Oponentní posudek disertační práce

Název práce:	Posouzení bezpečnosti vybraného objektu kritické Infrastruktury z pohledu integrální bezpečnosti a návrh na snížení kritičnosti objektu[1]
Doktorand:	Ing, Tomáš Kertis, České vysoké učení technické v Praze, Fakulta dopravní, Ústav bezpečnostních technologií a inženýrství
Školitel:	doc. RNDr. Danuše Procházková, CSc., DrSc.
Vypracován dne:	21. 5. 2021

Práce je strukturovaná do 7 kapitol včetně úvodu a závěru, její rozsah činí 124 stran textu práce a dále přílohy, z toho 10 stránek použité literatury (93 zdrojů), 22 obrázků a 13 tabulek.

Tématem práce *je posouzení bezpečnosti vybraného kritického objektu z pohledu integrální bezpečnosti a návrh na snížení kritičnosti objektu, ti. zvýšení jeho bezpečnosti. Vybraným kritickým objektem je metro v Praze.*

Hlavním cílem *je zvýšení bezpečnosti metra aplikací metod pro identifikaci a práci s aktivy, jejich kritičnostmi a riziky tak, aby bylo možné zajistit celkovou (integrální) bezpečnost metra na základě zvýšení znalostí o problémech a zranitelnostech aktiv, a to v oblasti techniky, v oblasti kybernetické, kde jde o zvýšení informačního výkonu systému, a dalších oblastech řízení, které jsou důležité pro bezpečný provoz.*

Dále jsou v práci uvedeny ***Dílčí cíle disertační práce***, ovšem ve skutečnosti se nejedná o dílčí cíle (ve smyslu dílčí výzkumné otázky nebo dílčí řešené problémy), ale jde o popis jednotlivých kroků při vytvoření dizertační práce. Proto je oponent dále nepopisuje.

Základní výzkumný problém je formulován v části 1.3 velmi obecnými formulacemi. Za podstatné lze považovat zaměření na tzv. nadprojektové jevy (vysvětleno až na s. 33), jež jsou popsány jako *původci rizik, dochází ke kritickým situacím, které jsou způsobeny vznikem nezadaných propojeni v složitém systému, tj. vznikají neočekávaná propojeni, která vedou k selhání, a často k celým kaskádám selháni.*

Kapitola 2 Rešeršní část – souhrn poznatků o sledovaném problému – obsahuje klasickou subkapitolu *Definice použitých pojmů*. Ne se všemi definicemi se oponent ztotožňuje, resp. se domnívá, že lze najít definici vhodnější, resp. zavedenější (např. definice aktiva, která v obecném pojetí v oblasti řízení rizik zní „*Aktivum je všechno, co má pro subjekt hodnotu, která může být zmenšena působením hrozby.*“). Podobně otázkou je, zda skutečně „*Příčinou rizik jsou*

[1] Oponent upozorňuje, že v dokumentu Teze k disertační práci je název práce zcela protismyslně uveden jako „…návrh na snížení bezpečnosti objektu“.

pohromy…“, tj. pouze pohromy, zejména chápeme-li pohromy ve smyslu zdroje, na který se přímo disertant odvolává a kde se uvádí, že pohromou se rozumí „*Výskyt přírodní katastrofy, technologické nehody nebo události způsobené člověkem, která vedla k vážným škodám na majetku, úmrtím nebo mnohočetná zranění.*“ Podobně je také definována pohroma např. v EM-DAT „*Situace nebo událost, která převažuje nad místními kapacitami, což vyžaduje požadavek na externí pomoc na národní nebo mezinárodní úrovni. Nepředvídaná a často náhlá událost, která způsobí velké škody, zkázu a lidské utrpení.*“[2] Lze tedy očekávat, že práce se tedy bude zřejmě zaměřovat na extrémní pohromy, které bývají označovány jako katastrofy.

Také s tabulkou č. 1 Rozložení pohrom lze diskutovat, zejména pokud není doplněna dalšími vysvětlivkami, jak k dané klasifikaci na pohromy relevantní, specifické, kritické autor u konkrétních hrozeb dospěl. Markantní je to vidět např. u položek Zemětřesení (proč by mělo mít menší dopad než Vichřice?) nebo Kriminalita (např. v oblasti kybernetické bezpečnosti může proběhnout kriminální útok stejným způsobem a se stejnými následky, jako v případě Teroristického útoku[3]). Celkově se jeví oponentovi tabulka jako překrývající se v jednotlivých druzích pohrom.

