VŠB TECHNICKÁ UNIVERZITA OSTRAVA | FAKULTA BEZPEČNOSTNÍHO INŽENÝRSTVÍ | KATEDRA OCHRANY OBYVATELSTVA

Konvergovaná bezpečnosť v kontexte resiliencie kritickej infraštruktúry

Tézy inauguračnej prednášky

k riadeniu k menovaniu profesorom v odbore

Bezpečnost a požární ochrana

doc. Ing. Martin Hromada, Ph.D.

Ostrava, květen 2023

HROMADA, Martin. *Konvergovaná bezpečnosť v kontexte resiliencie kritickej infraštruktúry*. [Tézy inauguračnej prednášky]. Ostrava: VŠB – Technická univerzita Ostrava, 2023. 53 s. ISBN 978-80-248-4667-5.

Vydala VŠB – Technická univerzita Ostrava

ISBN 978-80-248-4667-5

Obsah

1 Úvod

Kritická infraštruktúra (KI) vo svojej podstate zohráva strategickú úlohu pri naplňovaní vitálnych funkcií modernej spoločnosti. Je preto zrejmé, že spoľahlivosť, výkon, nepretržitá prevádzka, bezpečnosť, údržba a ochrana kritických infraštruktúr sa stali národnými prioritami spoločnosti (Alcaraz et al., 2015). Cieľom vymedzenia kritickej infraštruktúry je preto určenie tých prvkov, ktoré sú pre štát a spoločnosť kľúčové a bez ktorých by bola vážne narušená funkcia štátu a súčasne obmedzený život a funkcie spoločnosti. Takéto prvky kritickej infraštruktúry by potom mali byť vhodným a primeraným spôsobom chránené. Cieľom ochrany je teda vytvorenie podmienok, brániacich vonkajším a vnútorným činiteľom negatívne pôsobiť na chránené aktívum systému. Ak majú byť ochranné opatrenia účinné, malo by byť zrejmé do akej miery je systém či prvok schopný odolávať pôsobeniu vonkajších a vnútorných činiteľov resp. do akej miery je prvok zraniteľný (European Council, 2008).

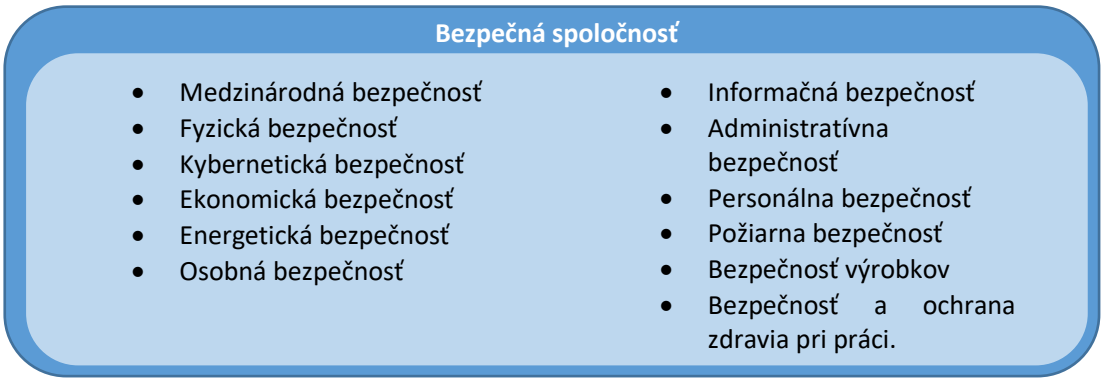
Bezpečnosť a ochrana prvku kritickej infraštruktúry je často spojená so skutočnosťou, že jednotlivé infraštruktúry sú vzájomne horizontálne a vertikálne prepojené, čo reprezentuje do istej miery koncept systém systémov. V súvislosti s prepojenosťou sa teda dá diskutovať aj o ich vzájomnej závislosti (interdependency), kde vzájomná závislosť kritických infraštruktúr vytvorila predpoklad klasifikácie typológie väzieb. Za základné väzby je možné preto považovať väzby fyzické, kybernetické, logické či geopriestorové. Táto skutočnosť poukazuje na fakt, že jednou zo základných vlastností kritickej infraštruktúry je jej sieťový charakter. Sieťový charakter je v súvislosti s predmetnou problematikou potrebné vnímať v širšom kontexte, kde sa nejedná len o siete hmotné ako napr. dopravné, logistické, komunikačné a energetické, ale aj abstraktné siete ekonomické, finančné, spoločenské a znalostné (Rinaldi et al., 2001). Je preto zrejmé, že izolované a ohraničené chápanie bezpečnosti a ochrany má len obmedzený efekt a je potrebné toto chápanie dať do súvislosti s konvergenciou bezpečnosti v kontexte resiliencie tejto skupiny infraštruktúrnych prvkov. Konvergovaná bezpečnosť v tomto prípade spája (konverguje) vybrané druhy bezpečnosti do komplementárneho celku. To odráža integrálne determinanty resiliencie v súvisiacich oblastiach bezpečnosti/zabezpečenia (Hromada et al., 2021).

Inauguračná prednáška preto stručne syntetizuje poznatky výskumu problematiky bezpečnosti a konvergovanej bezpečnosti v kontexte resiliencie kritickej infraštruktúry. Potrebný detail bude venovaný vzťahu medzi konvergovanou bezpečnosťou a resilienciou kritickej infraštruktúry, kde významná časť inauguračnej prednášky je prezentácia výsledkov výskumu autora v oblasti funkčnosti systémov fyzickej ochrany ako aspektu bezpečnosti, integrálnej bezpečnosti, resiliencie s aspektom hodnotenia kaskádových a synergických efektov, potrebám konvergencie vybraných druhov bezpečnosti a možnosti implementácie filozofie konvergencie v rámci atribútov resiliencie kritickej infraštruktúry.

Prednáška súčasne popisuje motiváciu k rozvoji vedeckovýskumnej činnosti a koncepcii pedagogické práce a prezentuje prehľad najvýznamnejších odborných a publikačných výsledkov autora.

2 Obecné chápanie bezpečnosti

Bezpečnosť vo svojej postate patrí medzi významné fenomény dnešnej spoločnosti v jej širších súvislostiach. V posledných desiatkach rokov začína byť bezpečnosť považovaná za vedný odbor s vlastným predmetom skúmania, cieľom a metódami. Bezpečnosť sa v konečnom dôsledku v spoločnosti zaisťuje prostredníctvom jednotlivých druhov bezpečnosti (viď obrázok 1), kde druh bezpečnosti je možné vnímať ako súbor opatrení predurčených k zaisteniu bezpečnosti vo vymedzenej časti reality resp. bezpečnostnom prostredí. V súčasnosti medzi základné druhy bezpečnosti patria medzinárodná, fyzická, kybernetická, ekonomická, energetická, osobná, informačná, administratívna, personálna, požiarna bezpečnosť, bezpečnosť výrobkov či bezpečnosť a ochrana zdravia pri práci.



