Analýza zdrojů rizik možného ohrožení prvku kritické infrastruktury

Nela Kadlčíková

Bakalářská práce
2016

Univerzita Tomáše Bati ve Zlíně
Fakulta logistiky a krizového řízení

Univerzita Tomáše Bati ve Zlíně
Fakulta logistiky a krizového řízení
Ústav krizového řízení
akademický rok: 2015/2016

ZADÁNÍ BAKALÁŘSKÉ PRÁCE
(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení:	**Nela Kadlčíková**
Osobní číslo:	**L13326**
Studijní program:	**B3909 Procesní inženýrství**
Studijní obor:	**Ovládání rizik**
Forma studia:	**prezenční**

Téma práce: **Analýza zdroju rizik možného ohrožení prvku kritické infrastruktury**

Zásady pro vypracování:

1. **Zpracujte teoretickou část zabývající se historií a vývojem kritické infrastruktury.**
2. **Popište současný stav ochrany kritické infrastruktury.**
3. **Popište možnosti analýzy rizik v oblasti ochrany kritické infrastruktury.**
4. **Analyzujte možné zdroje rizika pro vybraný prvek kritické infrastruktury.**

Rozsah bakalářské práce:

Rozsah příloh:

Forma zpracování bakalářské práce: **tištěná/elektronická**

Seznam odborné literatury:

[1] ŘEHÁK, David. Kritická infrastruktura elektroenergetiky: určování, posuzování ochrana. 1. vyd. V Ostravě: Sdružení požárního a bezpečnostního inženýrství, 2013, 79 s. Spektrum (Sdružení požárního a bezpečnostního inženýrství). ISBN 978-80-7385-126-2.

[2] ŠENOVSKÝ, Michail, Vilém ADAMEC a Pavel ŠENOVSKÝ. Ochrana kritické infrastruktury. 1. vyd. v Ostravě: Sdružení požárního a bezpečnostního inženýrství, 2007, 141 s. Spektrum. ISBN 978-80-7385-025-8.

[3] PROCHÁZKOVÁ, Dana. Bezpečnost kritické infrastruktury. Praha: České vysoké učení technické v Praze, 2012, 318 s. ISBN 978-80-01-05103-0.

Vedoucí bakalářské práce: **Ing. Slavomíra Vargová, Ph.D.**
Ústav krizového řízení

Datum zadání bakalářské práce: **5. února 2016**

Termín odevzdání bakalářské práce: **9. května 2016**

V Uherském Hradišti dne 22. února 2016

L.S.

UNIVERZITA TOMÁŠE BATI VE ZLÍNĚ
Fakulta logistiky a krizového řízení

doc. RNDr. Jiří Dostál, CSc.
děkan

Ing. et Ing. Jiří Konečný, Ph.D.
ředitel ústavu

Prohlašuji, že

- beru na vědomí, že odevzdáním bakalářské práce souhlasím se zveřejněním své práce podle zákona č. 111/1998 Sb. o vysokých školách a o změně a doplnění dalších zákonů (zákon o vysokých školách), ve znění pozdějších právních předpisů, bez ohledu na výsledek obhajoby;
- beru na vědomí, že bakalářská práce bude uložena v elektronické podobě v univerzitním informačním systému dostupná k prezenčnímu nahlédnutí, že jeden výtisk bakalářské práce bude uložen v příruční knihovně Fakulty logistiky a krizového řízení Univerzity Tomáše Bati ve Zlíně a jeden výtisk bude uložen u vedoucího práce;
- byl/a jsem seznámen/a s tím, že na moji bakalářskou práci se plně vztahuje zákon č. 121/2000 Sb. o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon) ve znění pozdějších právních předpisů, zejm. § 35 odst. 3;
- beru na vědomí, že podle § 60 odst. 1 autorského zákona má UTB ve Zlíně právo na uzavření licenční smlouvy o užití školního díla v rozsahu § 12 odst. 4 autorského zákona;
- beru na vědomí, že podle § 60 odst. 2 a 3 autorského zákona mohu užít své dílo – bakalářskou práci nebo poskytnout licenci k jejímu využití jen připouští-li tak licenční smlouva uzavřená mezi mnou a Univerzitou Tomáše Bati ve Zlíně s tím, že vyrovnání případného přiměřeného příspěvku na úhradu nákladů, které byly Univerzitou Tomáše Bati ve Zlíně na vytvoření díla vynaloženy (až do jejich skutečné výše) bude rovněž předmětem této licenční smlouvy;
- beru na vědomí, že pokud bylo k vypracování bakalářské práce využito softwaru poskytnutého Univerzitou Tomáše Bati ve Zlíně nebo jinými subjekty pouze ke studijním a výzkumným účelům (tedy pouze k nekomerčnímu využití), nelze výsledky bakalářské práce využít ke komerčním účelům;
- beru na vědomí, že pokud je výstupem bakalářské práce jakýkoliv softwarový produkt, považují se za součást práce rovněž i zdrojové kódy, popř. soubory, ze kterých se projekt skládá. Neodevzdání této součásti může být důvodem k neobhájení práce.

Prohlašuji,

- že jsem na bakalářské práci pracoval samostatně a použitou literaturu jsem citoval. V případě publikace výsledků budu uveden jako spoluautor.
- že odevzdaná verze bakalářské práce a verze elektronická nahraná do IS/STAG jsou totožné.

V Uherském Hradišti 14.4.2016

.....
podpis studenta

ABSTRAKT

Bakalářská práce se zabývá ochranou kritickou infrastrukturou. Teoretická část je zaměřena na historii, poté popisuje základní pojmy daného tématu a věnuje se určováním prvků kritické infrastruktury. Dále se věnuje ochraně kritické infrastruktury a metodám analýze rizik, které jsou úzce spjaty s kritickou infrastrukturou. V praktické části je popsán prvek kritické infrastruktury a to hasičská stanice v Luhačovicích, kde se provádí analýza rizik, pomocí metody FMEA procesu. Analyzují se zde zdroje rizika, které ohrožují prvek kritické infrastruktury. V konečné fázi je analýza vyhodnocena a navžena daná opatření.

Klíčová slova: kritická infrastruktura, prvek kritické infrastruktury, ochrana kritické infrastruktury, FMEA analýza, riziko

ABSTRACT

This thesis deals with the protection of critical infrastructure. The theoretical part focuses on the history, then describes the basic concepts of the topic and focuses on identifying critical infrastructure elements. It also discusses the critical infrastructure protection and risk analysis methods, which are closely linked to critical infrastructure. The practical part describes an element of critical infrastructure and a fire station in Luhačovice, wheretheyperform risk analysisusing FMEA process. Theyanalyzetheriskthatthreaten a criticalinfrastructure element. Theanalysisisevaluated and suggestedthemeasures in thefinalstage.

Keywords: critical infrastructure, a critical infrastructure element, a critical infrastructure protection, FMEA analysis, a risk

Děkuji vedoucí své bakalářské práce Ing. Slavomíře Vargové, Ph.D. za pomoc, vstřícnost, vynaložený čas a cenné rady, které mi poskytla při zpracování.

Dále děkuji panu Ing. Jaroslavovi Foldynovi z oddělení ochrany obyvatelstva a krizového řízení HZS ve Zlíně za ochotu při poskytování materiálů a informací k mé práci.

Děkuji také své rodině za trpělivost a podporu.

OBSAH

ÚVOD

Téma kritická infrastruktura je v dnešní době velmi aktuální. Terorismus, migrace a spousta dalších rizik ohrožují infrastrukturu víc a víc. Jakékoliv selhání nebo napadení infrastruktury by mohlo mít vážný dopad na životy lidí a celého chodu státu. Proto je potřebné, aby se ochrana kritické infrastruktury stále zdokonalovala jak na úrovni mezinárodní, tak na úrovni individuálních států.

Moje bakalářská práce bude zaměřena na jednu z devíti oblastí kritické infrastruktury a to na nouzové služby, do kterých spadá Hasičský záchranný sbor. Speciálně se budu věnovat hasičské stanici v Luhačovicích, kde budu analyzovat rizika, které tuto stanici ohrožují.

Bakalářská práce je rozdělena do dvou částí. V první teoretické části popisuji historii kritické infrastruktury v USA, NATU, Evropě a České republice, dále vymezuji základní pojmy, které spadají do daného tématu. Poté následuje problematika ochrany kritické infrastruktury, kde se speciálně orientuji na ochranu v oblasti nouzových služeb a dokumentací, která je s touto oblastí spjata. V poslední kapitole se zaměřuji na analýzu rizik. Popisuji metody analýzy rizik, které se v kritické infrastruktuře využívají a podrobněji se věnuji analýze FMEA, kterou aplikuji v praktické části.

Ve druhé praktické části popisuji prvek kritické infrastruktury a to hasičskou stanici v Luhačovicích, která spadá pod územní odbor Zlína. Věnuji se dennímu řádu příslušníka Hasičského záchranného sboru v Luhačovicích a zabývám deseti největšími riziky, která ohrožují Zlínský kraj včetně výše zmíněné stanice.

Cílem bakalářské práce je analýza zdrojů rizik, která můžou ohrožovat prvek kritické infrastruktury a návrhy možných opatření, která případné zdroje rizik sníží. K tomuto procesu používám metodu FMEA procesu.

I. TEORETICKÁ ČÁST

1 HISTORICKÉ POJETÍ KRITICKÉ INFRASTRUKTURY

Evropa je stále víc ohrožována různými riziky. Nejaktuálnějším problémem je terorismus a migrace, a proto je prvořadým úkolem Evropy a celého světa postarat se o bezpečnost svých občanů. Pokud nastane mimořádná událost, musí být prioritně zajištěno co nejrychlejší vyřešení této situace a občanům obstarány nezbytné zásoby. Proto se v minulosti začalo mluvit o nezbytných službách a systémech, které budou připraveny jak v běžném, tak v krizovém stavu. Tyto výše uvedené prvky byly později pojmenovány jako **kritická infrastruktura** (dále KI).

Římské impérium, ale také středověké čínské císařství patřilo mezi první společnosti, které si uvědomovaly, jak důležitá je infrastruktura společnosti. Tyto velmoci věděly, že pokud nebude dobře infrastruktura plnit své úkoly, může dojít ke kolapsu celé společnosti. Příkladem je kolaps římského impéria, který především z nefunkčnosti infrastruktury státu a nájezdů barbarů tento rozpad dovršily.

Problematika KI se v hojné míře začala prodiskutovávat v období 1. a 2. světové války. Válka, živelné katastrofy, politická bouření a další nežádoucí události dávají impuls k tomu, že infrastruktura společnosti pracovala a pracuje správně. Díky zachování správné funkčnosti infrastruktury v krizových situacích, vznikla KI jako důležitý podmět pro fungování lidské společnosti.

V současné době se ochrana prvků KI zaměřuje hlavně na ochranu před terorismem, který je v poslední době aktuální. Dále značnou míru věnuje zvládání živelných pohrom, včetně jejich následků. [1]

1.1 Vývoj v USA

USA byl jeden z prvních států, který začal pociťovat šíři problematiky KI. Prvním kompletním dokumentem, který se zaměřoval na ochranu KI byla tzv. Bílá kniha. Jde o směrnici č. 63, která byla vydána v roce 1998 jako rozhodnutí tehdejšího prezidenta Billa Clintona a jejímž cílem bylo přijetí důležitých opatření k rychlé eliminaci zranitelnosti, z pohledu hmotných a kybernetických útoků na kritickou infrastrukturu. [3]

Po teroristickém útoku 11. září 2001 na WorldTrade Center (Světové nákupní centrum) v New Yorku začaly otázky KI gradovat a nabývat nových rozměrů. Měsíc po této tragédii, přesně 16. října 2001 vydal prezident USA George W. Bush *„Vládní nařízení na ochranu kritické infrastruktury“*. Hlavním účelem, proč bylo toto nařízení vydáno, bylo zabezpečit

ochranu informačních systémů pro KI, dále pak pro nouzovou komunikační připravenost a ochranu hmotných zařízení, které informační systémy podporují. Zabezpečení ekonomiky, činnosti státu a vedení národní obrany bylo prioritní pro USA. [4]

V roce 2002 vyšla Národní strategie vnitřní bezpečnosti, která popisuje KI jako „ *systémy a zařízení hmotné a virtuální, které jsou životně důležité pro USA a zničení nebo vyřazení z činnosti takových systémů anebo zařízení by mělo vliv na snížení bezpečnosti, národní ekonomické bezpečnosti, národní veřejného zdraví nebo bezpečí, anebo jakoukoliv kombinaci“*. K největšímu vyvrcholení řešení KI došlo v roce v únoru 2003, když byla vydána Národní strategie fyzické ochrany kritické infrastruktury a klíčových zařízení a Národní strategie zabezpečení kybernetického prostoru, která je nejkomplexnější materiálem zabývající se KI. [4,5]

V roce 2006 byl vydán Národní plán KI a Strategie na ochranu kyberprostoru. Národní ochranná strategie je poslední dokument zabývající se národní bezpečností a od roku 1987 je každoročně obnovován. [1]

1.2 Kritická infrastruktura v NATO

Zprávu o schopnosti státu reagovat na krizovou situaci nebo mimořádnou událost projednal v roce 2003 Výbor pro civilní ochranu Severoatlantické aliance. Ve zprávě bylo vytyčených deset schopností:

- *centrální schopnost reakce,*
- *zásobování (doplňování) základních služeb,*
- *místní schopnost reakce,*
- *dekontaminace,*
- *místní očista,*
- *vakcinace a ošetřování,*
- *péče o hromadně zraněné,*
- *hromadná evakuace,*
- *zjišťování ohrožení a jejich pojmenování,*
- *informování, varování a vyrozumění veřejnosti.*

Jednání výboru se shodlo na faktu, že dvě nejkritičtější schopnosti jsou hromadná evakuace a informování, varování a vyrozumění veřejnosti. [6]

Ke zlepšení ochrany obyvatelstva a KI vede i skutečnost, že si informace mezi sebou vyměňují nejen členské státy, ale také státy partnerské. Tímto vzniká i zlepšení ochrany obyvatelstva a KI. Hlavní výbor pro civilní nouzové plánování (dále jen SCEPC) vybídl prozkoumat nejen hlavní aspekty KI, ale také neexistenci KI na společnost. Této práci se věnovaly podřízené plánovací výbory. [7]

Ministerská směrnice pro rok 2003 – 2004 se především zaměřuje na spolupráci a zapojení všech plánovacích výborů do činností na ochranu KI. Scénáře a rozpracování ochrany KI se objevuje v plánech plánovacích výborům. NATO rozlišuje tyto oblasti KI:

- energetiku,
- informační a komunikační systémy,
- dopravu,
- veřejné služby,
- strategické průmyslové sektory,
- zdravotní péči,
- telekomunikaci,
- bankovnictví a finance,
- nouzové služby,
- zachování kontinuity práce úřadů. [7]

1.3 Vývoj v Evropě

Problematikou KI v Evropě se jako první začalo zabývat Německo a Velká Británie. V Německu v roce 1999 byl projednán materiál o Informačně technickém ohrožení klíčových infrastruktur. Ve stejný rok Velká Británie ustanovila Koordinační centrum pro bezpečnost národní infrastruktury (CPNI – Center fortheProtectionofNationalInfrastructure). [1]