Co se týká další definice důležité pro tuto práci – pojem „riziko“, pak autor správně uvádí mnoho možných variant chápání rizika (s. 23), možná by bylo vhodné jednotlivé varianty okomentovat (např. poslední vzorec R = četnost · populace · zranitelnost je značně pythický).

V dalším textu lze plně souhlasit s důležitým tvrzením, že „*integrální bezpečnost lze zvyšovat pouze při zvažování a řízení integrálních rizik, které nezvažují pouze součet dílčích rizik, ale počítají i s vazbami a toky mezi aktivy*“. Následující vzorec pro kritičností aktiva *(K) = důležitost · zranitelnost* zavádí pojem „důležitost“. Otázkou je, zda se tím myslí „význam aktiva“ nebo „hodnota aktiva“ pro jeho vlastníka, provozovatele či jiné osoby (uživatele, v tomto případě cestující?), nebo ještě něco jiného. Protože s tímto termínem autor pracuje v rámci celé práce, detailní definici by si jistě zasloužil. Také vzorec *Kritičnost s ohledem na jistou pohromu = C = S · O · B, kde S je závažnost největšího dopadu pohromy (škodlivého jevu), O pravděpodobnost výskytu pohromy a B podmíněná pravděpodobnost, že se vyskytne nejzávažnější dopad* není srozumitelný. Přinejmenším pokud bude čtenář práce vnímat slovo „jistý“ jako událost, jejíž pravděpodobnost = 100 % (jev jistý), pak vzorec nedává smysl. Je ovšem možné, že autor tím myslel spíše „určitou“ než jistou pohromu.

[2] https://www.emdat.be/Glossary#letter_d

[3] K tomu viz např. Smejkal, Vladimír. Kapitola 10, § 8, 9. Nový fenomén kyberterorismus a Kybernetická válka a Kap. 11 § 2 Kybernetická kriminalita. In: Válková Helena, Kuchta Josef, Hulmáková Jana a kolektiv. *Základy kriminologie a trestní politiky.* 3. vydání, Praha: C. H. Beck, 2019, s. 515-521 a s. 542-570.

Co je naopak třeba ocenit, je správné chápání rozdílů mezi pojmy dnes často směšovanými – bezpečnost (Safety) a zabezpečení (Security). Zabezpečení (Security) je jen jedním z aspektů Safety, resp. zajištění bezpečnosti dosahujeme prostřednictvím zabezpečení před protiprávními činnostmi, ale i před jinými hrozbami (lidským chybám, selhání techniky či vlivu vyšší moci). Z toho vyplývá i správný závěr, že „*bezpečnost a riziko sice spolu souvisí, ale nejsou komplementárními veličinami*“, nicméně již méně lze souhlasit s tím, že „*bezpečnost lze zvýšit i organizačními opatřeními, kterými velikost rizika neovlivníme*“. Platí-li, že „*Úroveň rizika je určena hodnotou aktiva, resp. následkem pro jeho vlastníka či celou organizaci, zranitelností aktiva a úrovní hrozby. Na růstu úrovně rizika se podílí úroveň hrozby, zranitelnost a hodnota aktiva. Provedení opatření úroveň rizika snižuje*.“[4], pak samozřejmě i organizační opatření má vliv na velikost, resp. snížení hrozícího rizika.

Pokud se dále autor zabývá tzv. integrální bezpečností, pak tam se zjevně ocitá na poli mu dobře známém. S jeho pojetím lze souhlasit, zejména pak se závěrem „*pro to, aby byla zajištěná integrální bezpečnost, nestačí zvyšovat bezpečnost nebo zabezpečení jednotlivých prvků systému, které svými vzájemnými vazbami tvoří komplexní systém, ale musíme zajistit efektivnější systém řízení, který je schopen se se složitostí reálného světa co nejlépe vypořádat*“.

V části 2.1.5 a dále pak v práci (zejména v 2.4.6 Zabezpečení kyber-fyzických systémů) používá autor pojem „kyber-fyzický systém“, aniž by jej někde definoval. Má se snad jednat o pojem, který se objevil v souvislosti s tzv. Průmyslem 4.0 jako CPS (Cyber-Physical System)? Co si pod ním autor představuje? Oponent tento pojem za notorietu nepovažuje.