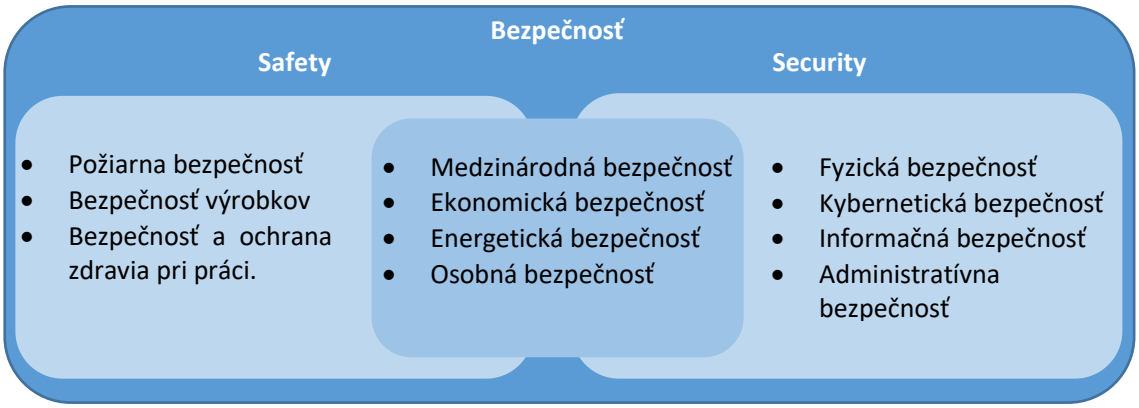
Obrázok 1: Základné druhy bezpečnosti vedného odboru bezpečnosť

Spoločná ambícia formovať a rozvíjať vedný odbor bezpečnosť je vo svojej podstate spojená a podmienená rozvojom teórie bezpečnosti. Problematika teórie bezpečnosti je relatívne nová, no dá sa konštatovať, že v súčasnosti už existujú súbory teoretických poznatkov, ktoré sú jednotlivými druhmi bezpečnosti využívané, sú v praxi osvedčené a implementované a zapadajú do mozaiky teórie bezpečnosti. Je preto zrejmé, že sa samotná teória bezpečnosti zameriava na systémové chápanie bezpečnosti, realizuje zarámovanie bezpečnostného problému popisom toho, čo to narušenie bezpečnosti je, v akých obecných formách a k akým typom narušenia bezpečnosti dochádza, na čom závisí a ako je možné zabrániť alebo minimalizovať veľkosť dopadu. Tak ako bolo konštatované, zvyšujúci sa dopyt po bezpečnosti je pragmaticky spojený s potrebou praxe a teda aj s bezpečnosťou infraštruktúrnych systémov.

2.1 Klasifikácia druhov bezpečnosti

V bezpečnostnom prostrední Českej a Slovenskej republiky je prijatá do určitej miery premisa, že bezpečnosť je stav, kedy sú na najnižšiu možnú mieru eliminované hrozby a na najnižšiu možnú mieru alebo akceptovateľnú mieru minimalizované riziká vybraného aktíva, a keď je aktívum k minimalizácii efektívne vybavené. Táto premisa do určite miery poukazuje na nedeliteľnosť bezpečnosti ako vedného odboru. Obecne sa však dá prevziať názor, že bezpečnostné opatrenia patriace do skupiny **Safety** reflektujú neintencionálne bezpečnostné hrozby, a bezpečnostné opatrenia patriace do skupiny **Security** reflektujú intencionálne bezpečnostné hrozby a z nich vyplývajúce riziká. Preto by sa za určitých špecifických okolností dalo prijať tvrdenie, že ekvivalentom pojmu **Safety** je bezpečnosť a pojmu **Security** je zabezpečenie.

Je nutné ale pripustiť fakt, že v bezpečnostnej praxi by sa našli príklady, ktoré by toto tvrdenie nemuseli v plnej miere potvrdiť, resp. by boli kombináciou oboch skupín opatrení (viď obrázok 2).



Obrázok 2: Členenie druhov bezpečnosti vo väzbe na odbor Bezpečnost a požární ochrana

Aspekt bezpečnostných hrozieb a z nich vyplývajúcich rizík je preto fundamentálnym základom pre vymedzenie a stanovenie druhov bezpečnosti. Formulácia druhov bezpečnosti preto do určitej miery reflektuje základnú klasifikáciu bezpečnostných hrozieb, ktorá je podľa (Řehák, 2012) kategorizovaná na:

- Vonkajšie hrozby
  - politické hrozby,
  - ekonomické hrozby,
  - sociálne hrozby,
  - technologické hrozby,
  - legislatívne hrozby,
  - ekologické hrozby,
- Vnútorné hrozby
  - procesné hrozby,
  - personálne hrozby,
  - vecné hrozby.

Ďalší filozofický pohľad na klasifikáciu druhov bezpečnosti popísali (Hromada a Lukáš, 2016) z pohľadu bezpečnostných modelov. Bezpečnostné modely sú v tejto súvislosti chápané ako „pojmové modely“, ktoré pomocou slovného a obrazového spôsobu popisujú podstatu a spôsob zaistenia bezpečnosti referenčného objektu. V modeli sa odráža podstata opatrení, prostredníctvom ktorých sa bezpečnosť zaisťuje. Bezpečnosť môže byť zaistená systémom opatrení logického alebo fyzického charakteru. Medzi opatrenia logického typu sa zaraďujú pravidlá, riadenie, vzdelávanie, vyjednávanie, predikcia, odstrašenie, šifrovanie atď. Tieto opatrenia sú založené na informáciách a práci s nimi. Opatrenia fyzického typu zahŕňajú zábrany (ploty, steny), absorbéry nárazu, fyzickú ostrahu, sily a prostriedky ozbrojených zborov, varovné a poplachové systémy, zásoby atď. Medzi základné modely zaistenia bezpečnosti patria:

- režimový model,
- proaktívny model,
- bariérový model,

- model pripravenosti,
- model kolektívnej bezpečnosti / spoločného záujmu,
- reaktívny model,
- model vnucovania pravidiel,
- model odstrašenia.

Treba však konštatovať, že v rade modelov je podstata zaistenia bezpečnosti realizovaná viacerými spôsobmi. Preto zahŕňajú viacero variantov modelov. Model vnucovania pravidiel a model odstrašenia sú špecifickými modelmi a majú pomocný charakter. Pri samotnom zaistení bezpečnosti sa len v ojedinelých prípadoch použije iba jeden typ bezpečnostného modelu. Obvykle sa bezpečnosť zaisťuje kombináciou opatrení, spadajúcich do agendy viacerých bezpečnostných modelov.

Z pohľadu vymedzenia druhu bezpečnosti v kontexte konvergovanej bezpečnosti konštatujú (Lukáš a Urbančoková, 2019), že druh bezpečnosti predstavuje súbor opatrení, riešiacich špecifickú skupinu bezpečnostných problémov. Ide o sústavné a opakované riešenie nežiaducich javov narušenia bezpečnosti určitého typu. Cieľom zavedených a realizovaných opatrení je zamedziť vzniku ujmy alebo aspoň minimalizovať dopady spôsobené narušením bezpečnosti. Príkladom druhu bezpečnosti je fyzická bezpečnosť, informačná bezpečnosť, bezpečnosť a ochrana zdravia pri práci, bezpečnosť cestnej premávky a medzinárodná bezpečnosť. Konvergovaná bezpečnosť v sebe zlučuje prevádzkovú bezpečnosť, fyzickú bezpečnosť a kybernetickú bezpečnosť.

2.2 Význam konvergovanej bezpečnosti v kontexte resiliencie kritickej infraštruktúry vo väzbe na obecné chápanie bezpečnosti

Konvergovaná bezpečnosť v kontexte resiliencie nerozlišuje oblasť Safety a ani oblasť Security. V oboch prípadoch sa jedná o spomínané spájanie (konvergenciu) aspektov a opatrení jednotlivých druhov bezpečnosti do komplementárneho celku, čo odráža integrálne determinanty resiliencie v súvisiacich oblastiach bezpečnosti/zabezpečenia. Tento prístup do určitej miery znižuje tak nevýhody izolovaného a uzavretého použitia spektra opatrení oblasti Safety a Security.