Orgány Evropské Unie (dále jen EU) se problematikou KI začaly zabývat až po narušení dodávek elektrické energie. Další příčinou byly přírodní katastrofy v některých evropských státech a také teroristické útoky v Madridě a Londýně. [7]

V rámci EU vznikla komplexní koncepce kritické infrastruktury a její ochrany v roce 2004, kdy byla Evropská komise požádána Evropskou radou o přípravu strategie na ochranu KI. Dne 20. září 2004 na základě této žádosti přijala Evropská komise zprávu pod názvem Ochrana KI v boji proti terorismu. Tato zpráva obsahovala návrhy ke zlepšení prevence připravenosti a schopnosti reagovat na teroristické útoky zasahující KI. [5]

Dne 17. listopadu 2005 byla v Bruselu vydána Zelená kniha o evropském programu na ochranu KI, která konkrétně řešila problematiku KI. Cílem této knihy bylo zapojit do spolupráce velké množství subjektů, které by svojí činností jakkoliv přispěly ke zlepšení a zkvalitnění ochrany KI. Evropský program pro ochranu kritické infrastruktury (dále jen EPCIP) uvádí, že: *"Účinná ochrana kritické infrastruktury vyžaduje komunikaci a spoluprací jak na národní úrovni, tak na evropské úrovni a to mezi všemi orgány, profesními organizacemi, vlastníky a provozovateli kritické infrastruktury, stejně tak na všech úrovních státní a veřejné zprávy a také veřejnosti"*. [9,5]

Hlavním cílem EPCIP by bylo zajistit, aby existovala přiměřená a rovnoměrná úroveň bezpečností ochrany KI v celé EU, aby docházelo k co nejmenšímu riziku možného selhání a také co k nejrychlejšímu nápravnému opatření. Na základě těchto faktů 8. prosince 2008 nabyla platnost „*Směrnice rady 2008/114/ES o určování a označování evropských kritických infrastruktur a o posouzení potřeby zvýšit jejich ochranu"*. Směrnice určuje postup pro označování evropské kritické infrastruktury (dále jen EKI). Umožňuje také kolektivní přístup k posouzení těchto infrastruktur s jednoznačným cílem a to zlepšit jejich ochranu. Směrnice se zejména věnuje odvětví energetiky a dopravy, dále pak zahrnuje pravidla pro zpracování plánů bezpečnosti provozovatelů evropské kritické infrastruktury. [10]

V roce 2006 EPCIP vydalo sdělení, které vyzvalo k vytvoření Informační sítě pro kritickou infrastrukturu (dále jen CIWIN). Tento informační a bezpečnostní systém na internetové bázi je určen k výměně informací a k diskuzi související s ochranou KI v rámci EU. V prosinci 2012 se CIWIN začal zprovozňovat a od ledna 2013 je funkční. Pozitivní vývoj byl zaznamenán hned v prvních měsících funkčnosti. [11]

Na základě celkového průzkumu EPCIP z roku 2006 a směrnice Rady 2008/114/EK byl 28. října 2013 přijat pracovní dokument Evropské komise o novém přístupu EPCIP. Díky výsledkům tohoto průzkumu dospěla Evropská komise k názoru, že zachováním aktuální směrnice a rozvojem meziodvětvového přístupu k ECIP lze řešit doposud známé nedostatky a zároveň se nezbavovat výhod současného právního rámce.

Nový přístup k EPCIP se věnuje praktickému provádění v rámci prevence, připravenosti a odezvy se zahájí se čtyřmi vybranými kritickými infrastruktury evropského rozměru: Elektrická přenosová síť, plynová přenosová síť, Eurocontrol (Síťový manažer) a Galileo (Evropský program pro globální satelitní navigační systém). [11]

1.4 Vývoj v České republice

Výbor pro civilní nouzové plánování (dále jen VCNP) byl první orgán, který byl zřízen usnesením vlády č. 391 o Bezpečnostní radě státu a o plánování opatření k zajištění bezpečnosti České republiky (dále jen ČR), který se zabýval řešením krizových situací na území státu.

„VNCP je stálým pracovním orgánem Bezpečnostní rady státu pro oblast civilního nouzového plánování a pro koordinaci a plánování opatření k zajištění ochrany vnitřní bezpečnosti státu.“ [12]

První dokument, který pojednával o dané problematice v rámci VNCP byla *„Zpráva o národní kritické infrastruktuře“* z 24. září 2002, která se zabývala především vymezením a definováním pojmů a jednotlivých oblastí KI. [5]

Na dalších schůzích dne 24. června 2003 a 23. března 2004 VNCP řešil gesce o rozdělení KI. [13]

„Koncept ochrany obyvatelstva do roku 2006 s výhledem do roku 2015“ byl výchozím dokumentem pro rozvíjení ochrany obyvatelstva v našich podmínkách v návaznosti na novou legislativu z roku 2000, kterou schválila vláda ČR č. 417 dne 22. dubna 2002 a byla aktualizována usnesením vlády č. 21 ze dne 5. ledna 2005. Ochrana obyvatelstva je v koncepci vyznačována jako soubor činností a postupů, věcně příslušných orgánů, dalších subjektů i jednotlivých občanů, směřujících k minimalizaci dopadů mimořádných událostí na lidské životy a zdraví obyvatelstva, majetku a životního prostředí. [14]

Další důležité dokumenty, které se zabývají rozvojem KI v ČR jsou:

- Usnesení Bezpečnostní rady státu č. 204/2001 – obsahuje veškeré informace ke zpracování definice a stanovení rozsahu základních funkcí státu za krizových situací,
- Usnesení VCNP č. 152/2002 – vymezuje rozsah základních funkcí státu za krizových situací,
- Usnesení VCNP č. 153/2002 – Zpráva o národní kritické infrastruktuře a ustanovení VCNP k tomu jak řešit problematiku zachování základních funkcí státu a KI,
- Usnesení VCNP č. 179/2003 – obsahuje seznamy subjektů KI na národní, regionální a místní úrovni (aktualizace usnesení VCNP č. 190/2004),
- Usnesení VNCP č. 222/2006 – byla ustanovena Zpráva o stavu řešení problematiky KI (popisuje první srovnání kroků ČR se zahraničím),
- Usnesení VNCP č. 244/2007 – obsahuje Zprávu o řešení problematiky KI,

- Usnesení Bezpečnostní rady státu č. 30/2007 – definuje Zprávu o řešení problematiky KI.

Vzhledem ke vstupu ČR do EU 1. 5. 2004 souvisí další dokumenty závazné pro ČR s nařízeními EU, která platí pro všechny členské státy EU. Tím nejdůležitějším dokumentem je Zelená kniha o Evropském programu na ochranu KI, která byla ustanovena v roce 2005 a tím nesla ji související ustanovení VCNP č. 236/2005 o informacích ČR ke stanovisku k Zelené knize. [15]

ČR má svůj zákon, který se týká problematiky KI. Je jím **zákon č. 240/2000 Sb**., o krizovém řízení a o změně některých zákonů (krizový zákon). [16]

V roce 2013 byla vypracována nová koncepce ochrany obyvatelstva platná do roku 2020 výhledově do roku 2030, která byla vypracována ministerstvem vnitra – generálního ředitelství Hasičského sboru České republiky (dále jen HZS) v souladu s ustanovením podle zákona 239/2000 Sb. o integrovaném záchranném sboru a o změně některých zákonů, ve znění pozdějších předpisů. *„Koncepce ochrany obyvatelstva do roku 2013 s výhledem do roku 2020“* obsahuje oblasti ochrany obyvatelstva, jako je třeba vzdělávání, výchova nebo úkoly ochrany obyvatelstva a krizového řízení. [17]

2 ZÁKLADNÍ POJMY V KRITICKÉ INFRASTRUKTUŘE

Hrozba – *„Hrozba je síla, událost, aktivita nebo osoba, která má nežádoucí vliv na bezpečnost nebo může způsobit škodu.“* [14]

Infrastruktura - pojem infrastruktura se vyskytl jako první v 19. století ve Francii. V první polovině 20. století pojem označoval vojenská zařízení. V nejobecnějším pojetí se infrastrukturu označuje jako množina položek, které propojují strukturální prvky systému, které udržují celou strukturu pohromadě. Definice infrastruktury zní: *„Infrastruktura je odvětví zajišťující ekonomické a sociální systémové funkce (např. doprava, energetika, stavby škol a zdravotnických zařízení).“* [18,19]

Kritická infrastruktura - definice KI se v každé zemi mírně rozlišují, ale základní koncept je vždy stejný. Ministerstvo vnitra ČR definuje KI jako: *„Kritickou infrastrukturou se rozumí výrobní a nevýrobní systémy a služby, jejichž nefunkčnost by měla závažný dopad na bezpečnost státu, ekonomiku, veřejnou správu a zabezpečení základních životních potřeb obyvatelstva.“* [20]

KI může být rozdělena na národní a evropskou. Národní kritická infrastruktura je specifikována pro každý členský stát samostatně a evropská kritická infrastruktura je taková, jejíž narušení by mělo dopad na více členských státu najednou. [9]

Krize - *„Krize je situace, v níž je významným způsobem narušena rovnováha mezi základními charakteristikami systému na jedné straně a postojem okolního prostředí k danému systému na straně druhé. Krize je vždy spjata s nějakou hrozbou. Krize obecně je tedy stav, kdy dojde k nežádoucí situaci a to překročení nebo naopak pokročení nějaké meze, kterou považujeme za kritickou.“* [14]

Krizová situace – podle zákona 240/2000 Sb. o krizovém řízení a zákona 110/1998 Sb. o bezpečnosti ČR je: *„Krizová situace nebo také krizový stav je mimořádná událost, při níž je vyhlášen stav nebezpečí, nouzový stav, stav ohrožení státu nebo válečný stav. Jedná se o situaci ohrožující životy, zdraví, majetek, životní prostředí nebo vnitřní bezpečnost a veřejný pořádek.“* [16]

Krizové řízení – *„Je to souhrn řídících činností věcně příslušných orgánů zaměřených na analýzu a vyhodnocení bezpečnostních rizik, plánování, organizování, realizaci a kontrolu činnosti prováděných v souvislosti s řešením krizové situace.“* [14]

Mimořádná událost – *„Událost nebo situace vzniklá v určitém prostředí v důsledku živelní pohromy, havárie, nezákonnou činností, ohrožením kritické infrastruktury, nákazami, ohrožením vnitřní bezpečnosti a ekonomiky, která je řešena obvyklým způsobem orgány a složkami bezpečnostního systému podle zvláštních právních předpisů.“* [22]

Objekt kritické infrastruktury - *„Stavba nebo zařízení zajišťující fungování kritické infrastruktury.“* [20]

Ohrožení –„*Ohrožení danou pohromou je určeno velikostí jevu, kterou lze očekávat v daném místě za specifikovaný časový interval s pravděpodobností rovnou stanovené hodnotě. Není-li určeno jinak, tak s pravděpodobností výskytu jevu větší nebo rovnou 0.05 za rok pro časový interval sto let. Je to soubor maximálních dopadů pohromy v daném místě za specifikovaný časový interval.“* [33]

Ochrana kritické infrastruktury - *„Souhrn opatření, která při zohlednění možných rizik směřují k zabránění jejího narušení.“* [20]

Riziko – *„Riziko je nebezpečí škod v souvislosti s hrozbou a konečnou ztrátou. Rizikem je pravděpodobnost škody.“* [23]

Subjekty kritické infrastruktury - *„Vlastník nebo provozovatel objektů kritické infrastruktury.*“ Z větší části jsou subjekty KI soukromé. Proto je nutná komunikace a spolupráce s veřejným a státním sektorem. [20]

2.1 Kritická infrastruktura společnosti

Dnešní společnost je závislá na dobře fungující infrastruktuře a to zejména na technologické (dodávky vody a potravin, dodávky elektřiny a tepla, dodávky pohonných hmot, mobilita, komunikace atd.). Její nefunkčnost by měla vážný dopad na základní lidské potřeby (zdraví, bezpečí) a kvalitu lidského života (majetek, spotřeba energie a potravin, ochrana krajiny, majetku a prostředí).

KI se ze společenského hlediska rozumí vzájemně propojené sítě či systémy obsahující identifikovatelné odvětví a instituce (včetně lidí a postupů) a poskytující spolehlivý tok produktů a služeb podstatných pro obranu a ekonomickou bezpečnost. Pod touto bezpečností se chápe schopnost státu konkurovat na globálních trzích, zatímco se udržují na přijatelné úrovni reálné příjmy obyvatel a fungování veřejné správy na všech úrovních společnosti. Dále pak rozlišu-

jeme bezpečnost fyzickou, která se týká ochrany fyzických aktiv před škodami v důsledku působení fyzických sil a bezpečnost kybernetickou, která se zabývá především ochranou před poruchami nebo neautorizovanými přístupy do počítačové sítě.

Infrastruktura společnosti se skládá z ekonomické, sociální a nehmotné infrastruktury.

Ekonomická infrastruktura obsahuje fyzická zařízení komunikační, dopravní, vodovodní sítě a také obsahuje veškeré typy budov, přehrad, továren, zásobníků atd.

Sociální infrastruktura obsahuje fyzická zařízení, jako jsou nemocnice, školy, kostely, věznice, obchodní centra, stadiony, muzea, parky atd.

Nehmotná infrastruktura je sestavena s nehmotných aktiv vyjadřujících schopnosti a zdravotní stav komunity a její produktivní vlastnosti. [8]

2.2 Vymezení kritické infrastruktury

Definice KI nepodává příliš jasný obraz o tom, jaké konkrétní prvky zahrnuje pojem KI. Konkrétněji se k tomuto vyjadřuje Nařízení vlády č. 432/2010 Sb., o kritériích pro určení prvku kritické infrastruktury, které stanovuje dvojí systém základních kritérií, podle kterých lze posoudit, zda daný systém nebo zařízení spadá pod kritickou národní infrastrukturu. [24]

Jako první jsou tzv**. průřezová kritéria**, která zahrnují tři typy kritérií. Jedná se o následující:

a) ***počet obětí*** *s mezní hodnotou více než 250 mrtvých nebo více než 2500 osob s následnou hospitalizací po dobu delší než 24 hodin,*
b) ***ekonomický dopad*** *s mezní hodnotou hospodářské ztráty státu vyšší než 0,5 % hrubého domácího produktu, nebo,*
c) ***dopad na veřejnost*** *s mezní hodnotou rozsáhlého omezení poskytování nezbytných služeb nebo jiného závažného zásahu do každodenního života postihujícího více než 125000 osob.* [24]

V průřezových kritériích není požadováno splnění všech tří skupin, ale pro zařazení do kritické národní infrastruktury stačí, aby došlo ke zničení daného prvku a došlo k naplnění **byť jen jednoho z nich**.