Výklad v části 2.1.8 Systémy systémů (SoS), projektové a nadprojektové jevy považuje oponent za velmi přínosný. Při dnešní provázanosti humánních a i technických systémů musíme vnímat prakticky každou oblast fungování lidské společnosti jako složitou strukturu systémů – systémů systémů – nadsystémů atd. To je dále umocňováno mírou interakce v rámci stále se rozšiřujícího kyberprostoru. Přínosná je rovněž navazující část 2.2 Bezpečnost technických děl. Co se týká části 2.3 Systémy řízení bezpečnosti (SMS), lze s textem zcela souhlasit. Pouze by bylo vhodné vysvětlit, zda SMS znamená Safety Management System nebo něco jiného.

Co se týká části 2.3.5 Řízení bezpečnosti v dopravě, pak v momentě, kdy se autor pouští do diskuse ohledně bezpečnosti informací a kybernetické bezpečnosti, dopouští se jisté nepřesností. Není pravdou že pojem „bezpečnost informací“ by byl specialitou v českých podmínkách a že by byl nepřesný. Pojem „bezpečnost informací“ je používán jak v mezinárodních normách (např. řada ISO/IEC 27000), tak v zákonu č. 181/2014, o kybernetické bezpečnosti, a je

[4] Smejkal, V., Sokol, T., Kodl. J. *Bezpečnost informačních systémů podle zákona o kybernetické bezpečnosti.* Plzeň: Aleš Čeněk, 2019, s. 298.

definován jako „zajištění důvěrnosti, integrity a dostupnosti informací“, tedy cílový stav, kterého je třeba dosáhnout ustavením ISMS (Information Security Management Systém) neboli česky Systém řízení bezpečnosti informací[5]. Tohoto cíle se dosahuje zabezpečením (ani tak nikoliv informací, ale spíše informačních systémů, včetně technologií a procesů).

Část 2.4 Informační systémy a technologie je velmi době zpracována a obsahuje důležité informace. Lze ji označit za jednu z nejpřínosnějších subkapitol rešeršní části. Připomínky lze mít pouze k části 2.4.6 Zabezpečení kyber-fyzických systémů, a to počínaje absencí definice těchto systémů, jak je již uvedeno výše, přes výklad pojmů, které platí obecně do oblasti kybernetické bezpečnosti až po závěrečnou proklamaci „*Proto musí mít kyber-fyzické systémy stanovené jisté limity a podmínky, které podmiňují jejich kvalitativní parametry (tj. bezpečnost, spolehlivost, dostupnost, celistvost, kontinuita a přesnost)*“. Čtenář práce si totiž uvedené pojmy – kvalitativní parametry musí doplnit obsahem podle vlastního uvážení či fantazie, přičemž u některých se toho ani oponent neodvažuje.

Souhrnně k rešeršní části 2. disertační práce oponent konstatuje, že z hlediska účelu a cílů práce tato část není nevyhovující, nicméně zejména v oblasti fundamentálních definic základních pojmů a následné práce s nimi nejsou tyto zavedeny vždy přesně a bez zohlednění dalších možných zdrojů informací kromě citovaných (mezinárodní normy, jiné literární zdroje), což pravděpodobně vede i jejich neúplnému či nepřesnému popisu a aplikaci na zkoumanou problematiku. Rešeršní část, resp. celá práce pracuje se zdroji převážně tuzemskými, a to až na výjimky se zdroji vytvořenými vlastní činností doktoranda jako autora či spoluautora, vzniklými především v rámci Ústavu bezpečnostních technologií a inženýrství FD ČVUT. Větší mezinárodní přesah tedy chybí.

Kapitola 3 Data o provoz metra v Praze a jeho řídicích systémů se věnuje popisu metra z hlediska vztahů mezi řídicími, zabezpečovacími a řízenými systémy. V této části autor shromáždil mnoho přínosných informací, které dobře vypovídají o řídicích, zabezpečovacích a dalších systémech řízení metra. Od obecného popisu metra jako takového (síť metra, stanice, délka tras, vozový park) se dostáváme k oblastem souvisejícím již se zaměřením práce: technologické systémy metra, zabezpečovací zařízení, řídicí systémy (ASDŘ) a jejich zařazení z hlediska klasifikace podle Urban Guided Transport Management and Command/Control System (UGTMS), přenosový systém řídícího systému metra a UGTMS. Lze mít jen dotaz, jaké systémy SCADA, jež se nacházejí na pravé straně obrázku č. 12, byly v systému ASDŘ-D pro řízení dopravy pražského metra identifikovány. Návaznost dříve provedených prací autorem disertace je velmi dobře popsána v subkapitole 3.5 Výsledky analýzy znalostí a praxe z drážního prostředí a

[5] Viz např. § 3 vyhl. č. 82/2018 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat.

provozu metra. Vyplývá z ní, že se autor zabývá problematikou systematicky a dlouhodobě a identifikoval významné nedostatky a a kritická místa drážního systému. Dále uvádí organizační zranitelnosti a fakta vyplývající z případových studií. Tuto subkapitolu považuje oponent za velmi vyznanou, představující vynikající východisko pro další zpracování disertační práce.