Súčasne použitie filozofie konvergencie v kontexte resiliencie umožňuje zohľadniť sieťový charakter kritickej infraštruktúry v prenesenom význame na kaskádové a synergické efekty (ako príklad vonkajších bezpečnostných hrozieb) a optimalizuje použitie prístupu bottom-up vzhľadom na dekompozíciu kritickej infraštruktúru na systém, sektor, subsektor a prvok kritickej infraštruktúry.

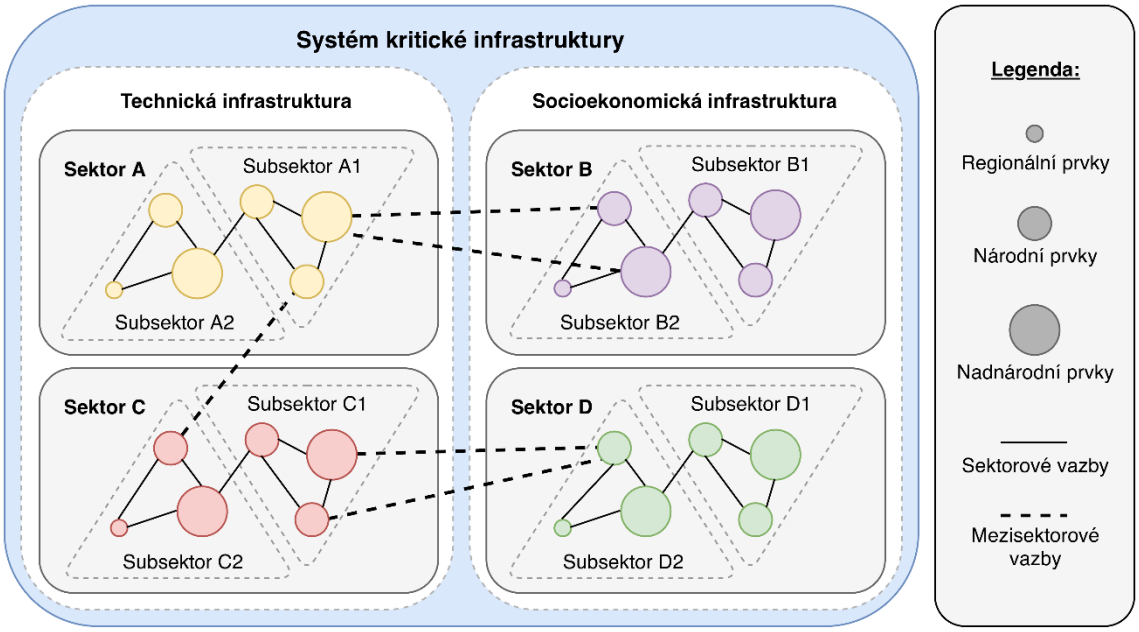
Vzhľadom na vedeckú činnosť autora bude bezpečnosť a ochrana prvkov kritickej infraštruktúry vnímaná s konkrétnou väzbou na fyzickú bezpečnosť v kontexte zvyšovania efektivity a účelnosti systémov fyzickej ochrany, tvorbu integrálneho bezpečnostného systému v prepojení na determinanty resiliencie, vplyv kaskádových a synergických efektov a konečnú konvergenciu aspektov bezpečnosti a resiliencie prvkov kritickej infraštruktúry.

3 Konvergovaná bezpečnosť v kontexte resiliencie kritickej infraštruktúry

Hlavnou ambíciou a podstatou tretej časti inauguračnej prednášky je prezentácia a zoznámenie odbornej verejnosti s vymedzením systému kritickej infraštruktúry a aspektu konvergovanej bezpečnosti v kontexte resiliencie.

3.1 Dekompozícia kritickej infraštruktúry

Kritická infraštruktúra ako systém je hierarchicky a logicky dekompovateľná na štyri hlavné úrovne, národná a teda systémová, sektorová, substektorová a elementárna a teda úroveň prvku kritickej infraštruktúry. Samostatnou kategóriou je úroveň európskej kritickej infraštruktúry, ktorá do istej miery vytvára spojenie elementárnej úrovne kritickej infraštruktúry jedného členského štátu a systémovej úrovne iných členských štátov. Z pohľadu aspektu funkčnosti (viď obrázok 3), je možné následne systémovú úroveň vnímať v kontexte technickej a socioekonomickej infraštruktúry, funkcií a služieb (Řehák a Hromada, 2018).



Obrázok 3: Technické a socioekonomické usporiadanie systémovej úrovne kritickej infraštruktúry (Řehák a Hromada, 2018)

Obecné chápanie rozdielu medzi technickou a socioekonomickou infraštruktúrou môže byť viazané s aspektom poskytovania základných resp. životných technických služieb a doplňujúcich podporných sociálnych či ekonomických služieb. Dá sa preto konštatovať, že technické infraštruktúry poskytujú služby v oblasti energetiky, dopravy, dodávky pitnej vody a dostupnosť komunikačných a informačných služieb. Význam a nezastupiteľnosť socioekonomickej infraštruktúry je na druhej strane vnímaná z pohľadu zaistenia služieb zdravotníctva, finančného trhu, núdzových služieb či služieb verejnej správy v širších súvislostiach (Serre et al., 2018).

Vychádzajúc z európskej smernice (European Council, 2008) vyjadruje sektorová a subsektorová úroveň v českej a slovenskej proveniencii určitú formu vzorkovania prvkov kritickej infraštruktúry podľa určitých spoločných markantov a vlastností (sektorových kritérií). V rámci Českej republiky

príslušné nariadenie vlády (ČR, 2010) formuluje „odvětvové kritéria“ ako prvý stupeň identifikácie a označenia prvkov kritickej infraštruktúry. Na príklade energetiky je toto odvetvie/sektor rozdelený na tri hierarchické úrovne subsektorov. Prvá úroveň je tvorená subsektormi elektřina, zemní plyn, ropa a ropné produkty a centrální zásobování teplem. Príkladom druhej úrovne subsektorov subsektoru elektřina je výroba elektřiny, přenosová soustav a distribuční soustava a poslední úroveň subsektorov subsektora výroba elektřiny je výrobna s celkovým instalovaným elektrickým výkonem nejméně 500 MW, výrobna poskytující podpůrné služby s celkovým instalovaným elektrickým výkonem nejméně 100 MW, vedení pro vyvedení výkonu a zabezpečení vlastní spotřeby výrobny elektřiny a dispečink výrobce elektřiny. Pre úplnosť procesu identifikácie a určenia prvku kritickej infraštruktúry a teda stanovenie elementárnej úrovne sú následne použité ďalšie spoločné markanty a vlastnosti „průřezové kritéria“, ktoré proces určenia prvku uzatvárajú.

Sieťový charakter, vzájomná prepojenosť a potenciálne negatívne dôsledky vyplývajúce zo vzájomných väzieb a závislostí jednotlivých infraštruktúr je možné vnímať aj z pohľadu kaskádového šírenia prípadnej degradácie funkčnosti vybraných prvkov, ktoré je často spájané s potenciálnym synergickým efektom. Táto skutočnosť vytvorila objektívne potreby hodnotiť kaskádové a synergické efekty zlyhania prvkov kritickej infraštruktúry v kontexte pôsobenia vonkajších hrozieb a súčasne zraniteľnosti kritickej infraštruktúry ako celku. Hodnotenie kaskádového a synergického efektu je preto možné považovať za základ zvyšovania stability a resiliencie kritickej infraštruktúry. Toto konštatovanie vychádza z aktuálneho stavu poznania, kde sa pre príklad problematikou vzájomných závislostí podrobnejšie zaoberali Rinaldi et al. (2001), ktorí klasifikovali väzby na fyzické, kybernetické, geografické a logické, a upozornili tak na skutočnosť, že vzájomné závislosti zvyšujú riziko závažného narušenia alebo zlyhania funkcie viacerých subsystémov.

