ochrany obyvatelstva, kde se stejná metoda využívá [24].

Dále je možné využít debatu odborníků (brainstorming), kteří vyberou ohrožené či kritické prvky na základě svých znalostí a odborných zkušeností. Prvek, který chce organizace chránit je zvolen po konzultaci subjektu, gestora a zainteresovaných stran (zejména investorů a odběratelů služeb). Může se jednat a bodový prvek umístěn na malé ploše, liniový prvek jako je např. vedení nebo koridor zajišťující přenos elektrické energie, plošný prvek (více klíčových technologií, např. datové centrum nebo elektrárna). Hodnocení vždy probíhá vůči konkrétní hrozbě na konkrétní prvek. [15]

Krok 2: Posouzení rizik

Narušení kritické infrastruktury může být způsobeno přírodními vlivy, selháním techniky i činností člověka. Pravděpodobnost vzniku mimořádné události vyplívá ze statistik, které jsou stále přesnější, protože evidují, klasifikují a vyhodnocují události z celého světa [25, 26]. Proces posuzování rizik se skládá z identifikace rizik, analýzy rizik a jejich hodnocení. Rizika se identifikují některou z navrhovaných metod. Nejprve se identifikují zdroje hrozeb. Jako nástroje mohou být použity metody brainstormingu [27], FMEA [28], check listy (kontrolní seznamy), pomocné seznamy, bezpečnostní audit, stromy příčin a následků (ETA, FTA), what if (Co se

stane, když), studie nebezpečí a provozuschopnosti (HAZOP), předběžná analýza ohrožení (PHA). Předběžná analýza ohrožení je nejčastěji souhrn technik pro posouzení rizika uvedených výše a jejich kombinace. [29, 30], Pomocí analýzy rizik se vyjádří hrozby, které mohou působit na prvek. Jednotlivé události působí na prvek rozdílným způsobem a při nežádoucí události budou aplikována jiná opatření. Z důvodu velkého množství nežádoucích událostí, které mají různé působení na resilienci prvku, je navrhováno subjektům KI řešit pouze konkrétní nežádoucí události, které ohrožují objekt. Následné hodnocení posléze pomáhá subjektům při aplikaci některého z opatření na snížení rizik, pokud je riziko nepřijatelné.

Krok 3: Definování scénáře nežádoucí události

Definovat teoretické scénáře události pomocí metod ETA [31], nebo FTA [32]. Metoda ETA (Analýza stromu událostí) se doporučuje pro lepší pochopení toho, jaké účinky může mít nežádoucí událost na objekt kritické infrastruktury. Metoda představuje grafické vyjádření procesů, které se mohou vyskytovat v pracovní činnosti objektu. Začátkem grafu je iniciační událost a konstrukce událostí, které mohou následovat. Výsledkem je identifikace a vyhodnocení potencionálně nebezpečných rizik. Podobnou metodou je FTA (Analýza stromu poruch), která analyzuje poruchy v procesu zpětně. Jedná se o dedukci událostí, které mohly zapříčinit výskyt rizika. Výstupem je rozvětvující se graf zobrazující strom poruch.

Krok 4: Hodnocení resilience a identifikace slabých míst

K hodnocení resilience lze použít některou z navrhovaných metod k hodnocení resilience, která zároveň umí identifikovat slabá místa, která by měla být posilována. v rámci tohoto kroku se hodnotí robustnost, obnovitelnost a adaptabilita prvku. Podstatou je posouzení míry odolnosti vůči působení nežádoucích událostí. Vhodnou metodou na hodnocení resilience na elementální úrovni je metodika CIERA [15], jejíž principem je vyhodnocování úrovně robustnosti, schopnosti obnovit své funkce a přizpůsobit se. Zahrnuje tedy posouzení technické i organizační resilience s určením slabých míst, která se identifikují pomocí dekompozice výsledků hodnocení resilience provedenou na úrovni dotčených měřitelných položek. Řada autorů prezentuje metodické postupy k hodnocení resilience vhodné pro aplikaci na úrovní systémů a sybsystému, např. Nan a Sansavini [33], Jovanovic et al. [34], Cai et al. [35], Eusgeld et al. [36]. Labaka et al. [37] tvrdí, že je třeba změnit krizové řízení jako nástroj pro reakci na neočekávané situace, zatímco Kanadská vláda zakládá svůj akční plán na řízení rizik [38]. Technické aspekty resilience síťové infrastruktury z hlediska její schopnosti odolat seismice aktivita jsou studovány publikaci Dueñas-Osorio et al. [39]. Několik studií se také zaměřuje na vzájemnou závislost prvků v kritické infrastruktuře a jejich zranitelnost, např. [40, 41, 42]. Tyto přístupy se zaměřují na síť kritické infrastruktury jako celku a jsou užitečné na úrovni strategického řízení sítě.