Druhá jsou tzv. **kritéria odvětvová**, tato kritéria obsahují podmínky specificky nastavené podle konkrétního odvětví. Například v rámci energetiky jsou kritéria pro zemní plyn stanovena zvlášť pro přepravní soustavu, distribuční soustavu a zvlášť pro skladování plynu. Větši-

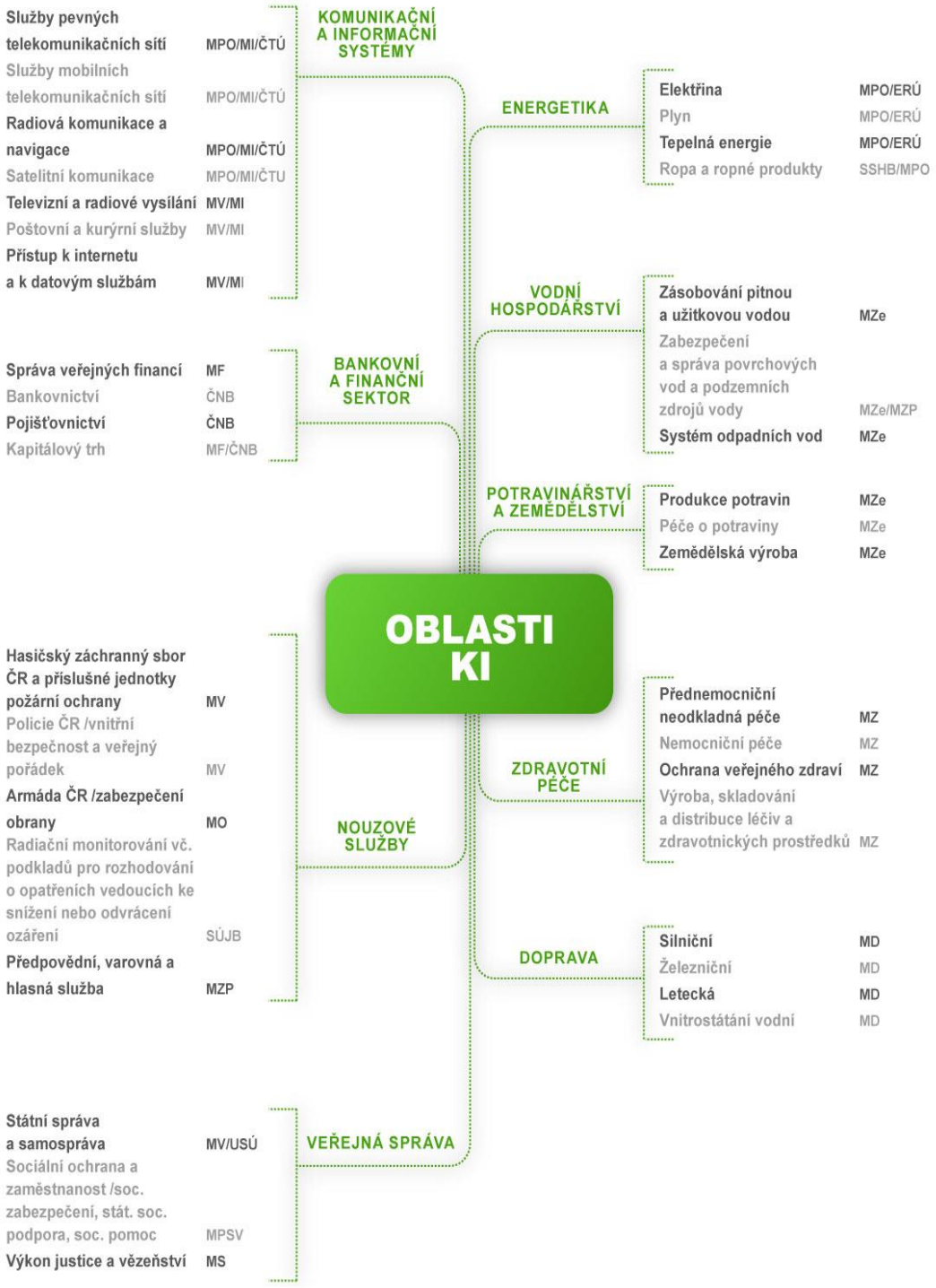
nou jsou pro všechny skupiny odvětví koncipována kritéria z hlediska výkonu, kapacity, velikost atd. [24]

2.3 Oblasti kritické infrastruktury

V ČR máme devět oblastí KI:

- *energetika,*
- *vodní hospodářství,*
- *zdravotní péče,*
- *potravinářství a zemědělství,*
- *zdravotnictví,*
- *doprava,*
- *finanční trh a měna,*
- *nouzové služby,*
- *veřejná správa.*

K dispozici je i dílčí členění jednotlivých skupin odvětvových kritérií, které se člení na další podskupiny v rámci kterých, jsou k dispozici i další sady kritérií. Cílem tohoto členění je snaha o co nejpřesnější nastavení kritérií v dané oblasti. [27]



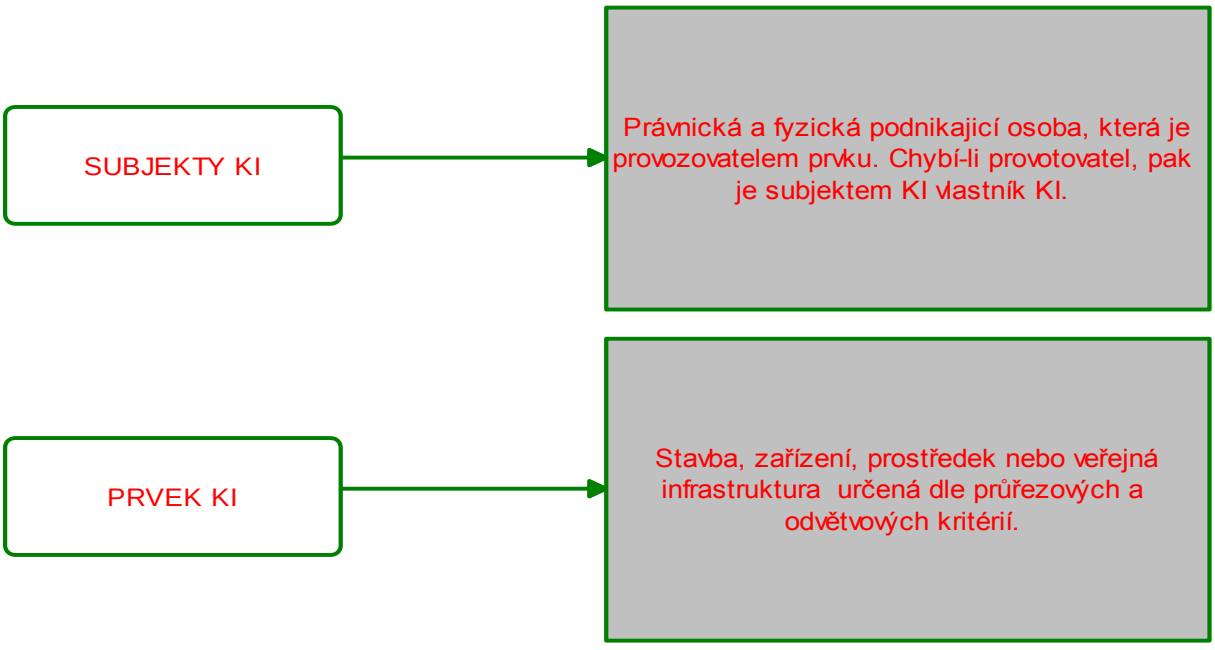
Obr. 1. Oblasti KI [vlastní]

2.4 Subjekty kritické infrastruktury

Subjektem KI je provozovatel prvku KI. Subjekt KI zodpovídá za ochranu prvků KI a jeho povinností je vypracovat plán krizové připravenosti subjektu KI do jednoho roku od rozhodnutí vlády, nebo ode dne dosažní právní moci, kterým byl prvek KI určen. Subjekt KI určuje styčného bezpečnostního zaměstnance a umožňuje příslušnému ministerstvu nebo ústředním správnímu orgánu provedení kontroly plánu krizové připravenosti subjektu KI a ochrany prvků KI a dále je také povinen oznámit informace o výrobní, organizační nebo jiné změně výše uvedeným orgánům, je-li zřejmé, že tato změna může mít vliv na určování prvků KI. [30]

2.5 Prvky kritické infrastruktury

Prvkem KI jsou především stavby, zařízení, prostředky nebo veřejná infrastruktura, určená dle výše zmiňovaných průřezových a odvětvových kritérií.



Obr. 2. Subjekty a objekty KI v České republice [vlastní]

2.5.1 Určování prvků kritické infrastruktury

Podmínka pro určení prvku KI je splnění jasně daných podmínek, a to splnění definice KI a splnění zákona č. 432/2010 Sb. o prvku KI a uplatnění průřezových a odvětvových kritérií. Poté je také třeba uvědomit si rozdíl určování prvků, když provozovatelem je organizační složka státu a naopak když není provozovatelem organizační složka státu. V případě, že provozovatelem je organizační složka státu, tak ministerstva a jiné ústřední správní úřady a také Česká národní banka zasílají návrhy prvků Ministerstvu vnitra (resp. generálnímu řediteli

HZS ČR), které k takto obdrženým podkladům zpracuje seznam. V dalším kroku je předložený vládě, která svým usnesením rozhoduje o KI, jejichž provozovatelem je organizační složka státu.

Když se určují prvky KI, jejichž **provozovatelem není organizační složka státu**, tak rozhodují příslušná ministerstva a jiné ústřední správní úřady a Česka národní banka, která o tomto určení informují Ministerstvo vnitra.

V roce 2011 proběhlo jednání mezi ČR a členskými státy EU, kdy byly Ministerstvu průmyslu a obchodu ČR předloženy návrhy určené k opatření celkem osmi prvkům KI v odvětví energetiky.

V témž roce uskutečnil proces určení státních prvků KI, jejichž provozovatelem je organizační složka státu. Ministerstvu vnitra byly zaslány příslušnými úřady návrhy prvků kritické infrastruktury. Na základě tohoto návrhu byl zpracován seznam, který byl předložen vládě. Tento seznam obsahoval 103 prvků v třech odvětvích (komunikační a informační systémy, veřejná zpráva a nouzové služby). Dne 4. prosince 2011 byl vládou schválen a přijat usnesením č. 934/2011 Sb. o určování prvků KI, jejichž provozovatelem je organizační složka státu.

Co se týká určování prvků KI, **kdy není provozovatelem organizační složka státu**, provádějí realizaci příslušná ministerstva, jiné ústřední správní úřady a Česká národní banka. V odvětvích energetiky byla určena elektřina a to 200 prvků, dále pak ropa a ropné produkty, kde bylo určeno 93 prvků. V odvětví hospodářství 11 prvků a dopravě 13 prvků. Pod odvětví komunikační spadaly technologické prvky pevné sítě elektrotechnických komunikací v počtu 719 prvků a technologické prvky pro poštovní služby v počtu 101 prvků. Poslední dvě odvětví byli finanční trh a měna, kde bylo určeno 74 prvků a nouzové služby s 19 prvky. [28]

*„**Dne 1. ledna 2015** nabylo účinnosti nařízení vlády č. 315 z 8. prosince 2014, kterým se mění nařízení vlády č. 432/2010 Sb. o kritériích pro určování prvku kritické infrastruktury.“*

Změny se týkají odvětvových kritérií a to konkrétně v odvětví energetiky, zdravotnictví, komunikačních a informačních systémů a nouzových služeb.

V odvětví **energetiky** přichází ke změně v limitu výkonu v oblasti elektřiny a nově vzniká pododvětví centrálního zásobování teplem. Pouze terminologická úprava je odvětví **zdravotnictví**. V odvětví **komunikačních a informačních systémů** dochází k zásadní změně. Je zde vloženo pododvětví kybernetické bezpečnosti, které obsahuje pět kritérií.

V posledním odvětví a to **nouzových služeb** přibylo kritérium pro stanice **HZS ČR**. [29]

3 OCHRANA KRITICKÉ INFASTUKTURY

KI musí fungovat za jakékoliv situace, a proto úkolem každé společnosti je ji chránit a to za běžných, mimořádných či kritických podmínek. Jakékoliv poškození, narušení nebo také zničení KI může být způsobeno přírodními katastrofami, vlivem činnosti lidského fakturu, selhání techniky, terorismem nebo také organizovaným zločinem. Ochrana kritické infrastruktury je proces zaměřený na opatření fungování subjektů a objektů KI, tak aby nedocházelo k jejich selhání. Podstatou ochrany KI je co nejmenší dopad výpadku činností infrastruktur tak, aby provoz funkcí, činností nebo služeb byl narušen krátkodobě, zvladatelně a územně omezen tak, aby postihl co nejméně lidí.

V ochraně KI je zahrnut velký počet existujících plánů zabývajících se prevencí, strategií, připraveností, odezvou a obnovou. Jde o souhrn existujících disciplín, do kterých patří například: krizové řízení, řízení rizik, plánování kontinuity podnikání, řízení bezpečnosti, ochrana obyvatelstva a strategie udržitelného rozvoje. Ochrana KI vyžaduje aktivní účast vlastníků a operátorů, regulátora, profesních asociací a institucí ochrany obyvatelstva. Tato spolupráce by se měla držet následujících zásad:

- Ochrana KI by se měla orientovat na minimalizaci zdravotních bezpečnostních rizik pro veřejnost a měla by být nápomocná ke sjednocení (kontinuitě) podnikání a kontinuitě služeb veřejné správy.
- Ochrana by se měla odrážet z analýzy vzájemných souvislostí a analýzy zranitelnosti vzhledem ke všem typům hrozeb a nebezpečí.
- Měly by se využívat vhodné postupy, metody a techniky řízení rizik pro určení úrovně bezpečné ochrany (ochranné bezpečnosti) a pro nastavení priorit rozdělení (alokace) zdrojů.
- Kritická společenská funkce je prioritním východiskem pro strukturování ochrany do tří vrstev. Vrstva fyzická (systém řízení bezpečnosti vlastníka), provozní (lidský faktor a organizační kultura) a strategická (veřejná správa zabývající se dopady na obyvatelstvo). [8,31]

3.1 Ochrana kritické infrastruktury v oblasti nouzových služeb

Základním aspektem ochrany KI v oblasti nouzových služeb je fungování složek integrovaného záchranného systému a dalších institucí a orgánů, které se podílejí na zajišťování aspektů ochrany KI. Tato ochrana spočívá v monitorování území nebo provozování předpovědní, va-

rovné a hlásné služby (Český hydrometeorologický ústav a Státní úřad pro jadernou bezpečnost). Uvedené subjekty plní své základní úkoly běžně, ale také hrají významnou roli při plnění úkolů při mimořádných událostech a krizových stavů. [32]

3.1.1 Opatření pro nouzové přežití

Zabezpečení opatření nouzového přežití je komplexní souhrn činností a postupů příslušných orgánů, subjektů a občanů prováděný s cílem snižovat negativní dopady mimořádných událostí a krizových situací na zdraví a životy obyvatelstva.

Opatření nouzového přežití se provádí přímo v místě mimořádné události nebo dochází k evakuaci obyvatelstva z postiženého území. Tato opatření jsou v Plánu nouzového přežití, který je součástí havarijního plánu kraje.