Pre sieťové odvetvia kritickej infraštruktúry absentujú explicitné definície (Hába, 2010). Častokrát sa konštatuje, že "sieťové odvetvie vyžaduje fixnú sieť pre distribúciu svojich služieb" (Murray a Grubesic, 2010). V tomto prípade sa uplatňuje sieťový efekt, ktorý poukazuje na fakt, že úžitok spotrebiteľov zo služieb dodávaných sieťovým odvetvím rastie s tým, ako rastie množstvo užívateľov majúcich prístup k tejto sieti. To sa dá chápať aj ako skutočnosť, že zvyšujúca sa súvzťažnosť, zvyšuje robustnosť či resilienciu sieťovej kritickej infraštruktúry. Silne sa ale prejavuje vplyv výstupov, pretože hodnota produktu/služby pre spotrebiteľov sa mení v niektorých prípadoch v závislosti od počtu spotrebiteľov užívajúcich tento produkt či službu, pokiaľ nie je samozrejme odvetvie kritickej infraštruktúry zásadne regulované.

Z pohľadu problematiky kritickej infraštruktúry sú do sieťových odvetví, a teda odvetví s najväčšou mierou súvzťažnosti, radené predovšetkým odvetvia energetiky (výroba, prenos a distribúcia elektrickej energie, zemného plynu a tepla), vodné hospodárstvo (verejné vodovody a kanalizácie) a informačných a komunikačných technológií. Dá sa súčasne konštatovať, že vybrané subjekty kritickej infraštruktúry pôsobiace v sieťových odvetviach patria medzi subjekty, ktoré majú vplyv na verejný záujem, slúžia potrebám verejnosti a chránia a podporujú blahobyt spoločnosti. Ochrana a stabilita týchto odvetví má strategický význam pre štát a jeho environmentálnu, sociálnu a hospodársku politiku (Machek a Hnilica, 2013).

Sieťový charakter a z neho vyplývajúce kaskádové a synergické efekty vytvárajú pragmatický potenciál narušenia resp. zlyhania funkcie kritickej infraštruktúry. V tejto súvislosti je preto potrebné identifikovať príčiny a ich intenzitu. Obecne je možné vychádzať z premisy, že bezpečnostné hrozby

budú mať charakter naturogénny, antropogénny a technogénny, kde miera dopadu bude úmerná úrovni konvergovanej bezpečnosti prvku kritickej infraštruktúry.

3.2 Definícia konvergovanej bezpečnosti v kontexte resiliencie kritickej infraštruktúry

V súčasnosti fungujú jednotlivé druhy bezpečnosti samostatne a nezávisle od ostatných druhov bezpečnosti. Tento spôsob zaistenia bezpečnosti má celé spektrum negatív. Medzi základné negatíva uvedenej skutočnosti patrí nemožnosť prepojiť demaskujúce príznaky vznikajúceho narušenia bezpečnosti, určené senzory v jednotlivých druhoch bezpečnosti, v jeden celok. Ďalším negatívom sú zvyšujúce sa náklady na zaistenie bezpečnosti, plynúce z nezávislého zaistenia jednotlivých druhov bezpečnosti. Čo prakticky znamená, že každý druh bezpečnosti je obvykle zaisťovaný samostatnou skupinou odborníkov, má vlastné bezpečnostné technológie a vlastné ochranné procesy, vlastný finančný rozpočet (Chen et al., 2011).

Formulované pragmatické dôvody poukazujú preto na skutočnosť, že je potrebné hľadať cesty pre zlučovanie jednotlivých druhov bezpečnosti do jedného celku. Tento trend vyústil v koncept konvergovanej bezpečnosti, ktorá predstavuje špecifický druh bezpečnosti, vzniknutý zlúčením viacerých zlučiteľných druhov bezpečnosti do jedného celku (Tyson, 2011). Takýto druh bezpečnosti umožňuje vďaka analýze súvzťažnosti prejavov narušenia bezpečnosti skôr (ešte v štádiu príznakov), rýchlejšie a lepšie odhaliť vznikajúce narušenie bezpečnosti a cielenejšie zaistiť jeho riešenie. Konvergovaná bezpečnosť zvyčajne zahŕňa fyzickú bezpečnosť a kybernetickú bezpečnosť (Anderson, 2007). Avšak, štruktúra zlučovaných druhov bezpečnosti môže byť aj iná. Trend konvergovanej bezpečnosti totiž predstavuje formálnu spoluprácu medzi predtým odlišnými bezpečnostnými funkciami. V kontexte rozvoja nových technologických koncepcií, ako sú napr. Internet of Things, Industry 4.0, Smart Cities, totiž dochádza k obrovskému nárastu dát, ktoré je možné vyhodnotiť iba na základe použitia algoritmov spracovania hromadných dát.

Spomínaná zlučiteľnosť vychádza predovšetkým z potreby ochrany rovnakých aktív referenčného objektu. Ďalšou podmienkou zlučiteľnosti sú časové charakteristiky prejavov narušenia bezpečnosti, ktoré by mali byť v približne rovnakých intenciách. V rámci vyššie uvedeného príkladu konvergovanej bezpečnosti budú prejavy v časovom rozmedzí sekúnd – minút – hodín. Ak by došlo k zlúčeniu druhov bezpečnosti, kedy u jedného dochádza k zmenám v minútach a v ďalšom v rokoch, potom by zlúčenie do konvergovanej bezpečnosti nemalo zmysel, pretože dominantnú úlohu by zohrával druh bezpečnosti s časovo obmedzenými zmenami. Základné princípy, na ktorých je konvergovaná bezpečnosť postavená, sú prezentované na obrázku 4.

Obrázok 4: Základné princípy konvergovanej bezpečnosti (Hromada et al., 2021)

Z vyššie uvedených princípov vyplýva, že konvergovaná bezpečnosť sa zaisťuje v rámci spoločného referenčného objektu. Tento referenčný objekt má jedno alebo niekoľko aktív a všetky zahrnuté druhy bezpečnosti sa podieľajú na zaistení ich bezpečnosti. Konvergovaná bezpečnosť zlučuje tieto druhy bezpečnosti do jedného celku (Contos et al., 2007). To umožňuje vyhodnocovať stav bezpečnostnej situácie ako jeden obraz, v ktorom sa premietajú všetky čiastkové bezpečnostné situácie jednotlivých druhov bezpečnosti. Pridanou hodnotou zlúčenia predtým nezávislých druhov bezpečnosti je možnosť vnímania súvzťažnosti jednotlivých prejavov narušenia bezpečnosti v jeden celok, rýchlejšie odhalenie narušenia bezpečnosti, jeho spôsobu, rozsahu a predikcia možného scenára ďalšieho priebehu. Medzi ďalšie významné prínosy konvergovanej bezpečnosti patrí komplexné a aktuálne hodnotenie bezpečnostnej situácie. Toto hodnotenie umožňuje bezpečnostnú situáciu adekvátne riešiť a tým minimalizovať negatívne dopady narušenia bezpečnosti. Z pohľadu referenčného objektu sa stav bezpečnostnej situácie hodnotí najčastejšie pomocou stavu resiliencie jeho systému ochrany (bezpečnostného systému), prípadne resiliencie referenčného objektu ako takého. Pre konvergovanú bezpečnosť platí, že sa u nej hodnotí resiliencia systému ochrany (Dunn Cavelty et al., 2015). Neposudzuje sa stav napĺňania cieľovej funkcie referenčného objektu, ale stav ochrany aktív referenčného objektu prostredníctvom systému ochrany referenčného objektu. Systém ochrany je tvorený opatreniami prijatými v jednotlivých druhoch bezpečnosti.