Kapitola 4 Popis použitých metod a nástrojů – návrh řešení nejprve popisuje použité metody, přičemž konstatuje, že „*Předmětný systém nelze analyzovat přesnými (exaktními) metodami a je nutné jej analyzovat pomocí metody vhodné pro analýzu měkkých systémů, tj. proto je nutné vybírat z heuristických metod, konkrétně metod expertních*“. S tím lze zcela souhlasit. Jako expertní metodu použitá pro sběr dat (přesněji možná řečeno pro získání informací) byla velmi vhodně zvolena vícestupňová metoda Delphi, která je s oblibou používána v rámci kvalitativních metod analýzy rizik. Podrobný popis se nachází v subkap. 4.1.2 až 4.1.3. Vágní pojem „důležitost“ byl kvantifikován na stupnici 1 až 3, čímž se poněkud řeší obtížná uchopitelnost tohoto pojmu. Na druhou stranu obvyklý rozsah stupnice (resp. stupnic v analýze rizik) je používán v rozpětí 1 až 5 a lze se domnívat, že tímto může dojít k jistému splynutí odlišných kategorií jednotlivých atributů. Obsah subkap. 4.2.1 Teorie citlivosti je pro oponenta jistým překvapením, zejména pak konstatování, že „*Z důvodů lepší interpretace a práce s informačními systémy lze zranitelnost definovat také jako citlivost…*“. Jedná se o poměrně inovační přístup, nicméně výklad provedený v násl. subkapitolách potvrzuje oprávněnost tohoto přístupu a jeho přínos pro disertační práci. Podrobný popis postupů v části 4.2 nicméně není ukončen popisem konkrétních výsledků, ale obecnými tezemi v subkap. 4.3 Zvýšení bezpečnosti s využitím znalosti a metody řízení rizik. Konkrétní výstupy se nacházejí až v další kapitole 6, což by mohlo být řešeno odkazem.

Kapitola 5 Bezpečnostní výzkum provozu pražského metra obsahuje výsledky použití metod a nástrojů z kapitoly 4.1. Je zde popsána identifikace aktiv důležitých pro bezpečný provoz metra v pěti úrovních řízení bezpečnosti (5.1), která proběhla standardním způsobem. Za zmínku nicméně stojí konstatování autora, že mezi aktiva, která nebyla dostatečně identifikována, patří i aktiva ekonomická, což otevírá prostor pro další bádání. Subkap. 5.2 popisuje zranitelnosti, důležitosti a kritičnosti aktiv (k důležitosti a použitým stupnicím viz výše). I v tomto poněkud hrubším škálování jsou výsledky pro skupinu aktiv Vazby a toky velmi přínosné. Subkap. 5.3 popisuje reálný stav zabezpečení systému vůči specifickým a kritickým pohromám. Velmi zajímavé jsou výsledky popisující, jak které pohromy hodnotí experti. Některé závěry jsou až alarmující (např. *Chybí plán kontinuity, který by ochránil kritická technická zařízení metra; v rámci krizového plánu města Prahy je řešena pouze ochrana životů a zdraví lidí.*). Přesto ale popsané výsledky obsahují jisté rozpory, které by měly být vysvětleny – jde o rozpory mezi

výčtem, které pohromy experti nepovažují za relevantní, a tabulkou č. 13, kde jsou tyto pohromy stále vedeny.