Plán nouzového přežití obyvatelstva obsahuje:

- *nouzové ubytování,*
- *nouzové zásobování potravinami,*
- *nouzové zásobování pitnou vodou,*
- *nouzové základní služby obyvatelstvu,*
- *nouzové dodávky energií,*
- *organizování humanitních pomocí a*
- *rozdělení odpovědnosti za provedení opatření pro nouzové přežití obyvatelstva.* [32]

3.2 Dokumenty ochrany kritické infrastruktury

Ochrana KI má své základní dokumenty, kterými jsou plány krizové připravenosti, které zpracovávají určené právnické nebo podnikající fyzické osoby a plány krizové připravenosti, které zpracovávají subjekty KI. [34]

3.2.1 Plán krizové připravenosti

Je dokumentem právnické nebo podnikající fyzické osoby, která zajišťuje provádění opatření, které vyplývá z krizového plánu a územního správního úřadu podle krizového zákona. Plán krizové připravenosti se skládá ze tří částí a je to prostředek k připravenosti na krizové situace. Základní část zahrnuje přehled a hodnocení možných zdrojů rizik a analýzu ohrožení. Operativní část obsahuje přehled opatření, které vyplývají z krizového plánu příslušného orgánu krizového řízení a způsob zjištění jejich provedení. Dále také obsahuje zabezpečení akceschopnosti ochrany činnosti právnické nebo podnikající fyzické osoby, postup jak řešit kri-

zové situace identifikované v analýze ohrožení a přehled spojení na orgány krizového řízení. Pomocná část poukazuje na právní předpisy, které se využívají při přípravě na mimořádné události nebo krizové situace a jejich řešení. [34]

3.2.2 Plán krizové připravenosti subjektu kritické infrastruktury

Je nástroj k obstarání připravenosti subjektu KI na krizové situace, které mohou ohrozit nebo narušit funkci prvku KI. Plán obsahuje tři části. V základní části se nachází seznam prvků KI a identifikace možného ohrožení funkce prvků KI. Operativní a pomocná část obsahuje opatření a náležitosti na ochranu prvku KI. [34]

4 ANALÝZA RIZIK

Analýza rizik je nejdůležitějším krokem ke snižování a dopadu rizik. Je to proces, který nám stanoví, jak velká je pravděpodobnost, že se hrozba uskuteční a jaký bude mít dopad na aktiva. Jejím úkolem je identifikovat pravděpodobnost nějaké mimořádné události a jejího dopadu. Jakékoliv efektivní řešení problému je založeno na dobře provedené analýze rizik. [35]

4.1 Metody analýzy rizik

Existuje velké množství způsobů, jak získávat data a informace, stejně jako existuje mnoho metod, které lze obecně rozdělit na kvantitativní a kvalitativní metody. Nejdůležitějším faktorem je ale lidská inteligence a všechny metody pouze plní pomocnou roli. Důležitým krokem je výběr vhodné metody analýzy rizik, který závisí na tom, zda:

- *známe nebo můžeme stanovit rozložení živelných pohrom, nehod, havárií, útoků, apod. v prostoru a v čase a můžeme spočítat četnostní rozložení živelných pohrom, nehod, havárií, útoků, apod. (počet vs. velikost) pro určité území a zvolený časový interval, dále vypočítat a zmapovat ohrožení,*
- *známe nebo můžeme stanovit rozložení živelných pohrom, nehod, havárií, útoků, apod., stanovit scénáře dopadů ve variantním provedení a pravděpodobnosti jejich výskytů.*

Níže uvedené metody jsou vhodné pro hledání rizik nebo kritických míst v systému. Je důležité podotknout, že nelze přesně určit, které metody jsou vhodné použít na hledání rizik nebo kritických míst a které nejsou. Výsledek použité metody hledání rizik by měl být každopádně jednoduchý a srozumitelný jak expertům, tak i běžným uživatelům. [36]

.

4.1.1 What – IF Analysis

Jedná se o nesystematickou analytickou metodu, která je určená pro detailní analýzu identifikovaných zdrojů rizik. Orientuje se na prověřování nebezpečných nebo neočekávaných událostí, které se můžou vyskytnout. Výsledkem metody pro každý identifikovaný zdroj rizika je seznam nebezpečných situací, které můžou mít nežádoucí následky. Metoda What-If také poskytuje návrhy ochranných opatření, aby zabránila identifikované nebezpečné situace, nebo aby minimalizovala následky. [37]

4.1.2 Check list (kontrolní seznam)

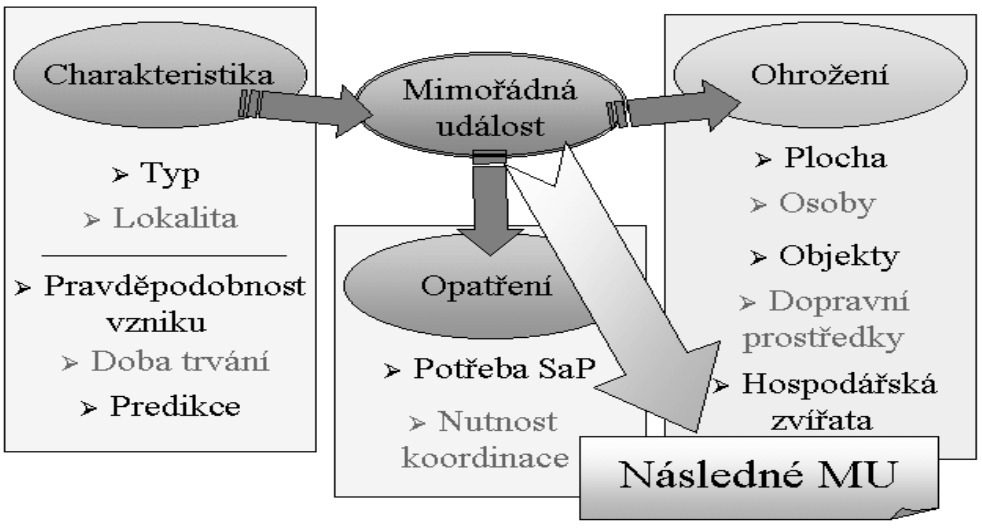
Check list je metoda založená na systematické kontrole plnění stanovených podmínek a opatření, která jsou předem stanovená. Seznamy kontrolních otázek jsou obvykle vytvářeny na základě seznamu charakteristik sledovaného systému nebo činností, které jsou spojeny s potencionálními dopady selhání prvků systému a vznikem škod. Struktura seznamů se může měnit. Je to proměnlivá metoda, která se u nás začíná využívat častěji. [7]

4.1.3 EventTreeAnalysis – ETA (analýza stromu událostí)

Metoda EventTreeAnalysis dohlíží na průběh procesu od začáteční události přes konstruování událostí vždy na základě dvou možností. A to, možnostech příznivých nebo nepříznivých. Je to graficko-statistická metoda, která názorně zobrazuje systémový strom událostí, který poté představuje rozvětvený graf se symbolikou a popisem. Všechny události, které se v posuzovaném systému můžou vyskytnout, jsou znázorněny. Se stoupajícím počtem událostí se výsledný graf rozvětvuje jako větve stromu. Tato analýza se spíše preferuje při složitějších procesech, které mají několik úrovní bezpečnostních systémů. [7]

4.1.4 Metoda expertních odhadů

Účelem metody expertních odhadů je stanovit množiny mimořádných událostí, u kterých se vzhledem k jejich rozsahu a dopadu předpokládá vyhlášení třetího nebo zvláštního stupně poplachu, pro který se zpracovává havarijní plán okresu. Metoda je založena na odhadním stanovení kvantitativních ukazatelů, jež vyplývají z definice jednotlivých stupňů poplachů. Ukazatele se vymezují ve třech základních skupinách – charakteristika, opatření, ohrožení.



Obr. 3. Stanovení kvantitativních ukazatelů [38]

Výpočet míry rizika ze stanovených ukazatelů:

$$Míra\ rizika = \frac{P*(T*10)*((O+S+B+D+C+Z+K)*10)}{Pr*10} \quad (1)$$

P - pravděpodobnost vzniku

T - doba trvání

O - osoby

S - plocha

B- objekty

D- dopravní prostředky

C - hospodářská zvířata

Z - potřeba sil a prostředků

K- nutnost koordinace

Pr- predikce

Kromě ukazatele pravděpodobnosti vzniku se všechny ostatní ukazatele násobí číslem10 z důvodu rozdílného řádu stupnic. [38]

4.1.5 Analýza FMEA

Analýza FMEA (Failure Mode and EffectAnalysis), v českém překladu analýza možných vad a jejich důsledků, se poprvé objevila ve vojenském předpisu, který vznikl v listopadu roku 1949. V tomto stádiu metoda FMEA využívala techniku hodnocení spolehlivosti, a tak bylo možné stanovit dopady poruch systémů a zařízení. Poté se hodnotil vliv na výsledek osob bezpečnost nebo výkonnost zařízení. [2]

Společnost NASA aplikovala tuto myšlenku v 60. letech na projekt Apollo 13 a použila ho jako spolehlivostní analýzu složitých systémů v kosmickém výzkumu. V roce 1977 firma FORD jako první využívá metodu FMEA v automobilovém průmyslu k preventivnímu zajištění kvality vyráběných součástek. FMEA byla kompletně zpracována v 80. letech a to do

papírové normy QS9000. Vývojem procházela 20 let a postupně se zdokonalovala a vyvíjela. Začala se využívat v dalších odvětvích, jako je letecký průmysl, jaderná energetika a dostala se i do popředí netechnických oblastí. V 90. letech se uplatnila například v lékařských oborech. [25,26]

Metoda FMEA se zejména využívá v předvýrobních etapách na preventivní odstranění možných závad a chyb. Zjišťuje nejkritičtější a nejpravděpodobnější chyby ve výrobku či procesu. Dále dokáže rozeznat v různých fázích procesů nebo v návrhu výrobku poruchu, určit její následek, ohodnotit riziko a bezpečně této poruše předejít.

Cílem FMEA je rozbor celého výrobku už v předvýrobní etapě. Zjišťuje poruchy a udává nápravná opatření ve stádiu konstrukce a technické přípravy výroby. Pro každý projev poruchy na nejnižší úrovni se analyzují možné následky.

FMEA se používá v následujících formách:

- FMEA konstrukce
- FMEA procesu
- FMEA výrobku
- FMEA výrobních prostředků [21]

FMEA PROCESU

FMEA procesu se uskutečňuje většinou před zahájením výroby nebo inovací technologického postupu.

Tato metoda je určená pro přezkoumání a validací návrhu technologického postupu, ale je také velmi významnou metodou pro analýzu přezkoumání již používaného postupu, jelikož dokáže odhalit jeho slabá místa a iniciovat jeho zlepšení. Pověřený pracovník zodpovídá za provedení FMEA procesu a předkládá týmu FMEA návrh na technologický postup výroby. Tento postup by měl obsahovat všechny fáze výroby a také po výrobní operace až do okamžiku předání výrobku zákazníkovi.

Celý průběh analýzy je složen ze tří částí a to z Analýzy a hodnocení současného stavu, Návrhu opatření, Hodnocení stavu po opatření. [39,2]

Analýza a hodnocení současného stavu

Jednotlivé operace procesu v pořadí, ve kterém na sebe navazují, se postupně analyzují. Tým má za úkol vymezit možné vady, které se můžou při procesu vyskytnout. Týká se to vad, které se přenesou do konečného výrobku, ale i vad, které způsobí, že některé z operací nebudou

úspěšné. Dále tým analyzuje působnost možných vad na obsluhu procesu. Ke každé vadě, která vznikne, tým analyzuje možné příčiny, které mohly vadu způsobit. Při stanovení možné vady a její příčiny se dále zjišťuje, jaké postupy se v procesu využívají, aby možné vady byly odhaleny.

V případě vzniku vady se u FMEA procesu posuzuje pravděpodobnost, že v průběhu operace vlivem nějaké příčiny vzniknou výrobky s vadou, případně že nastane selhávání procesu. Při odhalení vady tým hodnotí účinnost stávajících kontrolních postupů pro zjištění výskytu možné vady nebo její příčiny předtím, než výrobek nebo součást opustí místo výroby. Rizikové číslo se vypočítá jako součin bodového hodnocení významu vady, pravděpodobnosti výskytu vady a pravděpodobnosti odhalení vady. [40,2]

Závažnost

Číselná hodnota (1 – 10) nám vyjadřuje závažnost důsledku chyby na celý proces. Známku závažnosti může ovlivnit jen změna návrhu. Pro posouzení závažnosti slouží tab. č. 1. [41]

Tab. 1. Navržená kritéria závažnosti metody FMEA [upraveno podle 41]

Důsledek	Kritéria závažnosti důsledku	Známka
Zanedbatelný	Je nepravděpodobné, že by chyba měla negativní dopad na proces.	1
Nepatrný	Vyskytlá chyba je nepatrná.	2 - 3
Středně závažný	Význam chyby je středně závažný, proces může být ohrožen.	4 - 6
Velký	Význam chyby je velký, proces je ohrožen.	7 - 8
Mimořádně závažný	Význam chyby je mimořádně vysoký, je ohrožena bezpečnost.	9 - 10

Výskyt chyby

Výskyt je pravděpodobnost, že se určitá chyba při procesu vyskytne. Vyjadřuje ji číselná hodnota od 1 – 10, která nám určuje pravděpodobnost výskytu příčiny chyby. [41]

Tab. 2. Navržená kritéria výskytu chyby metody FMEA [upraveno podle 41]

Pravděpodobnost chyby	Kritéria výskytu chyby	Známka
Nepravděpodobná	Chyba je skoro vyloučena.	1
Nepatrná	Velmi ojedinělá chyba.	2 - 3
Mála	Chyba se může občas vyskytnout.	4 - 6
Velká	Chyba se vyskytuje často.	7 - 8
Velmi vysoká	Chyba se vyskytuje téměř pořád.	9 - 10

Odhalení chyby

Odhalitelnost je známka, která je přiřazená nejlepším opatřením k odhalení, uvedených ve sloupci opatření k řízení návrhu. Ke snížení hodnocení se musí zlepšit plánované řízení návrhu. Využívá se číselná hodnota 1 – 10, která nám vyjadřuje pravděpodobnost odhalení příčiny vzniku chyby. [41]

Tab. 3. Navržená kritéria odhalení chyby metody FMEA [upraveno podle 41]

Pravděpodobnost odhalení	Kritéria odhalení chyby	Známka
Vysoká	Metody zabezpečení procesu s velkou pravděpodobností odhalí potenciální chybu.	1
Mírná	Metody zabezpečení procesu většinou odhalí potenciální chybu.	2 - 5
Malá	Metody zabezpečení procesu mají pravděpodobnost odhalit potenciální chybu.	6 - 8
Velmi malá	Je velmi malá pravděpodobnost, že metody zabezpečení procesu odhalí potenciální chybu.	9
Nepravděpodobná	Metody zabezpečení procesu nezjistí, nebo nemůžou zjistit potenciální chybu.	10

Ukazatel priority rizika (UPR)

Je to součin závažnosti (Z), výskytu (V) a odhalitelnosti (O).

$$UPR = (Z) \times (V) \times (O) \quad (2)$$

Výsledek UPR :

- 0 – 125 malé riziko,
- 126 – 768 střední riziko,
- 769 – 1000 vysoké riziko. [2]

Návrh opatření

Tým navrhuje opatření pro skupinu možných vad s vyššími hodnotami rizikového čísla, než je zvolena mezní hodnota. Cílem je riziko snížit. Opatřením, které je vhodné v této oblasti, může být zavedení statistické regulace a pravidelné hodnocení způsobilosti procesu. Soubor opatření, který tým navrhl, předává vedoucímu ke schválení a k přidělení odpovědnosti a termínu realizace. [40]

Hodnocení stavu pro realizaci opatření

Po realizaci opatření tým FMEA následně analyzuje, jestli provedená opatření souhlasí s plánovaným opatřením a znovu hodnotí riziko vad, na které byla opatření zaměřena. Po zjištění nových hodnot umožňuje tým posoudit, jak účinná jsou jednotlivá opatření a opětovně může vyčlenit vady s vysokou mírou rizika. Formulář FMEA zaznamenává celý průběh analýzy. [2]

Metodu FMEA procesu budu dále aplikovat v bakalářské práci.