3.2.1 Východiská posudzovania resiliencie z pohľadu konvergovanej bezpečnosti

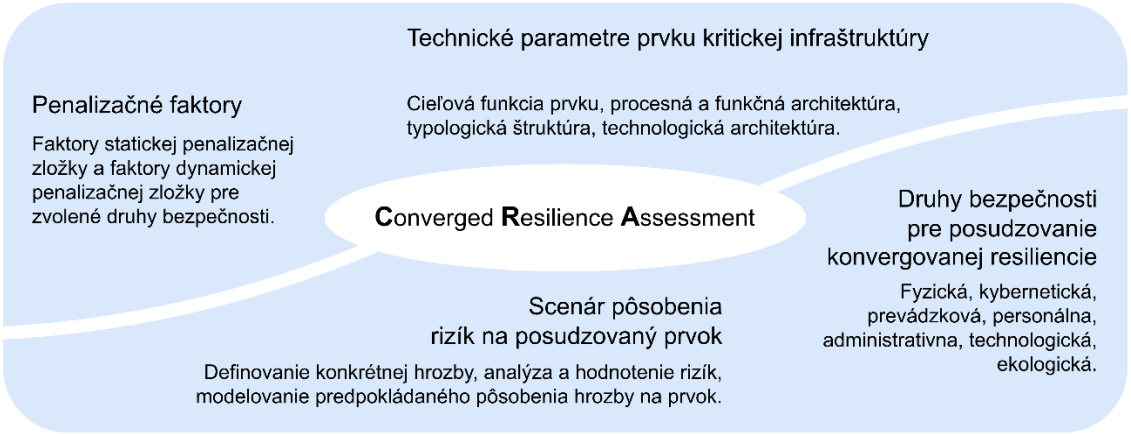
Resiliencia patrí medzi základné parametre, ktoré sa v rámci jednotlivých druhov bezpečnosti sledujú (Králík et al., 2018). Resiliencia je v tomto kontexte vnímaná ako vlastnosť systému ochrany referenčného objektu, ktorá vyjadruje, ako je daný celok pripravený chrániť a brániť referenčný objekt a jeho aktíva, prípadne zvládať pôsobenie škodiaceho účinku jednotlivých hrozieb (Řehák et al., 2018). Priebežná a aktuálna znalosť úrovne resiliencie systému ochrany umožňuje jednotlivé narušenia bezpečnosti riešiť a prijímať účinné opatrenia na ich nápravu. Ak dochádza vplyvom nedostatkov v organizácii a zaistení bezpečnosti, vplyvom technických porúch či vplyvom

klimatických podmienok k zhoršovaniu jednotlivých parametrov systému ochrany, znižuje sa tak aj jeho resiliencia (Hess et al., 2018). Neriešenie poklesu resiliencie môže v prípade narušenia bezpečnosti viesť k ľahšiemu prekonaniu systému ochrany a vzniku ujmy na aktívach referenčného objektu. Posudzovanie resiliencie v reálnom čase by malo takéto situácie identifikovať a umožniť tak prijať adekvátne opatrenia na ochranu aktív, obnovu resiliencie a nápravu stavu (Fath et al., 2015).

Resiliencie systému ochrany referenčného objektu z pohľadu konvergovanej bezpečnosti predstavuje schopnosť opatrení (realizovaných v jednotlivých druhoch bezpečnosti zahrnutých do konvergovanej bezpečnosti) ochrániť jeho aktíva a zaistiť tak napĺňanie cieľovej funkcie referenčného objektu. Posudzovanie resiliencie by malo odrážať jej aktuálny stav ako vlastnosti referenčného objektu. Tento stav je možné sledovať prostredníctvom snímania prejavov či zmien vonkajších a vnútorných faktorov (Coaffe a Fussey, 2015).

Všeobecne platí, že každá zmena sa môže do resiliencie premietnuť kvalitatívne alebo kvantitatívne, a preto môže byť ohodnotená vplyvmi a dopadmi na resilienciu referenčného objektu. Posudzovanie resiliencie tak môže byť založené primárne na snímaní tých zmien stavu faktorov, ktoré sa do zmien resiliencie premietajú podstatne (Argyroudis et al., 2020). V tomto prípade môže byť miera vplyvu týchto faktorov na resilienciu prvku vyjadrená formou penalizácie. Prostredníctvom penalizácie sa posudzuje, o koľko sa pri zmene stavu znížila úroveň resiliencie systému ochrany. Všetky kľúčové faktory, ktoré popisujú zmeny resiliencie systému ochrany vzhľadom na určité aktíva, sú označované ako penalizačné faktory.

Na základe vyššie uvedeného je možné konštatovať, že konkrétna úroveň resiliencie systému ochrany je funkciou všetkých podstatných zmien a prejavov, ktorých dôsledky v danom čase platia a majú na referenčný objekt zásadný vplyv z pohľadu ujmy na jeho aktívach. V tomto kontexte bol nadefinovaný rámec posudzovania konvergovanej resiliencie (viď obrázok 5), ktorý je východiskom posudzovania resiliencie z pohľadu konvergovanej bezpečnosti.



Obrázok 5: Rámec posudzovania konvergovanej resiliencie (Hromada et al., 2021)

Podstatou metódy posudzovania konvergovanej resiliencie (CRA method) je vymedzenie štyroch oblastí potrebných na zabezpečenie podpory procesu hodnotenia. Tieto oblasti poskytujú nielen informácie potrebné na hodnotenie (technické parametre prvku a penalizačné faktory), ale aj informácie vymedzujúce prostredie, v ktorom bude hodnotenie prebiehať. Vymedzenie tohto prostredia je realizované výberom konkrétnych druhov bezpečnosti pre posudzovanie

konvergovanej resiliencie a definovaním konkrétneho scenára pôsobenia rizík na posudzovaný prvok.

4 Doterajší vedecký prínos

Doterajšia vedecká práca v oblasti konvergovanej bezpečnosti v kontexte resiliencie kritickej infraštruktúry súvisí s výskumom prístupov k ochrane kritickej infraštruktúry vzhľadom na vybrané oblasti bezpečnostných hrozieb (myslí sa tým oblasť vnútorných bezpečnostných hrozieb) a s výskumom prístupov k minimalizácii dopadov narušenia či zlyhania funkcie kritickej infraštruktúry (myslí sa tým oblasť vonkajších bezpečnostných hrozieb).

4.1 Výskum v oblasti vnútorných bezpečnostných hrozieb

Výskum prístupov k ochrane kritickej infraštruktúry vzhľadom na vybrané skupiny bezpečnostných hrozieb je primárne zameraný na:

- funkčnosť systémov fyzickej ochrany s využitím vybraných aspektov modelovania a simulácie,
- tvorbu integrálneho systému riadenia ochrany,
- hodnotenie odolnosti prvkov kritickej infraštruktúry,
- hodnotenie statickej resiliencie prvkov kritickej infraštruktúry,
- konvergovanú bezpečnosť a resilienciu kritickej infraštruktúry.

4.1.1 Funkčnosť systémov fyzickej ochrany s využitím vybraných aspektov modelovania a simulácie

Výskum v oblasti ochrany prvkov kritickej infraštruktúry bol v novodobej histórii pragmaticky viazaný na fyzickú bezpečnosť a implementáciu systémov fyzickej ochrany. Navzdory právnemu a hlavne normatívnemu ukotveniu predmetnej problematiky, chýbal aspekt optimalizácie použitia jednotlivých komponentov systému fyzickej ochrany, vzhľadom na ich funkčnosť.

V tejto súvislosti preto bola východiskom formulácia základných a očakávaných funkcií v rámci jednotlivých zón vybraného prvku kritickej infraštruktúry:

- detection / detekcia,
- delay / spomalenie,
- response /reakcia.