Krok 5: Výběr oblasti a vhodných nástrojů k posílení resilience

Na vybranou oblast s výskytem slabých míst je vhodné aplikovat adekvátní metody či nástroje k posílení resilience. Při nízké, nedostačující či kritické úrovni resilience, se podle hodnocení vybere oblast, kterou je vhodné posílit a aplikují se opatření na zvýšení robustnosti, adaptability či obnovitelnosti prvku kritické infrastruktury [6]. Aplikací a dodržováním opatření na posílení robustnosti prvků se zvýší jejich absorpční kapacita, tj. schopnost prvku absorbovat působení dopadů nežádoucích událostí. Může se jednat např. o zvyšování úrovně zpracování bezpečnostních plánů, realizaci vhodné analýzy rizik, připravenost managementu, dostatečnou kapacitu záložního systému, včasné varování, monitorování hrozeb, udržování reakceschopnosti, použití technických prostředků a zvýšení fyzické odolnosti, ochranná opatření nebo projektovou dokumentaci. Nástroji na posílení obnovitelnosti prvku se zvyšuje schopnost prvku obnovit svou činnost a výkon na požadovanou úroveň poskytovaných služeb. Navrhovanými nástroji mohou být např. automatické restartování elektronických částí, opravitelnost či nahraditelnost klíčové technologie, časová dostupnost náhradních dílů, finanční zdroje na obnovu, kvalifikovaný personál, personální bezpečnost, nakládání s citlivými informacemi, plán obnovy funkce a kontinuity činností, zvýšení úrovně krizové připravenosti. Pokud má subjekt dostupné komponenty k realizaci opravy, má k dispozici finanční zdroje a rezervy k rychlé obnově prvku a lidi s potřebnou kvalifikací, může dojít k posilování resilience. Navrhované nástroje posilují adaptabilitu prvku, tj. schopnost připravit se a přizpůsobit se na stále se opakující událostí. Podstatou adaptability je vytváření co nejlepších podmínek pro posilování technické resilience. Posilovat organizační resilienci lze správným posouzením rizik, vhodnou úrovní managementu rizik, lepší úrovní specifikace scénářů NU, implementací systémů řízení, inovací procesů řízení, technologií a technologických postupů, bezpečnostních opatření, zapojením organizace do výzkumu a vývoje, vzdělávacími a rozvojovými procesy. v neposlední řadě nelze opomenout, že organizační resilience se skládá nejen z resilience organizace ale i resilience jednotlivých zaměstnanců, kterým je potřeba vytvořit vhodné pracovní místo, motivovat je, nepřetěžovat a naslouchat jejich potřebám pro zvýšení jejich pracovitosti a odolnosti v práci.

4 Závěr

Fungování kritické infrastruktury je klíčový předpoklad pro zabezpečení základních funkcí státu a lidských potřeb. Proto se státy snaží chránit je před působením negativních vlivů a dopady nežádoucích událostí. Každá taková událost může ovlivnit fungování prvků kritické infrastruktury a narušit jeho resilienci. Základem ochrany kritické infrastruktury je posilování její resilience. Posilování resilience kritické infrastruktury je náročný proces, který vyžaduje jasně definované funkční podmínky. Základem je vymezení a vnímání faktorů, které determinují resilienci kritické infrastruktury. Při posilování resilience jde tedy o zvyšování úrovně mnoha faktorů, kterými je resilience determinována. Tyto faktory se mohou dělit do oblasti technické resilience (tj. robustnosti a obnovitelnosti) a resilience organizační (tj. adaptability). [43]

Poděkování

Tento článek byl zpracován za podpory projektu SP2020/40 „Výzkum přístupů a metod posilování resilience prvků kritické infrastruktury v pododvětví elektroenergetiky“ studentské grantové soutěže VŠB-TU Ostrava.