5 ZÁVĚR TEORETICKÉ ČÁSTI

V první kapitole se věnuji historii KI. Z celkového pohledu na historii KI je jasně vidět, že KI se nejvíce prodiskutovávala v období, kdy byla ohrožena lidská společnost. Ať už tomu byla válka, či živelné pohromy. V USA začalo téma ochrany KI silně gradovat po teroristickém útoku 11. září 2001 na Světové obchodní centrum. V ČR se poprvé KI začal zabývat VNCP, který se především věnoval vymezením a definováním pojmů a jednotlivých oblastí KI.

Ve druhé kapitole popisuji základní pojmy, které jsou úzce spjaty s KI. Dále se věnuji oblastem KI. Seznamuji čtenáře také se subjekty a prvky KI a vymezuji podmínky pro jejich určování.

V předposlední kapitole se zabývám rozsáhlým tématem a to ochranou KI a její dokumentací, pod kterou spadají plány krizové připravenosti.

V poslední kapitole popisuji analýzu rizik a metody analýzy rizik, které se využívají v KI. Nejvíce jsem se věnovala metodě FMEA, kterou dále aplikuji v praktické části práce.

6 CÍLE A METODY BAKALÁŘSKÉ PRÁCE

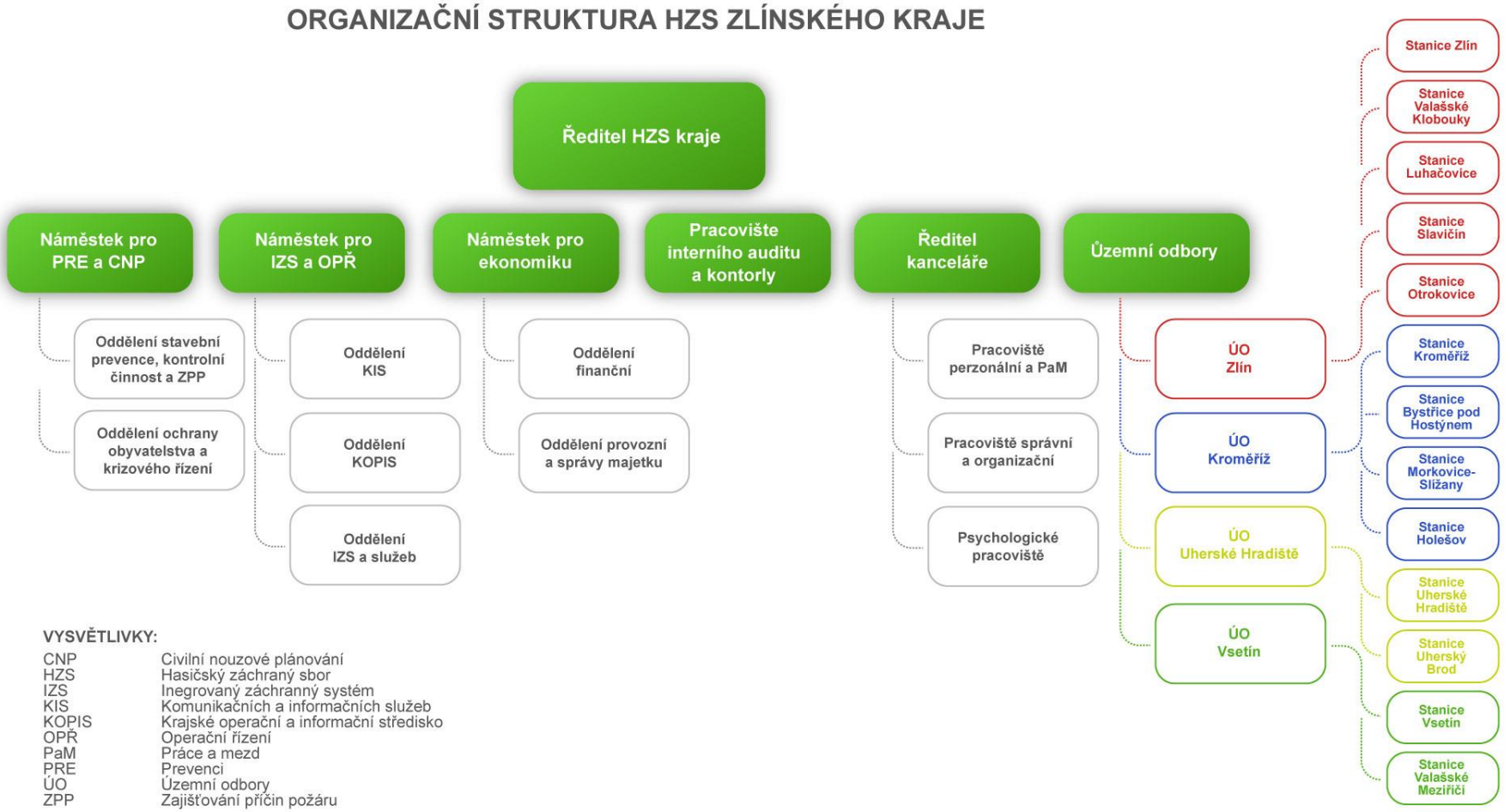
Cílem práce je analýza možného ohrožení prvku KI HZS Luhačovice a hodnocení rizik v daném systému. Pro analýzu bude použita metoda FMEA procesu, která bude analyzovat jednotlivé procesy v rámci činnosti HZS Luhačovice. Následně budou stanovena opatření pro snížení rizik.

II. PRAKTICKÁ ČÁST

7 HASIČSKÝ ZÁCHRANNÝ SBOR ZLÍNSKÉHO KRAJE

HZS Zlínského kraje, organizační složka státu a samostatná účetní jednotka, vznikla dne 1. ledna 2001 na základě zákona *č. 238/2000 Sb. o Hasičském záchranném sboru ČR*. Krajské ředitelství HZS má sídlo ve Zlíně. Organizační strukturu tvoří ředitel HZS, ředitel kanceláře a náměstků, kteří zodpovídají za příslušné oddělení a odbory (viz Obr. 5). Do obecné struktury spadají i územní odbory a to územní odbor Zlín, Kroměříž, Vsetín a Uherské Hradiště. Každý územní odbor má vlastní vedení, které se zodpovídá krajskému ředitelství a jednotlivým stanicím, které pod daný odbor spadají. V mé bakalářské práci se budu zabývat hasičskou stanicí v **Luhačovicích**, která spadá po územní odbor Zlína. [42]

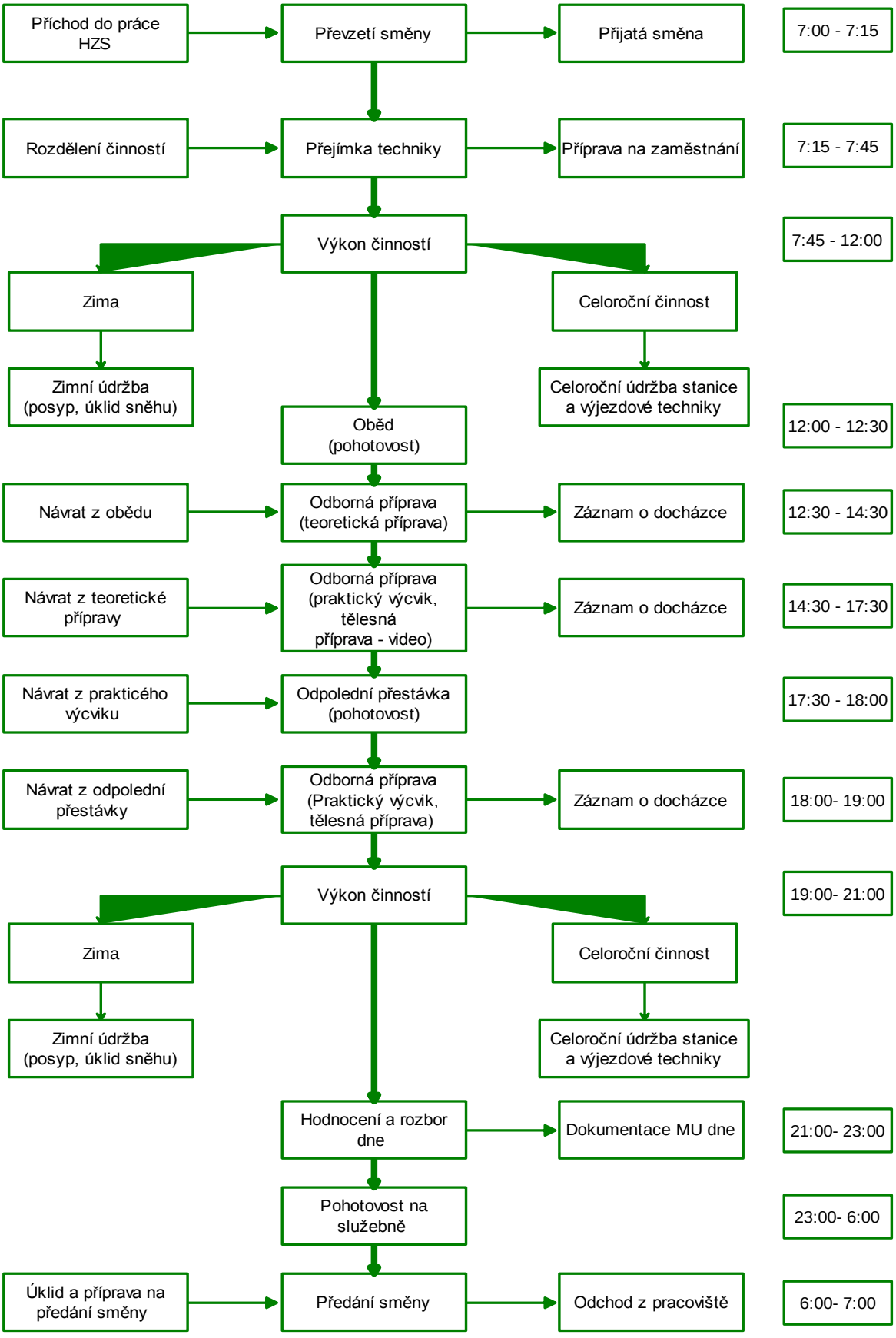
Obr. 4. Hasičská stanice Luhačovice [vlastní]



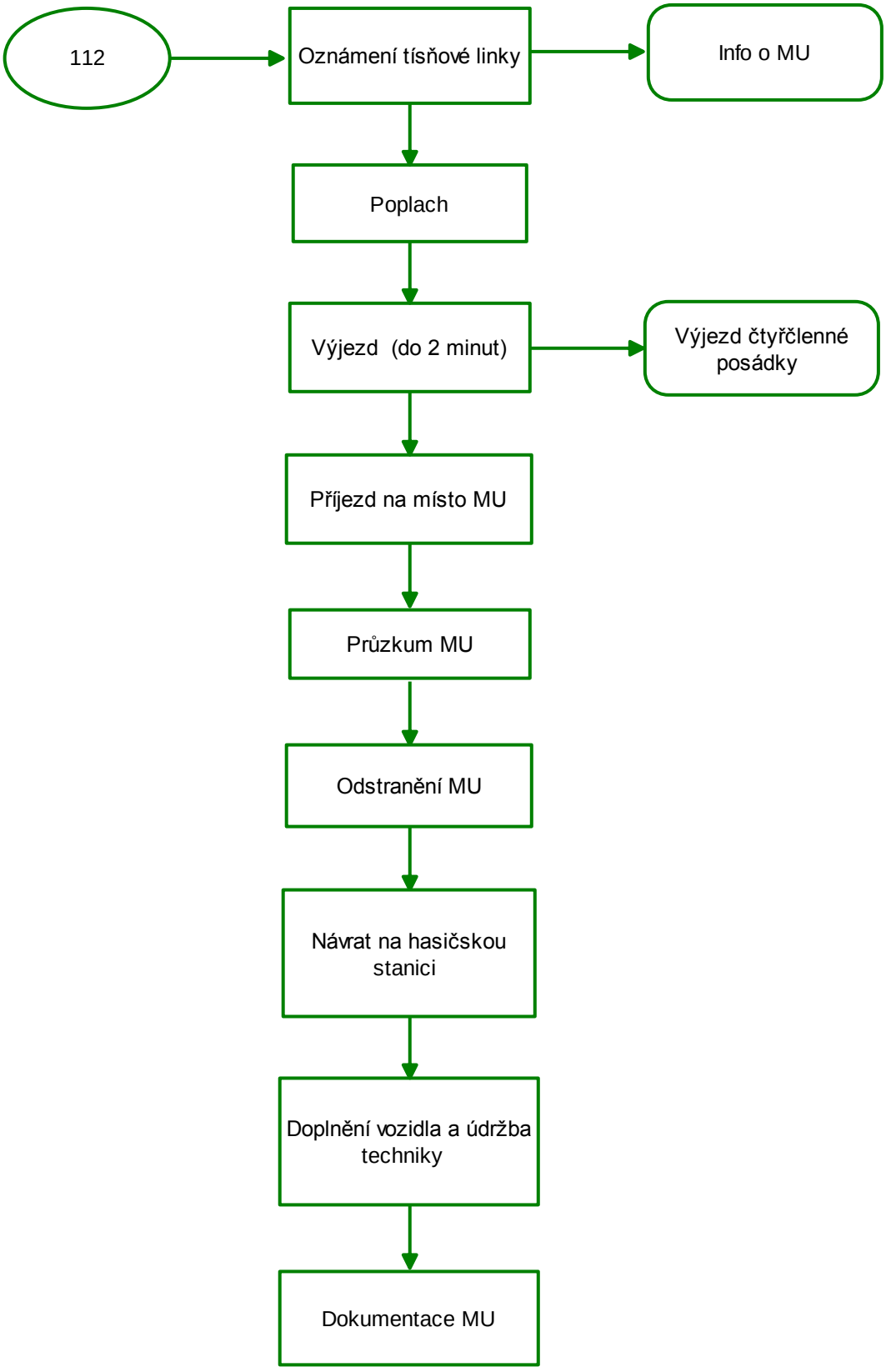
Obr. 5. Organizační struktura HZS Zlínského kraje [upraveno podle 42]

7.1 Prvek kritické infrastruktury - hasičská stanice Luhačovice

Hasičská stanici v Luhačovicích má 15 pracovníků, kteří pracují na tři směny. Podle vyhlášky *č. 247/2001 Sb., o organizaci a činnosti jednotek požární ochrany ve znění vyhlášky č. 226/2005 Sb.* musí být na každé směně 4 – 5 příslušníků. Pracovní směna začíná v 7:00 hod., kdy dochází k převzetí směny a rozdělení činností a přejímky techniky. Dále následuje tzv. zaměstnání, které je specifické jak pro zimní období, tak pro celoroční. V zimě se např. odklízí sníh, posypává výjezdová cesta atd. Celoročně se provádí údržba stanice a výjezdové techniky. Od 12:00 hod. je polední pauza, která trvá 30 minut, ale stále mají všichni příslušníci pohotovost. Kdyby byla nahlášena nějaká mimořádná událost (dále jen MU), jsou povinni i o přestávce do 2 minut od vyhlášení MU vyjet k zásahu. Po pauze následuje odborná příprava a to teoretická i praktická část - video. Tyto výcviky jsou stanoveny na celý rok a vychází ze sbírky interních aktů řízení generálního ředitele HZS ČR. Každý den má každá směna již dopředu stanoveno, co se bude v teoretické i praktické části probírat a co se bude cvičit. Po absolvování výcviku, je každý z příslušníků povinen podepsat záznam o účasti. Dále je na řadě 30 minutová odpolední přestávka na jídlo a odpočinek, který je ale spojen s pohotovostí na stanici. Po přestávce následuje praktický výcvik a tělesná příprava, kde se příslušníci fyzicky připravují v posilovně, přímo na stanici. Následuje tzv. zaměstnání, které je popsáno již výše a v odpoledních hodinách následuje totéž co dopoledne, opět se provádí různé opravy atd. Poté přichází na řadu dokumentace celého dne a rozbor zásahové činnosti. Ve 23:00 hod. začíná pohotovost na služebně, která trvá do ranních 6:00 hod. Dále se provádí úklid a probíhá příprava na předání směny v 7:00 hod. Viz. Obr. 6. [43,44]



Obr. 6. Celodenní činnost příslušníka HZS Luhačovice [vlastní zpracování]



Obr. 7. Zásah při MU [vlastní zpracování]

7.2 Rizika ohrožující Zlínský kraj

Zlínský kraj postihuje nespočet rizik, ovšem deset z nich je považováno za největší a ty můžou způsobit krizovou situaci.