Štruktúra a prepojenosť jednotlivých komponentov systému fyzickej ochrany vzhľadom na ich funkčnosť vytvorila základ pre použitie vybraných optimalizačných modelov. Tak ako uvádza publikácia (Lukáš a Hromada, 2011) jedným z použiteľných modelov je model EASI (Estimate of Adversary Sequence Interruption).

Estimate of Adversary Sequence Interruption

Probability of Guard Communication		Response Force Time (in Seconds) Mean	Standard Deviation
0,97		172,8	78,8

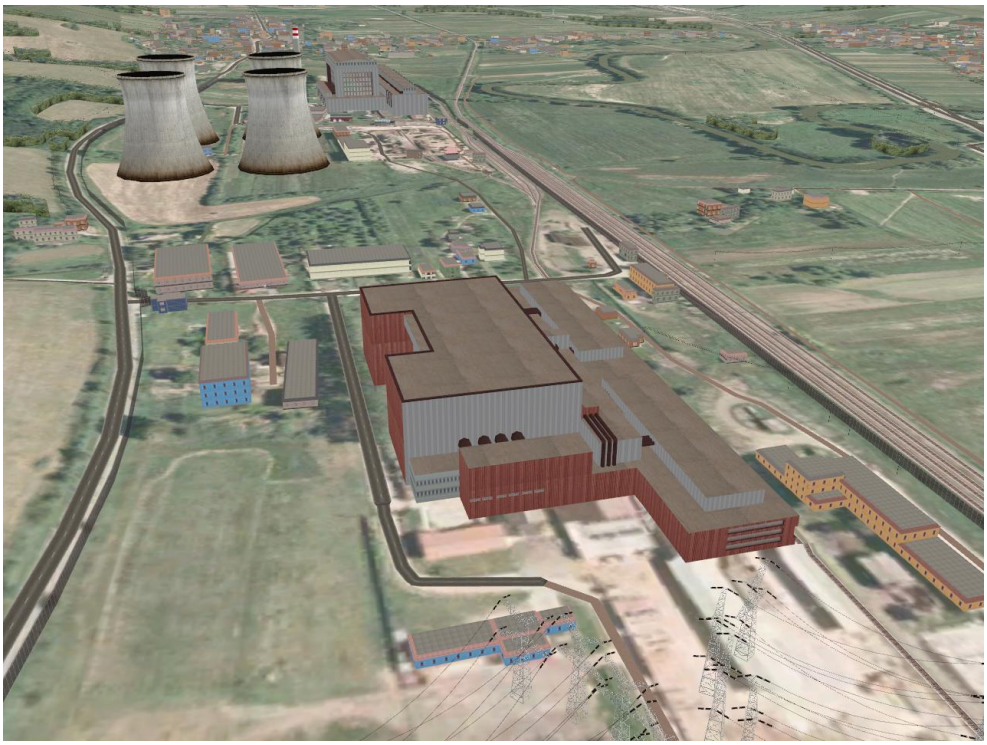
Task	Description	P(Detection)	Location	Delays (in Seconds): Mean:	Standard Deviation
1	Zone 1	0,9	I	25,5	9,2
2	Zone 2	0,9	I	75	22,5
3	Zone 3	0,9	I	113,4	32,6
4	Zone 4	0,9	I	285	85,5
5	Zone 5	0,9	I	77,7	22,1
6	Zone 6	0,9	I	285	85,5
7	Zone 7	0,9	I	17,1	4,1
8	Zone 8	0	I	0	0
9					
10					
11					
12					

Probability of Interruption:	0,969935157

Obrázok 6: Využitie modelu EASI pre optimalizáciu systému fyzickej ochrany (Lukáš a Hromada, 2011)

Predmetný model a jeho využitie vytvorilo základ pre hodnotenie pravdepodobnosti úspešného prerušenia činnosti narušiteľa.

Vzhľadom na určitú mieru neurčitosti a chybovosti bolo ambíciou autora potvrdiť výstupy modelu vhodnou formou simulácie, ktorá znižovala mieru zjednodušeného chápania reality a súčasne verifikovala výstupy modelu EASI. V spolupráci so Simulačným centrom Akadémie ozbrojených síl v Liptovskom Mikuláši a s využitím simulačného nástroja OTB SAF bol vytvorený model prostredia referenčného prvku elektroenergetickej kritickej infraštruktúry, v rámci ktorého boli autorom prostredníctvom simulácie narušenia objektu verifikované výstupy modelu EASI.



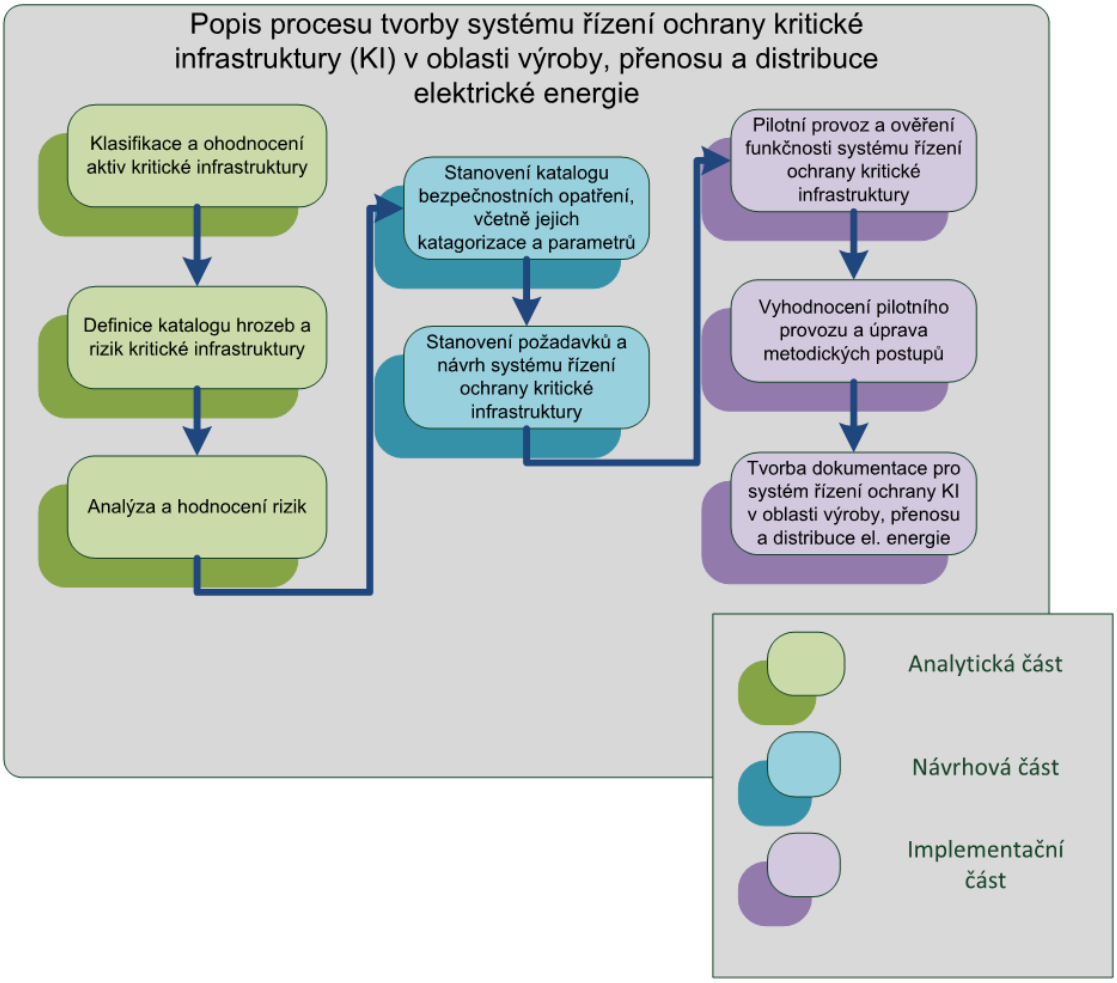
Obrázok 7: Využitie OTB SAF prostredia pre verifikáciu výstupov EASI modelu (Lukáš a Hromada, 2011)

Vzhľadom k stanoveným parametrom a funkčnosti jednotlivých komponentov systému fyzickej ochrany sa následne dala konštatovať celková funkčnosť systému a relevantnosť využitia modelu EASI v rámci optimalizácie systému fyzickej ochrany prvku kritickej infraštruktúry.