Literatura

[1] Zákon 430. 2010. Zákon, kterým se mění zákon č. 240/2000 Sb., o krizovém řízení a o změně některých zákonů (krizový zákon), ve znění pozdějších předpisů.
[2] Nařízení Vlády č. 432/2010 Sb., o kritériích pro určení prvku kritické infrastruktury
[3] MV GŘ HZS ČR. 2013. Koncepce ochrany obyvatelstva do roku 2020 s výhledem do roku 2030. Praha: MV GŘ HZS ČR
[4] Řehák, D. 2012. Úvod do problematiky řízení rizik. In book: Bezpečnostní technologie, systémy a management II. Zlín: Radim Bačuvčík - VeRBuM. pp. 74-95. ISBN 978-80-87500-19-4.
[5] ISO/IEC 27001. 2013. Information technology — Security techniques — Information security management systems — Requirements.
[6] National Infrastructure Advisory Council (NIAC). 2009. Critical Infrastructure Resilience Final Report and Recommendations. U.S. Department of Homeland Security, Washington, D.C
[7] PPD-21. 2013. Presidential Decision Directive: Critical Infrastructure Security and Resilience. The White House, Washington, D.C
[8] Rogers, Ch. D. F., Bouch, Ch. J., Williams, S. et al. 2012. Resistance and resilience – paradigma for critical local infrastructure. Proceedings of the ICE - Municipal Engineer. Vol. 165, pp. 73-84. ISSN 0965-0903.
[9] A Summary of the 2014 Sector Resilience Plans. 2014. United Kingdom, London: Cabinet Office.
[10] Hokstad, P., Utne, I. B., Vatn, J. 2013. Risk and Interdependencies in Critical Infrastructures: a Guideline for Analysis. Springer. 252 p. ISBN 978-1-44714661-2.
[11] Ouyang, M. 2014. Review on modeling and simulation of interdependent critical infrastructure systems. Reliability Engineering & System Safety. Vol. 121, pp. 43-60. ISSN 0951-8320.
[12] Rada EU. 2008. Směrnice rady 2008/114/ES ze dne 8. prosince 2008, o určování a označování evropských kritických infrastruktur a o posouzení potřeby zvýšit jejich ochranu
[13] ISO 31000. 2018. Risk management (Řízení rizik - Principy a směrnice). Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví. 40 s.
[14] ISO 31010. 2019. Risk management – Risk assessment techniques. Geneva: International Organization for Standardization.
[15] Řehák, D. et al. 2018. Metodika hodnocení resilience prvků kritické infrastruktury. Ostrava: VŠB –Technická univerzita Ostrava, 2018. 90 s. ISBN 978-80-2484164-9.
[16] Petit, F., Bassett, G., Black, R., et al. 2013. Resilience Measurement Index: An Indicator of Critical Infrastructure Resilience. Chicago, IL: Argonne National Laboratory.
[17] Carlson, J., Haffenden, R., Bassett, G., Buchring. W., Collins, M., Pettit, F., Phillips, J., Verner, D., Whitfilld, R. 2012. Resilience: Theory and Application. Chicago, IL: Argonne National Laboratory. 60 p. DOI: 10.2172/1044521
[18] Alheib, M., Baker, G., Bouffier, C., Cadete, G., Carreira, E., Gattinesi, P., Guay, F., Honfi, D., Eriksson, K., Lange, K., Lundin, E., Malm, A., Melkunaite, L., Merad, M., Miradasilva, M., Petersen, L., Rodrigues, J., Salmon, R., Theocharidou, M., Willot, A. 2016. Report of Criteria for Evaluating Resilience. Ref. Ares 2519174 - 31/05/2016
[19] Bertochi et al. 2016. Guidelines for Critical Infrastructure Resilience Evaluation. Roma, Italy: Italian Association of Critical Infrastructures' Experts.
[20] Bhamra A. 2015. Resilience Framework For Measuring Development