Kapitola 6 Výsledky, jejich interpretace a posouzení obsahuje výsledky použití metod a nástrojů z kapitoly 4.2. Nachází se zde 1. interpretace výsledků pomocí matic citlivostí a jejich analýza, 2. transformace matic citlivostí do grafu za použití aparátu teorie grafů, 3. analýza scénáře dopadů na vybranou kritickou pohromu. Podle názoru oponenta je tato kapitola jednou z nejpřínosnějších částí disertační práce. Popsaný postup zohledňuje i zranitelnost vůči výpadku okolních aktiv, tedy to, co je v práci nazváno jako nadprojektové jevy. Příkladem konkrétních závěrů vyplývajících ze zpracování dat uvedenými postupy je obr. 18 a z něj vyplývající poznatky, které mohou posloužit pro zvýšení odolnosti metra proti uvedeným hrozbám. Podobně zajímavé a užitečné výsledky ohledně vazeb a toků představují obr. 20 a 21 a navazující závěry. Subkap. 6.3 Vybraný scénář dopadů popisuje zjednodušený příklad, a to scénář dopadů pandemie a plán odezvy na pandemii – pravděpodobně jako reflexi na současnou situaci s covidem. Popis toho, že musí plány odezvy pro případ epidemie/pandemie v metru obsahovat plán pro zajištění čistého vzduchu je velmi konkrétní a dobře ilustruje použití metodiky popsané v disertační práci. Subkap. 6.4 Celkové vyhodnocení a návrh na snížení kritičnosti konstatuje prioritní rizika a v obecné rovině uvádí opatření pro snížení kritičnosti. Zde by bylo vhodné uvést i příklady konkrétních doporučovaných bezpečnostních opatření pro zlepšení představy o aplikační využitelnosti práce.

V kap. 7 Závěr shrnuje autor obsah disertační práce a zcela správně konstatuje, že *Praktické výsledky výzkumu ukazují na kritické vazby systémů, které mohou v provozu v různých úrovních řízení bezpečnosti způsobovat problémy. Proto uvedené vazby a jejich aktiva je v praxi nutné ošetřit plánem řízení rizik, ve kterém budou uvedena opatření podpořena zajištěním techniky, postupem provedení, personálem, odpovědnostmi a financemi. Pro vypracování uvedeného plánu předložená disertační práce poskytuje základ.* S tím lze souhlasit, zejména pokud byly předané výsledky ještě konkrétnější, než je v práci naznačeno (pravděpodobně v publikaci [7]). Pokud pak dále autor uvádí, že *popsanými výsledky svůj cíl splňuje v teoretické i praktické rovině, vede ke zvýšení znalosti v systémech řízení bezpečnosti a jejich úrovní na základě moderních proaktivních přístupů, a znalostí o aktivech a jejich vazbách v systému řízení bezpečnosti pro provoz metra*, tomuto závěru oponent zcela přisvědčuje. Souhlasí rovněž s tím, že *práce poskytuje platformu pro další výzkum a vývoj,* a domnívá se, že vytvoření softwarových nástrojů, které by na bázi popsaných metod umožnily je používat v různých oblastech nasazení, by bylo velmi žádoucí.

Závěry oponentního posudku

Téma práce je v dnešní době, kdy je třeba kontinuálně testovat a zvyšovat zabezpečení (nejen) kritické infrastruktury a její odolnost proti hrozbám spočívajících především v kriminální činnosti, teroristickým útokům a vybraným přírodním hrozbám (od pandemií po povodně), vysoce aktuální.

Přínos do vědecko-výzkumné oblasti spočívá ve vlastním výzkumu týkajícím se metodik a postupů pro analýzu rizik z pohledu integrální bezpečnosti metra a zohlednění tzv. nadprojektových jevů.

Přínos pro praktické použití je nezpochybnitelný. Práce obsahuje významné argumenty ve prospěch používání popsaných postupů zejména v rámci kritické infrastruktury.

Autor svojí prací potvrzuje fundovanost v dané problematice. V disertační práci naplnil stanovené cíle.

Grafická i formální úprava vyhovuje standardům.

Na základě posouzení předložené disertační práce lze jednoznačně konstatovat, že cíle práce byly naplněny. Posuzovaná disertační práce splňuje všechny na ni kladené požadavky. Jedná se o původní vědeckou práci obsahující samostatný přínos autora.

Otázky pro obhajobu disertační práce:

1. Co to je „kyber-fyzický systém“? Definujte jej a uveďte, kdy a kde byl tento pojem všeobecně zaveden.
2. Proč jste celý výklad postavil na pojmu „pohroma“, který nevystihuje všechna rizika, resp. negativní události, ale pouze ty, které mají charakter katastrof. Bylo záměrem tím nastavit určitou úroveň dopadů, pod níž není riziko řešeno (je považováno za zbytkové)?
3. Vysvětlete, jak lze dostupnost a integritu vyjádřit například pomocí pravděpodobnostních parametrů ve vztazích (15) až (20) uvedených v práci, jak tvrdíte na s. 57.

Závěrečné doporučení oponenta:

D i s e r t a č n í p r á c i d o p o r u č u j i k o b h a j o b ě .

prof. Ing. Vladimír Smejkal, CSc., LL.M., DrSc.
Ústav informatiky
Fakulta podnikatelská
Vysoké učení technické v Brně
Kolejní 2906/4
612 00 Brno