4.1.2 Tvorba integrálneho systému riadenia ochrany

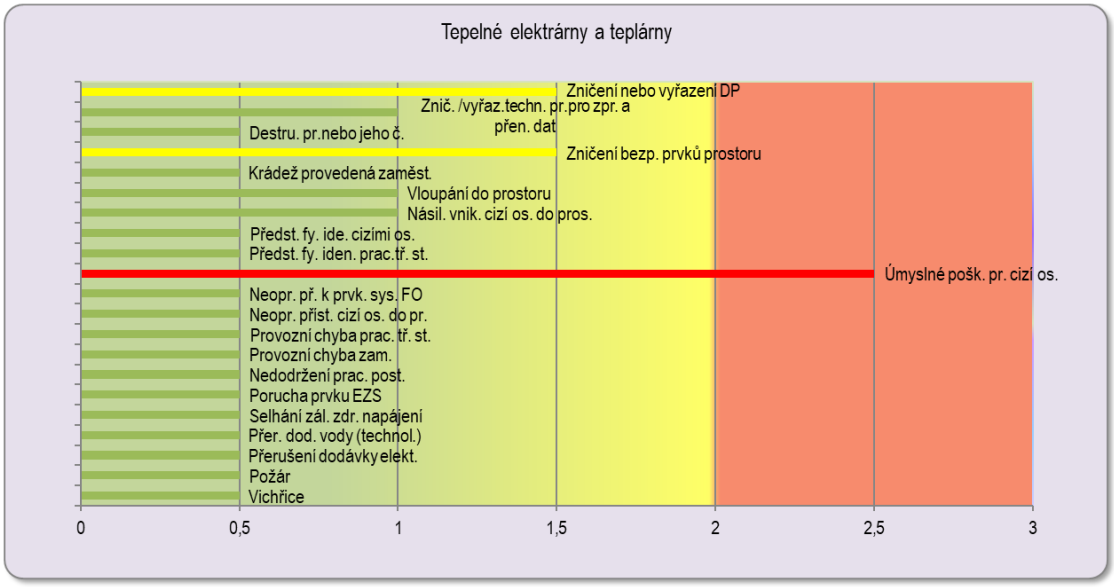
Vývoj problematiky ochrany prvkov kritickej infraštruktúry bol, vzhľadom na požiadavky prevádzkovateľov/subjektov kritickej infraštruktúry a aktuálny stav bezpečnostného prostredia, rozšírený aj na ďalšie oblasti bezpečnosti. Tak ako sa uvádza v publikácii (Hromada a Lukáš, 2012) ďalšími oblasťami bezpečnosti boli informačná bezpečnosť, business continuity management, administratívna a personálna bezpečnosť.

Tento koncept bol následne implementovaný aj do národného prostredia bezpečnostného výskumu a zhmotnený autorom do certifikovanej metodiky „Metodika zajištění ochrany kritické infrastruktury v oblasti výroby, přenosu a distribuce elektrické energie“ (Deloitte, 2012).



Obrázok 8: Proces tvorby systému riadenia ochrany kritickej infraštruktúry (Deloitte, 2012)

Tak ako bolo konštatované, predmetný integrálny systém riadenia ochrany vybranej skupiny prvkov kritickej infraštruktúry vychádzal z aktuálneho stavu bezpečnostného prostredia a teda zo špecifikovaných bezpečnostných hrozieb a z nich vyplývajúcich rizík.



Obrázok 9: Aktuálny stav bezpečnostných rizík vybranej skupiny prvkov kritickej infraštruktúry (Deloitte, 2012)

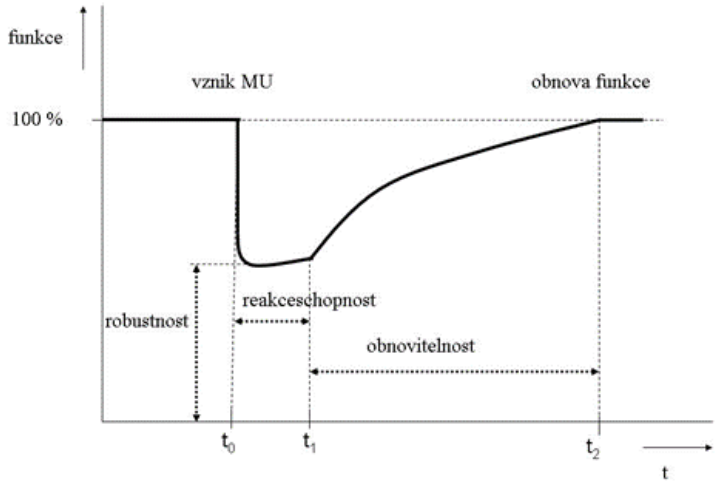
Vzhľadom na predmetné skutočnosti bola autorom následne formalizovaná štruktúra integrálneho systému riadenia bezpečnosti, implementujúca aspekty fyzickej, informačnej, administratívnej a personálnej bezpečnosti a súčasne vybraných aspektov objektového krízového riadenia a plánovania. Navzdory určitej evolúcii je predmetná problematika stále aktuálna a kontinuálne sa jej autor venuje aj v ďalších publikáciách (Hromada et al., 2020).

4.1.3 Hodnotenie odolnosti prvkov kritickej infraštruktúry

Tak ako v prípade systémov fyzickej ochrany a ich funkčnosti, bolo výzvou aj integrálny systém riadenia ochrany do určitej miery optimalizovať, a to vzhľadom na pôsobenie vnútorných a vonkajších faktorov. Oblasťou výskumu bola preto problematika odolnosti v širších súvislostiach. Vzhľadom na výskumnú činnosť autora s väzbou na problematiku kritickej infraštruktúry bola v tejto súvislosti odolnosť prvku kritickej infraštruktúry vnímaná ako schopnosť zabezpečiť jeho fungovanie v podmienkach pôsobenia vonkajších a vnútorných činiteľov. Odolnosť prvku kritickej infraštruktúry je tiež možné charakterizovať ako schopnosť prekonať účinok negatívneho pôsobenia a zabezpečiť kontinuálnu činnosť prvku kritickej infraštruktúry. Odolnosť sa dosahuje celým spektrom spôsobov, ako napr. schopnosťou vydržať účinky negatívneho pôsobenia, flexibilitou činnosti, absorpciou účinku negatívneho pôsobenia, adaptáciou na novú situáciu, zapojením redundantných prvkov, obnovou funkcie atď. (Hromada et al., 2013).

Za základné atribúty odolnosti boli považované:

- robustnosť,
- pripravenosť,
- reakcieschopnosť,
- obnoviteľnosť.