[21] Walker B. et al. 2019. Becoming agile: a guide to building adaptive resilience. The University of Canterbury, New Zealand. ISBN 978-0-473-36036-8
[22] ManagementMania. 2019. SWOT analýza. In: ManagementMania.com [online]. Wilmington (DE) 2011-2019, 22.01.2017 [cit. 07.04.2019]. Dostupné z: https://managementmania.com/cs/swot-analyza
[23] Skalická, P. 2017. Ochrana a obrana kritické infrastruktury, Úskalí a možnosti rozvoje v České republice. The science for population protection. Institut ochrany obyvatelstva Lázně Bohdaneč. Online. Dostupné z: http://www.population protection.eu/prilohy/casopis/35/294.pdf
[24] MV ČR. 2010. Komplexní strategie České republiky k řešení problematiky kritické infrastruktury. Praha: Ministerstvo vnitra.
[25] IRDR. 2014. Peril. Classification and Hazard Glossary (IRDR DATA Publication No. 1). Beijing: Integrated Research on Disaster Risk.
[26] UNISDR. 2019. Centre for Research on the Epidemiology of Disasters – CRED, Brussels, Belgium. Online. Dostupné z: https://www.emdat.be/
[27] ISO 9001. 2008 Systémy managementu jakosti – Požadavky na systém
[28] ČSN EN 60812 (010675): 2007. Techniky analýzy bezporuchovosti systémů – Postup analýzy způsobů a důsledků poruch (FMEA)
[29] Bumba, J., Kelnar, L., Sluka, V. 2000. Postupy a metodiky analýz a hodnocení rizik. Praha: Výzkumný ústav bezpečnosti práce. Dostupné z: https://vubp.cz/soubory/prevence-zavaznych-havarii/metodiky/postupy-a-metodiky-analyz-a-hodnoceni-rizik.pdf
[30] Procházková, D. 2004. Metodiky hodnocení rizik. Časopis 112, ročník III, číslo 3/2004, s. 22 – 23. Dostupné z: http://www.hzscr.cz/clanek/archiv-2004-az-2008-
[31] ČSN EN 62502 (010676):2011. Techniky analýzy spolehlivosti - Analýza stromu událostí (ETA)
[32] ČSN EN 61025 (010676):2007. Analýza stromu poruchových stavů (FTA)
[33] Nan, C., Sansavini, G. 2017. a quantitative method for assessing resilience of interdependent infrastructures. Reliability Engineering and System Safety 157: 35-53. DOI: 10.1016/j.ress.2016.08.013
[34] Jovanović, A., et al. 2018. D1.2 - Analysis of Existing Assessment Resilience Approaches, Indicators and Data Sources. Stuttgart: EU-VRi. http://www.smartresilience.euvri.eu/sites/default/files/publications/SmartResD1.2.pdf.
[35] Cai, B., Xie, M., Liu, Y., Liu, Y., Feng, Q. 2018. Availability-based engineering resilience metric and its corresponding evaluation methodology. Reliability Engineering & System Safety 172: 216-224. DOI 10.1016/j.ress.2017.12.021
[36] Eusgeld I. et al. 2011. "System-of-systems" approach for interdependent critical infrastructures, Reliability Engineering and System Safety 96:6. 679-686. doi:10.1016/j.ress.2010.12.010
[37] Labaka, L., Hernantes, J., Sarriegi, J.M. 2015. A framework to improve the resilience of critical infrastructures. International Journal of Disaster Resilience in the Built Environment 6: 4, 409-423.
[38] Action Plan for Critical Infrastructure (2014-2017). 2014. Ottawa: Public Safety Canada. 14 p. ISBN 9781-100-23291-1.
[39] Dueñas-Osorio, J.I. et al. 2007. Seismic response of critical interdependent networks, Earthquake Engineering & Structural Dynamics 36:2. 285-306. doi:10.1002/eqe.626
[40] Guidotti, R. et al. 2016. The resilience of critical infrastructure: The role of network dependencies, Sustainable and Resilient Infrastructure 1:3–4. 153-168. doi:10.1080/23789689.2016.1254999
[41] He, X., Cha, E.J. 2018a. Modeling the damage and recovery of interdependent critical infrastructure systems from natural hazards, Reliability Engineering & System Safety 177. 162-175. doi:10.1016/j.ress.2018.04.029
[42] He, X., Cha, E.J. 2018b. Modeling the damage and recovery of interdependent civil infrastructure network using Dynamic Integrated Network model, Sustainable and Resilient Infrastructure 1-16. doi:10.1080/23789689.2018.1448662
[43] Řehák, D. 2018. Východiska hodnocení resilience prvků kritické infrastruktury. 23. medzinárodná vedecká konferencia Riešenie krízových situácií v špecifickom prostředí. Žilina: Fakulta bezpečnostného inžinierstva.