7.2.1 Technologická havárie velkého rozsahu, únik nebezpečných látek, výbuch

Zlínský kraje je obklopen několika organizacemi, které můžou sloužit jako jistý zdroj hrožení s následkem technologické havárie a úniku nebezpečných látek. Podle zákona č. 59/2006 Sb., o prevenci závažných havárií způsobených vybranými nebezpečnými chemickými přípravky jsou tyto firmy zařazeny do skupiny A nebo B.

Dále se zde vyskytují organizace, které do tohoto zákona nespadají, ale přesto mohou způsobit krizovou situaci. Jsou to například zimní stadiony, pivovary, úpravny vody, čerpací stanice atd.

7.2.2 Zranitelnost území

Zranitelnost území se nachází převážně v záplavových oblastech přirozených a zvláštních povodní, kdy většina vodních toků kraje protéká zastavěnými částmi jednotlivých měst a obcí. V zónách havarijního plánování podniků, které spadají do skupiny B dle zákona č. 59/2006 Sb., o prevenci závažných havárií, je koncentrace obyvatelstva vysoká a může se stát, že toto území bude zamořeno a dojde k jeho ohrožení. Další zranitelnost se může vyskytovat v podobě vzniku hromadné nákazy zvířat, protože pásma dozoru jednotlivých velkochovů drůbeže pokrývají téměř celé území kraje.

Při výpočtu zranitelnosti území se nesmí zapomenout na místa, kde se vyskytuje velký počet osob, jako jsou například stadiony, multikina, obchodní centra, která jsou převážně ve velkých městech Zlínského kraje.

7.2.3 Přirozené povodně

Přirozené povodně vznikají v kteroukoliv roční dobu. V zimních a jarních měsících se objevují převážně táním sněhové pokrývky a vydatnými dešťovými srážkami. Poté přirozená povodeň vzniká tzv. ledovými jevy, kdy dochází k ucpání vodního koryta plovoucími ledovými krami.

V letním období vznikají tzv. bouřkové povodně, které způsobují krátkodobé srážky, ovšem s velkou intenzitou. Zasahují ale poměrně malá území. Vyskytují se je většinou na malých tocích, ale mají katastrofální důsledky převážně na vějířovitých povodích.

7.2.4 Zvláštní povodně

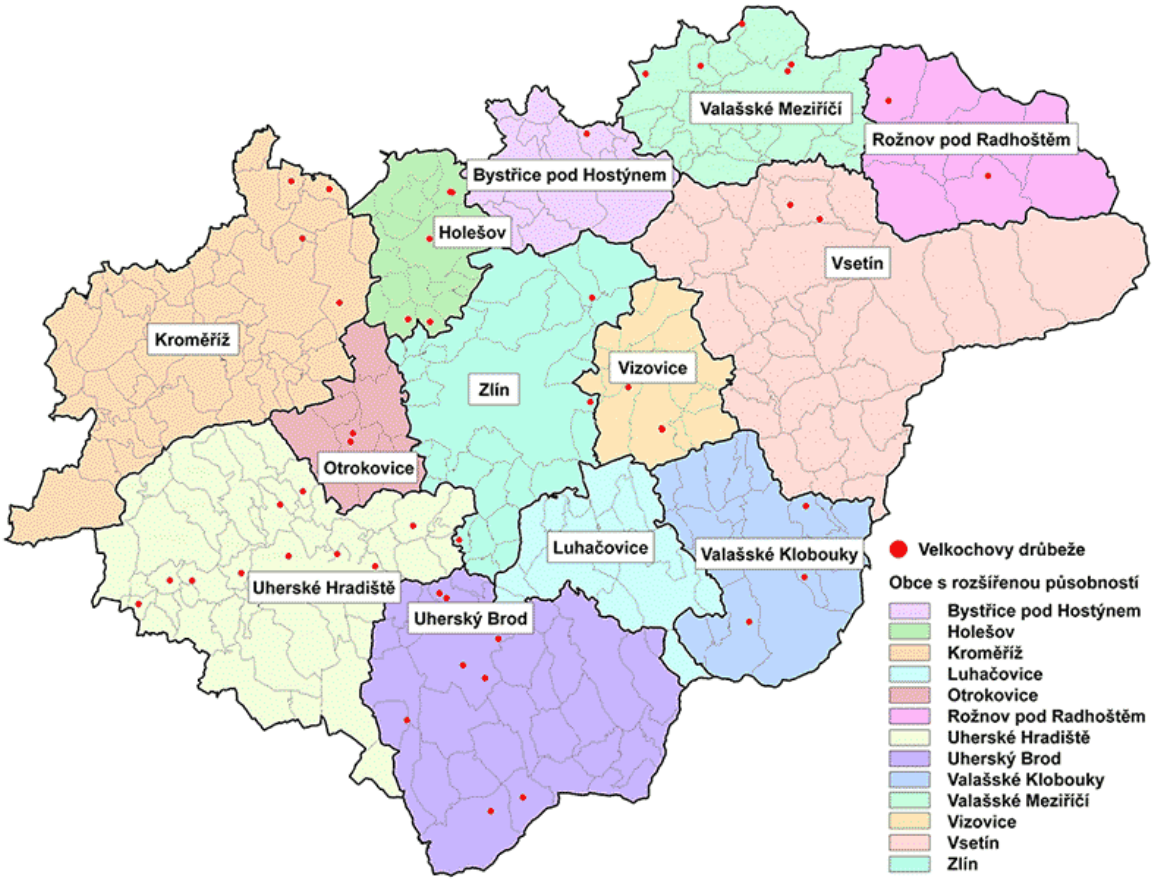
Zvláštní povodeň vzniká poruchou nebo havárií vodního díla. Příčiny vzniku můžou být:

- konstrukční porucha stavebních prvků vodního díla,
- selhání lidského faktoru při provozu vodního díla a technicko bezpečnostního dohledu,
- jinou živelnou pohromou, například sesuvem půdy do vodní nádrže
- diverzní činností (teroristický útok).

Zvláštní povodně jsou typické především rychlým a neočekávaným průběhem a mají rozsáhlé následky na zasaženém území.

7.2.5 Hromadné nákazy zvířat

Vznik epizootie nebo ohrožení zvířat se předpokládá zejména ve velkochovech hospodářských zvířat. Velikost postižení je závislá na druhu nákazy a množství zvířat. Přímé ohrožení populace obyvatel hrozí při antropozoonóze tzv. nemoci přenesené ze zvířete na člověka. V tomto případě lze předpokládat velké škody na živých hospodářských zvířatech a také na surovinách živočišného původu. Nemoc nebo likvidace hospodářských zvířat při vzniku nebezpečné nákazy může vést k haváriím v potravinářských výrobních a zpracovatelských závodech a obchodních sítí, tzn. při zásobování obyvatelstva potravinami.



Obr. 8. Velkochovy drůbeže ve Zlínském kraji [45]

7.2.6 Ostatní živelné pohromy

Zde jsou zařazeny takové jevy, které jsou vyvolány přírodními vlivy a můžou způsobit krizovou situaci. Patří sem například sesuvy půdy, vichřice, krupobití, sněhové kalamity a námrazy. Oblast karpatského flyše leží na území Zlínského kraje a patří do oblasti s vysokým počtem aktivních sesuvných jevů (Hostýnské a Vizovické vrchy, Bílé Karpaty, Chřiby). Příčinou zvýšeného počtu sesuvných jevů je jsou dlouhotrvající intenzivní srážky a podmáčený terén.

V zimních měsících se nejčastěji objevují sněhové kalamity s omezením dodávek elektrické energie převážně v horských oblastech.

7.2.7 Narušení dodávek energií

Pod pojmem narušení dodávek energií rozumíme přerušení distribuce ropy, ropných produktů, elektrické energie, plynu a tepelné energie. Zdrojem vzniku krizové situace může být přerušení distribuční soustavy jednotlivých komodit v důsledku živelných pohrom, technologických havárií, terorismu nebo uvalení embarga. Následek těchto situací může

být ohrožení zdraví lidí, kontaminace potravin, zvýšení rizika požáru, nedostatek pitné vody, narušení infrastruktury a veřejného pořádku. A také je velmi nutno zdůraznit, že dlouhodobý výpadek elektrické energie může mít rozsáhle ekonomické dopady.

7.2.8 Havárie v letecké dopravě

Ve Zlínském kraji se nachází dvě významná letiště a to Kunovicích a Otrokovicích.

Letiště v Kunovicích je veřejné, s mezinárodním provozem a osobní přepravou. Provozní doba je od dubna do září, každý všední den od 8:00 do 16:00, mimo provozní dobu pouze na vyžádání.

Letiště v Otrokovicích je neveřejné, s mezinárodním provozem speciálů, osobní a nákladní přepravou, pouze však na vyžádání 24hod předem.

7.2.9 Havárie v železniční dopravě

Přepravování nebezpečných látek po železnici je upraveno zvláštními právními předpisy, ale i přesto může dojít ke krizové situaci. Ta může být způsobena únikem nebezpečné látky nebo přepravou osob či jiných kombinací.

Nejdůležitější železniční tratě ve Zlínském kraji jsou následující:

- železniční koridor č. 330, Hulín – Staré město u Uherského Hradiště
- trať č. 280, Valašské Meziříčí – Vsetín – Horní Lideč
- trať č. 283, Horní Lideč – Brumov - Bylnice
- trať. 303, Kojetín – Hulín – Valašské Meziříčí
- trať č. 331, Otrokovice – Vizovice
- trať. 341, Kunovice – Bylnice

7.2.10 Havárie v silniční dopravě

Havárie v silniční dopravě může být příčinou krizové situace. Při haváriích na silnici dochází ke zničení komunikace v důsledku živelných pohrom (sesuv půdy, zatopení komunikací), nekontrolovatelnému úniku nebezpečných látek na komunikaci a tím může být ohroženo obyvatelstvo. Při narušení dopravní infrastruktury může dojít k narušení dodávek základních potravin do horských oblastí a dopravní obslužnosti území kraje.

Nejdůležitější komunikace ve Zlínském kraji jsou:

- dálnice D1, Kojetín – Říkovice

- komunikace R55, Hulín – Otrokovice
- komunikace I/34, Valašské Meziříčí – Rožnov pod Radhoštěm – Slovensko
- komunikace I/47, Kroměříž – Hulín – Přerov
- komunikace I/49, Otrokovice – Zlín – Horní Lideč – Slovensko
- komunikace I/50, Uherské Hradiště – Starý Hrozenkov – Slovensko
- komunikace I/54, Boršice u Blatnice – Slovensko
- komunikace I/55, Přerov - Otrokovice – Uherský Ostroh4
- komunikace I/57, Valašské Meziříčí – Vsetín – Brumov Bylnice - Slovensko

Podkladem pro popis rizik ohrožujících Zlínský kraj mi byl interní dokument HZS Zlín.

8 ANALÝZA MOŽNÉHO OHROŽENÍ PRVKU KI

Analýza FMEA procesu nám umožňuje poukázat na rizika, která můžou ohrožovat prvek KI. Tab. č. 4. poukazuje na 24 hodinovou činnost příslušníka HZS Luhačovice a tab. č. 5. na činnosti při výjezdu k MU.

8.1 Analýza a hodnocení současného stavu

8.1.1 Analýza procesu denní činnosti příslušníka HZS Luhačovice

Do první kolonky **Proces/funkce** byly vypsány jednotlivé činnosti příslušníka HZS Luhačovice, tak jak jdou po sobě během 24 hodinové směny.

Poté byly u každého procesu či funkce zaznamenány **Možné chyby**, které byly navrženy a které by se při daném procesu mohly vyskytnout. Platí, že se vyhodnocují i vady, které nejsou na první pohled významné a vyskytují se jen zřídka. Při procesu převzetí směny je to nemoc příslušníka, u přejímky techniky její poškození či nefunkčnost, při údržbě stanice výpadek elektrické energie či zranění příslušníka. U teoretické či praktické přípravy je to situace, kdy příslušník nepochopí probírané téma, při tělesné přípravě, může dojít ke zranění příslušníka, při údržbě venkovního areálu může opět dojít ke zranění příslušníka, nebo nefunkčnosti výjezdových vrat, dále při pohotovosti na směně může dojít k poruše sirén a při úklidu může nastat porucha techniky.

Dalším krokem je **Možný následek chyby**, zde jsou určeny jednotlivé možné následky, k nimž by vyústil vznik možné chyby. Je to například menší počet příslušníků na směně, nevyjetí výjezdové techniky k MU atd.

V další fázi jsou jednotlivé následky chyb oklasifikovány v kolonce **Význam,** hodnotami 1 – 10 (tab. č. 1.), kdy hodnota 1 znamená zanedbatelný následek, ale na druhé straně hodnota 9 – 10 velmi závažný následek. Jednotlivé následky jsou oklasifikovány, kdy např. nevyhlášení poplachu je hodnoceno osmičkou, naopak nepochopení probíraného tématu v praktické části je hodnoceno čtverkou.

Další položkou jsou **Možné příčiny chyby**. Zde se detekují všechny příčiny, které mají vliv na možný vznik chyby. Při převzetí směny je to nemoc příslušníka, při přejímce techniky špatné zacházení či poškození techniky při zásahu. Dále při údržbě stanice je příčinou výpadek elektrické energie či zranění příslušníka. U teoretické či praktické přípravy dochází k nepozornosti příslušníka a u tělesné přípravy k nedbalosti. Při údržbě venkovního

areálu, kdy možnou příčinou zranění příslušníka je jeho nepozornost. Také může dojít k poruše výjezdových vrat se starými zámky. Poruchu sirén má na svědomí výpadek elektrické energie a poruchu techniky její poškození.

Dalším krokem je určení **Výskytu** dané chyby, který je klasifikován od 1 – 10 přičemž jednička je nepravděpodobný výskyt chyby a 9 – 10 je velmi vysoký výskyt chyby. Viz. tab. č. 2.

Poté následuje vypsání všech **Stávajících opatření pro prevenci** a to jsou metody, jejichž vhodným užitím dochází ke snížení pravděpodobnosti výskytu chyby.

V kolonce **Stávající řízení procesu** se uvádí veškeré kontrolní mechanismy, které mohou výskyt chyby odhalit již během procesu nebo v co nejkratší době po jeho ukončení. V tomto případě je to u procesu převzetí směny zpráva, kterou musí příslušník zaslat před nástupem do práce, např. že je nemocný atd. Při přejímce techniky je to zkouška její funkčnosti. Dále při údržbě stanice může dojít už k zmíněnému výpadku elektrické energie, proto je povinná kontrola elektrické energie na počátku směny. Při zranění příslušníka se kontrolují ochranné osobní prostředky. Ve fázi teoretické a praktické části, kdy nepochopí příslušník probírané téma, je možnost konzultace daného tématu s přednášejícím. Při poruše výjezdových vrat je stávajícím řízením kontrola zámků jednou za půl roku a při poruše sirén je to kontrola na počátku směny. V poslední fázi může opět dojít k poruše techniky, kde k odhalení chyby může dojít při zkoušce funkčnosti.

Odhalitelnost velká nebo malá je pravděpodobnost odhalení chyby během procesu. Přičemž jednička stanovuje, že odhalitelnost je velká, naopak 10 stanovuje nepravděpodobné odhalení chyby během procesu. Viz. tab. č. 3.

Hodnota **rizikového čísla** je součin významu, výskytu a odhalitelnosti. Určení rizikového čísla je detailně popsané v teoretické části práce.

Tímto momentem byla ukončena fáze posouzení současného stavu procesu a jeho vyhodnocení. Byly odhaleny vzniklé chyby. U chyb s číslem vyšším než 125 bylo vypracováno **doporučené opatření.** U nemoci příslušníka byla navržena jeho zastupitelnost, dále byla navržena kontrola techniky po zásahu a konci směny. Vyšší rizikové číslo vyšlo také u výpadku elektrické energie a s tím spojenou i poruchou sirén, kde byl navržen náhradní zdroj elektrické energie. Vůbec nejvyšší číslo vyšlo u poruchy výjezdových vrat, kde byla navržena častější kontrola zámků. Tedy bylo dosaženo cíle, který byl stanoven.

Po stanovení doporučených opatření byl stanoven **Odpovědný pracovník**, který navržené změny provede. V našem případě je to ve všech fázích velitel.

Posledním krokem metody FMEA je zhodnocení přínosu provedených opatření. Zhodnocení bylo provedeno tak, že byl opět klasifikován Výskyt, Význam, Odhalitelnost a znovu se stanovila hodnota Rizikového čísla, u něhož došlo vlivem provedených změn k snížení pod hodnotu 125, čili pod míru rizika a tímto krokem byla metoda FMEA ukončena.

Tab. 4. FMEA procesu denní činnosti příslušníka HZS Luhačovice [vlastní zpracování]

Funkce, proces	Možná chyba	Možné následky chyby	Význam	Možná příčina chyby	Výskyt	Stávající opatření (prevence)	Stávající řízení procesu (odhalování)	Odhalitelnost	Rizikové číslo	Doporučené opatření	Odpovědnost	Význam	Výskyt	Odhalitelnost	Rizikové číslo
Převzetí směny	Nemoc příslušníka	Menší počet příslušníků na směně	7	Přepracovanost, infekce	6	Žádné	Zpráva před nástupem do práce	3	**126**	Zastupitelnost	Velitel	7	6	2	**84**
Přejímka techniky	Poškození	Nepoužitelnost	8	Špatné zacházení	6	Žádné	Zkouška funkčnosti	3	**144**	Kontrola na konci směny	Velitel	8	6	2	**96**
	Nefunkční	Nepoužitelnost	8	Poškození při zásahu	6	Žádné	Zkouška funkčnosti	3	**144**	Kontrola po zásahu	Velitel	8	6	2	**96**
Údržba stanice	Výpadek elek. energie	Nevyhlášení poplachu	9	Odstávka elek. energie	3	Žádné	Kontrola na počátku směny	6	**162**	Náhradní zdroj elek. energie	Velitel	9	3	2	**54**
	Zranění příslušníka	Menší počet příslušníků při výjezdu	5	Nedbalost příslušníka	5	Žádné	Kontrola ochranných osobních prostředků	4	100	Beze změn		5	5	4	100

Teoretická příprava	Nepochopení probírajícího tématu	Špatná využitelnost v praxi	4	Nepozornost příslušníka	4	Žádné	Možnost konzultace s přednášejí-cím	5	80	Beze změn		4	4	5	80
Praktická příprava	Nepochopení probírajícího tématu	Špatná využitelnost v praxi	4	Nepozornost příslušníka	4	Žádné	Možnost konzultace s přednášejícím	5	80	Beze změn		4	4	5	80
Tělesná příprava	Zranění příslušníka	Menší počet příslušníků na směně	5	Nedbalost	5	Žádné	Kontrola ochranných osobních prostředků	4	100	Beze změn		5	5	4	100
Údržba venkovního areálu	Zranění příslušníka	Menší počet příslušníků na směně	5	Nepozornost příslušníka	5	Žádné	Kontrola ochranných osobních prostředků	4	100	Beze změn		5	5	4	100
	Porucha výjezdových vrat	Nevyjetí výjezdové techniky k MU	9	Staré zámky ve vratech	3	Žádné	Kontrola jednou za půl roku	7	**189**	Častější kontrola zámků	Velitel	9	3	2	**54**
Pohotovost na služebně	Porucha sirén	Nevyjetí výjezdové techniky k MU	9	Výpadek elek. energie	3	Žádné	Kontrola na počátku směny	6	**162**	Náhradní zdroj el. energie	Velitel	9	3	2	**54**
Úklid a předání směny	Porucha techniky	Nepoužitelnost	8	Poškození	6	Žádné	Zkouška funkčnosti	3	**144**	Kontrola na konci směny	Velitel	8	6	2	**96**

8.1.2 Analýza současného stavu při výjezdu k MU

Jak již bylo výše popsáno, Zlínský kraj ohrožuje nespočet rizik. Avšak deset z nich je vyhodnoceno jako největší. Výjezd HZS k těmto MU je prakticky vždy podobný. Tab. č. 5. nám pomocí metody FMEA procesu vyhodnocuje rizika, která můžou nastat po dobu celého výjezdu HZS Luhačovice.

Proces/funkce - zde byly vypsány jednotlivé procesy při výjezdu HZS Luhačovice k MU.

Možné chyby – chybu u oznámení tísňové linky je výpadek elektrické energie, dále u vyhlášení poplachu může jít o planý. Při výjezdu posádky může dojít k nefunkčnosti výjezdové techniky či zranění příslušníka. Příjezd na místo MU ovlivní na příklad nehoda posádky. U průzkumu MU může opět dojít k zranění příslušníka. Po odstranění MU jsou jako chyby vyhodnoceny tyto aspekty: poškození vodní, hasicí a výjezdové techniky a otrávení příslušníka nebezpečnou chemickou látkou. Dalším aspektem je nehoda při návratu posádky. Při doplnění vozidla a údržbě techniky je jako chyba vyhodnoceno poškození hasící techniky či nedoplnění materiálu. Poslední fáze je dokumentace MU, kde může nastat její neaktuálnost.

Možný následek chyby – jsou to následky, které můžou nastat, pokud by se chyba objevila. Je to např. výjezd méně členné posádky, nebo dokonce žádný výjezd. Dále by mohlo dojít k neodstranění MU apod.

Možná příčina chyby – u výpadku elektrické energie je možnou příčinou chyby odstávka elektrické energie, u planého poplachu legrace dětí a nefunkčnost výjezdové techniky může být způsobena špatným zacházením. Možnou příčinou zranění příslušníka je jeho nedbalost a nehodu může zavinit řidič výjezdové techniky. Při poškození vodní, hasící či výjezdové techniky může být možná příčina chyby špatná kontrola nebo špatné zacházení s touto technikou. Příčinou otrávení příslušníka nebezpečnou chemickou látkou mohou být špatné osobní ochranné prostředky. Při nedoplnění vozidla nemůže být vozidlo zařazeno do výjezdu a za neaktuálností dokumentace MU může stát špatná aktualizace.

Stávajících opatření pro prevenci - jsou metody, jejichž vhodným užitím dochází ke snížení pravděpodobnosti výskytu chyby.

Stávající řízení procesu – veškeré kontrolní mechanismy, které mohou výskyt chyby odhalit již během procesu nebo v co nejkratší době po jeho ukončení. V tomto případě je to u oznámení tísňové linky výpadek elektrické energie, kde odhalitelnost je určena kontrolou

na počátku směny. Při vyhlášení planého poplachu je stávajícím řízením ověření totožnosti volajícího. U nefunkčnosti výjezdové techniky je to zkouška funkčnosti a při zranění nebo otrávení příslušníka nebezpečnou chemickou látkou je to kontrola ochranných osobních prostředků, u nehody následují psychologické testy či školení řidičů. V další fázi poškození vodní, hasící či výjezdové techniky je to běžná kontrola, kontrola na začátku a konci směny nebo školení obsluhy. Stávajícím řízením při nedostatku materiálu je kontrola množství materiálu a v poslední fázi při neaktuálnosti dokumentace MU je to její kontrola.

Význam, Výskyt, Odhalitelnost a Rizikové číslo – tyto čtyři aspekty jsou podrobně popsány v analýze procesu denní činnosti příslušníka HZS Luhačovice a při procesu výjezdu MU se hodnotí zcela stejně.

Tímto momentem byla ukončena fáze posouzení současného stavu procesu a jeho vyhodnocení. Byly odhaleny vzniklé chyby. U chyb s číslem vyšším než 125 bylo vypracováno **doporučené opatření**. U výpadku elektrické energie byl navržen náhradní zdroj elektrické energie. Vyšší rizikové číslo vyšlo u vyhlášení planého poplachu, kde byla navržena archivace telefonních čísel. Při nefunkčnosti výjezdové techniky byla doporučena její kontrola na konci i počátku směny. Vůbec nejvyšší rizikové číslo vyšlo u nehody posádky k MU, kde byla navržena zastupitelnost. Dále při odstraňování MU, kdy dojde k poškození vodní techniky, bylo navrženo zajištění náhradního člunu a u poškození hasící techniky zajištění náhradní hasící techniky. Poslední dvě doporučení byla stanovena u poškození výjezdové techniky. Zde bylo navrženo prověření znalostí obsluhy a při poškození hasící techniky při údržbě byl navržen servis.

Po stanovení doporučených opatření byl stanoven **Odpovědný pracovník**, který navržené změny provede. Je jím velitel a v jednom případě operační důstojník.

Posledním krokem metody FMEA bylo opět zhodnocení přínosu u provedených opatření. Zhodnocení bylo provedeno tak, že se u nich opět klasifikoval Výskyt, Význam, Odhalitelnost a znovu se stanovila hodnota Rizikového čísla, u něhož došlo vlivem provedených změn k snížení pod hodnotu 125, tzn. pod míru rizika. Tímto krokem byla metoda FMEA ukončena.

Tab. 5. FMEA procesu při výjezdu k MU [vlastní zpracování]

Funkce, proces	Možná chyba	Možné následky chyby	Význam	Možná příčina chyby	Výskyt	Stávající opatření (prevence)	Stávající řízení procesu (odhalování)	Odhalitelnost	Rizikové číslo	Doporučené opatření	Odpovědnost	Význam	Výskyt	Odhalitelnost	Rizikové číslo
Oznámení tísňové linky	Výpadek elek. energie	Nevyjetí k MU	9	Odstávka elek. energie	3	Žádné	Kontrola na počátku směny	6	**162**	Náhradní zdroj elek. energie	Velitel	9	3	2	**54**
Vyhlášení poplachu	Planý poplach	Výjezd posádky	9	Legrace dětí	4	Žádné	Ověření totožnosti volajícího	6	**216**	Archivace tel. čísla	Operační důstojník	9	4	2	**72**
Výjezd čtyř-členné posádky k MU	Nefunkčnost výjezdové techniky	Nevyjetí k MU	8	Špatné zacházení	6	Žádné	Zkouška funkč-nosti	3	**144**	Kontrola na konci i začátku směny	Velitel	8	6	2	**96**
	Zranění příslušníka	Výjezd méně členné posádky	5	Nedbalost pracovníka	5	Žádné	Kontrola ochranných prostředků	4	100	Beze změn		5	5	4	100
Příjezd na místo MU	Nehoda	Nepřijetí k MU	9	Neopatrnost řidiče výjezdové techniky	4	Žádné	Psychologické testy	8	**288**	Zastupitelnost	Velitel	9	4	2	**72**
Průzkum MU	Zranění příslušníka	Průzkum méně členné posádky	5	Nedbalost pracovníka	5	Žádné	Kontrola ochranných osobních prostředků	4	100	Beze změn		5	5	4	100
Odstranění MU	Poškození vodní techniky	Neodstranění MU	8	Špatná kontrola vodní techniky	4	Žádné	Běžná kontrola	4	**128**	Zajištění náhradního člunu	Velitel	8	4	2	**64**

	Otrávení příslušníka nebezpečnou chem. látkou	Nedokončení zásahu	6	Špatné osobní ochranné prostředky	3	Žádné	Kontrola osobních ochranných prostředků	3	54	Beze změn		6	3	3	54
	Poškozená hasící techniky	Neodstranění MU	8	Špatné kontrola hasící techniky	4	Žádné	Kontrola hasící techniky na začátku a konci směny	4	**128**	Náhradní hasící technika	Velitel	8	4	2	**64**
	Poškození výjezdové techniky	Neodstranění MU	8	Špatné zacházení s výjezdovou technikou	6	Žádné	Školení obsluhy	3	**144**	Prověření znalosti obsluhy	Velitel	8	6	1	**48**
Návrat na hasičskou stanici	Nehoda	Zranění posádky	6	Nepozornost	3	Žádné	Školení řidičů	3	54	Beze změn		6	3	3	54
Doplnění vozidla a údržba techniky	Nedostatek materiálu	Nedoplnění vozidla	7	Nemožnost zařazení do výjezdu	3	Žádné	Kontrola množství materiálu	2	42	Beze změn		7	3	2	42
	Poškození hasící techniky	Nefunkčnost	7	Poškození zařízení	5	Žádné	Zkouška funkčnosti	4	**140**	Zajištění servisu	Velitel	7	5	2	**70**
Dokumentace MU	Neaktuálnost	Nemožnost zásahu	7	Špatná aktualizace	3	Žádné	Kontrola	3	63	Beze změn		7	3	3	63

ZÁVĚR

Cílem mé bakalářské práce bylo analyzovat zdroje rizik možného ohrožení prvku KI. Jako prvek KI jsem si vybrala hasičskou stanici v Luhačovicích. Jedním z aspektů bylo to, že hasičské stanice se staly prvkem KI v roce 2015, proto je toto téma velmi aktuální.

Po obeznámení čtenáře s historií kritické infrastruktury a základními pojmy daného tématu jsem se věnovala ochraně kritické infrastruktury a analýze rizik. V analýze rizik popisuji jednu z metod, přesněji metodu FMEA, kterou dále aplikuji v praktické části.

V praktické části jsem nejprve popsala hasičskou stanici v Luhačovicích a denní řád příslušníka na směně, který jsem dále analyzovala. Snažila jsem se vystihnout veškeré zdroje rizik, které můžou ohrožovat prvek kritické infrastruktury během 24 hodinové směny. Podklady k vypracování FMEA procesu mi byly poskytnuty přímo na hasičské stanici v Luhačovicích. Chyby, které mají určitý vliv na správný chod prvku kritické infrastruktury a kde stávající řízení s velkou pravděpodobností tuto chybu ani neodhalí, tak bylo navrhnuto doporučené opatření, které rizikové číslo analýzy výrazně snížilo

Dále jsem se zabývala deseti největšími riziky, která ohrožují Zlínský kraj včetně hasičské stanice v Luhačovicích a analyzovala jsem možné chyby, které se můžou vyskytnout při výjezdu k těmto mimořádným událostem. Opět jsem pomocí metody FMEA sestavila tabulku a veškeré dostupné údaje jsem do ní zařadila. U vysokých rizikových čísel, které v analýze vyšly, jsem navrhla doporučená opatření. A tím jsem **cíl** mé **bakalářské práce splnila**.

Na závěr práce bych chtěla podotknout, že problematika ochrany kritické infrastruktury je velmi rozsáhlá a složitá a zasloužila by si podstatně větší pozornost než jakou v současné době má. Nestačí, aby se problematice věnovalo jen pár odborníků, ale měla by se dostat do podvědomí co největšího počtu obyvatel.

SEZNAM POUŽITÉ LITERATURY

[1] ŘEHÁK, David. *Kritická infrastruktura elektroenergetiky: určování, posuzování ochrana*. 1. vyd. V Ostravě: Sdružení požárního a bezpečnostního inženýrství, 2013, 79 s. Spektrum (Sdružení požárního a bezpečnostního inženýrství). ISBN 978-80-7385-126-2

[2] ZEMAN, Martin: Zavedení metody FMEA do podniku StöriMantel s.r.o. *Diplomová práce: Univerzita Tomáše Bati ve Zlíně, Fakulta technologická* [online]. [cit. 2016-04-23]. Dostupné z: http://digilib.k.utb.cz/bitstream/handle/10563/11911/zeman_2010_dp.pdf?sequence=1

[3] TheWhite House. PresidentalDecisionDirective 63 [on-line]. 1998 [cit. 2016-02-03]. Dostupný z: WWW: <http://fas.org/irp/offdocs/pdd/pdd-63.htm>.

[4] Časopis 112 ROČNÍK II ČÍSLO 1/2013. *Hasičský záchranný sbor ČR* [online]. [cit. 2016-05-08]. Dostupné z: Dostupné z:http://www.hzscr.cz/soubory/casopis_112_rok_2003.pdf

[5] HROMADA, Martin. *Systém a způsob hodnocení odolnosti kritické infrastruktury*.1.vyd. V Ostravě: Sdružení požárního a bezpečnostního inženýrství, 2013, 177 s. ISBN 978-80-7385-140-8.

[6] ŘÍHA, Josef. *Typologické znaky kritické infrastruktury* [online]. [cit. 2016-04-23]. Dostupné z: http://www.population-protection.eu/prilohy/casopis/6/43.pdf

[7] ŠENOVSKÝ, Michail, Vilém ADAMEC a Pavel ŠENOVSKÝ. *Ochrana kritické infrastruktury*. 1. vyd. V Ostravě: Sdružení požárního a bezpečnostního inženýrství, 2007,141 s. Spektrum (Sdružení požárního a bezpečnostního inženýrství). ISBN 978-80-7385-025-8.

[8] MOZGA, Jaroslav, Miloš VÍTEK a František KOVÁŘÍK. *Kritická infrastruktura společnosti*. Vyd. 1. Hradec Králové: Gaudeamus, 2008, 156 s. ISBN 978-80-7041-299-2.

[9] Komise evropských společenství. *Zelená kniha o evropském programu na ochranu kritické infrastruktury* [online]. [cit. 2016-02-03]. Dostupné z:

http://krizport.firebrno.cz/dokumenty/zelena-kniha-o-evropskem-programu-na-ochranu-kritické-infrastruktury

[10] Směrnice Rady 2008/114/ES, o určování a označování evropských kritických infrastruktur a o posouzení potřeby zvýšit jejich ochranu

[11] Evropský program na ochranu kritické infrastruktury. *Hasičský záchranný sbor ČR* [online]. [cit. 2016-02-04]. Dostupné z: http://www.hzscr.cz/clanek/evropsky-program-na-ochranu-kriticke-infrastruktury-european-programme-for-critical-infrastructure-protection.aspx

[12] Výbor pro civilní nouzové plánování. *Vláda České republiky* [online]. [cit. 2016-02-04]. Dostupné z: http://www.vlada.cz/cz/ppov/brs/pracovni vybory/civilni-nouzove-planovani/13] vybor-pro-civilni-nouzove-planovani-109279/

[13] Zpráva o stavu zajištění bezpečnosti České republiky v oblasti ochrany před mimořádnými událostmi. *Vláda České republiky* [online]. [cit. 2016-02-04]. Dostupné z: http://www.vlada.cz/assets/ppov/brs/dokumenty/Zprava.pdf

[14] LINHART, Petr. *Krizový management: kombinovaná forma studia*. Vyd. 1. Pardubice: Univerzita Pardubice, 2004, 97 s. ISBN 80-719-4674-5.

[15] HEJDOVÁ, Jaroslava, Anna ŠEBKOVÁ. *Současnost a budoucnost kritické infrastruktury ve zdravotnictví*[online]. [cit. 2016-04-23]. Dostupné z: http://www.unbr.cz/Data/files/Konf%20MeKa09/07_Hejdov%C3%A1.pdf

[16] ČESKO. Zákon č. 240/2000 Sb., o krizovém řízení a o změně některých zákonů (krizový zákon). In Sbírka zákonů ČR, ročník 2000, částka 73. Dostupné na: <http://www.zakonyprolidi.cz/cs/2000-240> [cit. 2016-01-01]. ISSN 1211-1244

[17] Koncepce ochrany obyvatelstva do roku 2013 s výhledem do roku 2020. *Hasičský záchranný sbor ČR*[online]. [cit. 2016-05-08]. Dostupné z: http://www.hzscr.cz/clanek/koncepce-ochrany-obyvatelstva-do-roku-2013-s-vyhledem-do-roku-2020-503181.aspx

[18] PROCHÁZKOVÁ, Dana. *Bezpečnost kritické infrastruktury*. Praha: České vysoké učení technické v Praze, 2012, 318 s. ISBN 978-80-01-05103-0.

[19] LINHART, Jiří. *Slovník cizích slov pro nové století: základní měnové jednotky: abecední seznam chemických prvků: jazykovědné pojmy: 30000 hesel*. Litvínov:

Dialog, 2007, 412 s. ISBN 80-738-2005-6.

[20] Kritická infrastruktura. *Ministerstvo vnitra ČR* [online]. [cit. 2016-05-08]. Dostupné z: http://www.mvcr.cz/clanek/pojmy-kriticka-infrastruktura.aspx

[21] FMEA analýza příčin a důsledků. *Svět produktivity* [online]. [cit. 2016-04-23]. Dostupné z: http://www.svetproduktivity.cz/slovnik/FMEA-Analyza-pricin-a-dusledku.htm

[22] Mimořádná událost. *Ministerstvo vnitra ČR* [online]. [cit. 2016-05-08]. Dostupné z: http://www.mvcr.cz/clanek/mimoradna-udalost-851851.aspx

[23] KRAUS, Jiří. *Nový akademický slovník cizích slov A-Ž*. Vyd. 1. Praha: Academia, 2005, 879 s. ISBN 80-200-1351-2

[24] ČESKO. Nařízení vlády č. 432/2010 Sb., o kritériích pro určení prvku kritické in frastruktury. In Sbírka zákonů ČR, ročník 2010, částka 149. Dostupné na: <http://www.zakonyprolidi.cz/cs/2010-432> [cit. 2015-01-01]. ISSN 1211-1244

[25] NENADÁL, Jaroslav. *Moderní systémy řízení jakosti: quality management*. Vyd. 1. Praha: Management Press, 1998. ISBN 80-859-4363-8.

[26] VESELÝ, Milan. Použití metody FMEA pro prevenci chyb v průmyslovém podniku. *Diplomová práce: VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ* [online]. [cit. 2016-04-23]. Dostupné z: https://www.vutbr.cz/www_base/zav_prace_soubor_verejne.php?file_id=52063

[27] Krizové řízení při nevojenských krizových situacích. *Hasičský záchranný sbor České republiky* [online]. [cit. 2016-02-04]. Dostupné z: www.hzscr.cz/../modul-c-krizove-rizeni-pri-nevojenskych-krizovych- situacich-pdf.aspx

[28] Časopis 112 ROČNÍK XI ČÍSLO 10/2012. *Hasičský záchranný sbor České republiky* [online]. [cit. 2016-02-04]. Dostupné z:http://www.hzscr.cz/clanek/informacni-servis-casopis-112-2012-casopis-112-rocnik-xi-cislo-10-2012.aspx?q=Y2hudW09NQ%3D%3D

[29] Časopis 112 ROČNÍK XIV ČÍSLO 2/2015. *Hasičský záchranný sbor České republiky* [online]. [cit. 2016-02-04]. Dostupné z:http://www.hzscr.cz/clanek/casopis-112-rocnik-xiv-cislo-2-2015.aspx?q=Y2hudW09NA%3D%3D

[30] ŠTOREK, Josef: Kritická infrastruktura zdravotnictví ano či ne ? *Katedra radiologie a toxikologie, ZSF JCU, České Budějovice* [online]. [cit. 2016-04-23]. Dostupné z: http://www.zsa.cz/katastrofy2011/storek.pdf

[31] DVOŘÁKOVÁ, Kateřina: Ochrana prvků kritické infrastruktury v Evropské unii. *Bakalářská práce: Univerzita Pardubice* [online]. [cit. 2016-04-23]. Dostupné z: https://dk.upce.cz/bitstream/handle/10195/52450/DvorakovaK_OchranaPrvku_OS_2013.pdf?sequence=2&isAllowed=y

[32] *Kritická infrastruktura a její postavení v rámci bezpečnostního systému ČR* [online]. [cit. 2016-02-04]. Dostupné z: https://sis.polac.cz/predmety/index.php?do=down&did=3406

[33] PROCHÁZKOVÁ, Dana a Josef ŘÍHA. *Krizové řízení*. Ministerstvo vnitra - generální ředitelství Hasičského záchranného sboru ČR, 2004. Praga. ISBN 80-86640-30-2.

[34] ČESKO. Nařízení vlády č. 462/2000 Sb., k provedení § 27 odst. 8 a § 28 odst. 5 zákona č. 240/2000 Sb., o krizovém řízení a o změně některých zákonů (krizový zákon). In Sbírka zákonů ČR, ročník 2000, částka 132. Dostupné na: <http://www.zakonyprolidi.cz/cs/2000-462> [cit. 2011-01-01]. ISSN 1211-1244

[35] SMEJKAL, Vladimír a Karel RAIS. *Řízení rizik ve firmách a jiných organizacích*. 3., rozš. a aktualiz. vyd. Praha: Grada, 2010, 354 s. Expert (Grada). ISBN 978-80-247-3051-6

[36] Kritická infrastruktura a její ochrana. *Hasičský záchranný sbor* [online]. [cit. 2016-02-04]. Dostupné z: http://www.hzscr.cz/clanek/kriticka-infrastruktura-a-jeji-ochrana.aspx

[37] MARADA, Vojtěch: Porovnání metod analýzy rizik závažných havárií. *Bakalářská práce: VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ* [online]. [cit. 2016-04-23]. Dostupné z: https://www.vutbr.cz/www_base/zav_prace_soubor_verejne.php?file_id=52944

[38] KROMER, Antonín, Marek SMETANA: Analýza vzniku mimořádných událostí v rámci havarijního plánování metodou expertních odhadů: Publikační činnost odboru ochrany obyvatelstva a krizového řízení. *Hasičský záchranný sbor Moravsko-slezského kraje* [online]. [cit. 2016-04-23]. Dostupné z: http://hzsmsk.cz/index.php?ID=118

[39] PLÁŠKOVÁ, Alena. *Jednoduché nástroje řízení jakosti II.: výstup z projektu podpory jakosti č. 5/16/2004*. Vyd. 1. Praha: Národní informační středisko pro podporu jakosti, 2004. Průvodce řízením jakosti. ISBN 80-020-1690-4.

[40] PLURA, Jiří. *Plánování a neustálé zlepšování jakosti*. Vyd. 1. Praha: Computer-Press, 2001. Business books (ComputerPress). ISBN 80-722-6543-1.

[41] *Analýza možných způsobů a důsledků poruch (FMEA): referenční příručka*. 4. vyd. Překlad Ivana Petrašová. Praha: Česká společnost pro jakost, 2008. ISBN 978-80-02-02101-8.

[42] Organizační struktura krajského ředitelství Zlín. *Hasičský záchranný sbor ČR* [online]. [cit. 2016-05-08]. Dostupné z: http://www.hzscr.cz/clanek/schema-organizacni-struktury.aspx

[43] ČESKO. Vyhláška č. 247/2001 Sb., Ministerstva vnitra o organizaci a činnosti jednotek požární ochrany. In *Sbírka zákonů ČR*, ročník 2001, částka 95. Dostupné na: <http://www.zakonyprolidi.cz/cs/2001-247> [cit. 2012-06-15]. ISSN 1211-1244

[44] Interní dokument HZS Luhačovice

[45] Postup při případném výskytu ptačí chřipky. *Magazín o životě a dění ve Zlínské kraji* [online]. [cit. 2016-05-08]. Dostupné z: http://hexxa.websystem.cz/article/2929.postup-pri-pripadnem-vyskytu-ptaci-chripky/

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

CIWIN	Informační sítě pro kritickou infrastrukturu
ČR	Česká republika
EKI	Evropská kritická infrastruktura
EPCIP	Evropský program pro ochranu kritické infrastruktury
EU	Evropská Unie
HZS	Hasičský záchranný sbor
KI	Kritická infrastruktura
MU	Mimořádná událost
SCEPC	Hlavní výbor pro civilní nouzové plánování SCEP
VNCP	Výbor pro civilní nouzové plánování

SEZNAM OBRÁZKŮ

SEZNAM TABULEK