Obrázok 10: Základné atribúty odolnosti (Hromada et al., 2013)

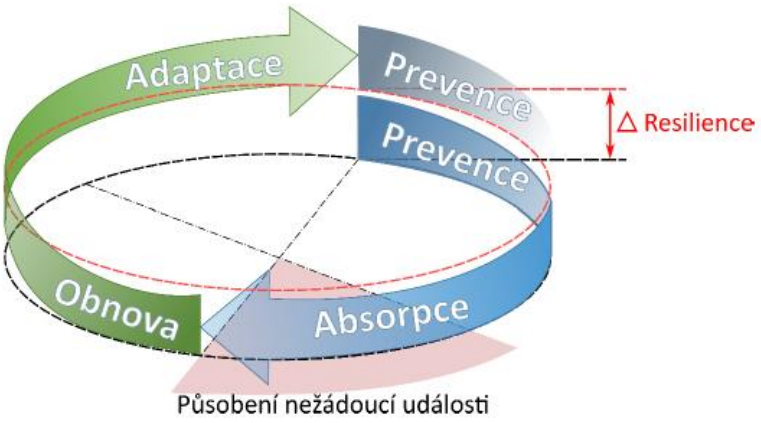
Základným procesným modelom hodnotenia odolnosti bola následne:

- systémová analýza hodnoteného prvku kritickej infraštruktúry,
- analýza a hodnotenie rizík,
- stanovenie hodnotených oblastí zabezpečenia (bezpečnosti),
- určenie hodnôt atribútov a výpočet veľkosti ukazovateľov,
- výpočet stupňa odolnosti prvku kritickej infraštruktúry,
- vyhodnotenie odolnosti prvku kritickej infraštruktúry.

V rámci ďalšej výskumnej činnosti autora boli následne rozpracované jednotlivé atribúty odolnosti, kde vzhľadom na odborné zameranie, s väčším detailom na robustnosť prvkov kritickej infraštruktúry, sa jednalo o aspekty fyzickej, informačnej, administratívnej a personálnej bezpečnosti (Hromada a Lukáš, 2013) , (Řehák et al., 2020) alebo (Hromada et al., 2020).

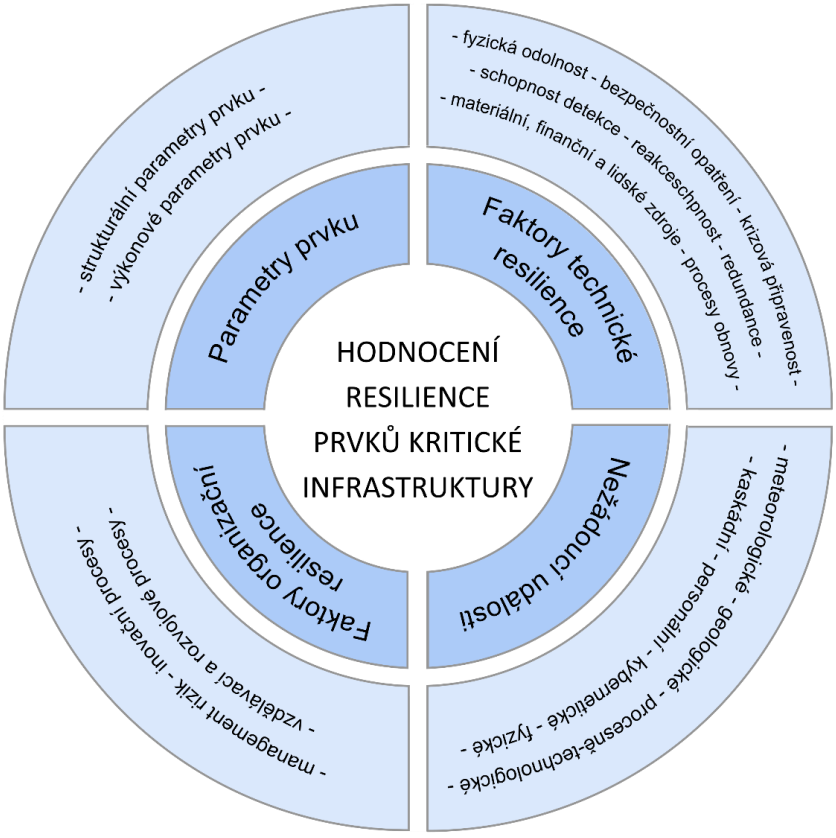
4.1.4 Hodnotenie statickej resiliencie prvkov kritickej infraštruktúry

Vzhľadom na ďalšiu výskumnú činnosť autora v rámci problematiky odolnosti bol pojem odolnosť logicky (vzhľadom na správne terminologické vnímanie pojmu) viazaný na anglický ekvivalent resiliencia. V tejto súvislosti resiliencia predstavuje vnútornú pripravenosť subsystémov kritickej infraštruktúry na nežiaduce udalosti, resp. schopnosť týchto subsystémov zaistiť a udržiavať si svoje funkcie pri negatívnom pôsobení vnútorných a/alebo vonkajších faktorov.



Obrázok: 11 Cyklus resiliencie kritickej infraštruktúry (Řehák et al., 2018)

Resilienciu prvkov kritickej infraštruktúry možno v súčasnej dobe merať tzv. statickým spôsobom. Tento spôsob poskytuje informácie o úrovni resiliencie, ktorú prvok dosahuje v čase pred pôsobením nežiaducej udalosti. Tento koncept a tvrdenie bolo rozpracované v rámci metódy Critical Infrastructure Elements Resilience Assessment (CIERA) vzniknutej v rámci riešenia projektu VI20152019049 "RESILIENCE 2015: Dynamické hodnocení odolnosti souvztažných subsystémů kritické infrastruktury", kde dochádza k hodnoteniu základných štrukturálnych a výkonových parametrov hodnoteného prvku, faktorov determinujúcich technickú resilienciu, faktorov determinujúcich organizačnú resilienciu a konkrétne nežiaduce udalosti, voči ktorým je resiliencia hodnotená (Řehák et al., 2019).



Obrázok 12: Rámec hodnotenia resiliencie prvkov kritickej infraštruktúry (Řehák et al., 2019)

Je zrejmé, že aktuálne vytvorený komplexný prístup hodnotenia resiliencie vychádzajúci z menovanej Critical Infrastructure Elements Resilience Assessment (CIERA) metódy rozvíja procesný model hodnotenia resiliencie, kde algoritmus hodnotenia resiliencie je logicky radený na:

- výber prvku,
- deskripcia prvku,
- deskripcia hrozby,
- hodnotenie robustnosti,
- hodnotenie obnoviteľnosti,
- hodnotenie adaptability,
- výpočet resiliencie prvku,
- vyhodnotenie resiliencie, identifikácia slabých miest a návrh opatrení.

Vytvorené metodika, či algoritmus hodnotenia resiliencie tak stanovuje vo svojej postate postup pre zber, evidenciu a analýzu relevantných technických a štrukturálnych parametrov o prvku kritickej infraštruktúry a vytvára spôsob hodnotenia aktuálneho stavu, ako východiska pre chápanie vybraných aspektov resiliencie prvkov kritickej infraštruktúry, hodnotenie slabých miest či formuláciu opatrení, zvyšujúcich statickú hodnotu resiliencie.

4.1.5 Konvergovaná bezpečnosť v kontexte resiliencie kritickej infraštruktúry

Tak ako bolo konštatované a vyplýva z predošlých výskumných prác autora, resiliencia systému ochrany referenčného objektu z pohľadu konvergovanej bezpečnosti predstavuje schopnosť opatrení (realizovaných v jednotlivých druhoch bezpečnosti zahrnutých do konvergovanej bezpečnosti) ochrániť jeho aktíva a zaistiť tak napĺňanie cieľovej funkcie referenčného objektu. Posudzovanie resiliencie by malo odrážať jej aktuálny stav ako vlastnosti referenčného objektu. Tento stav je možné sledovať prostredníctvom snímania prejavov či zmien vonkajších a vnútorných faktorov (Coaffe and Fussey, 2015).

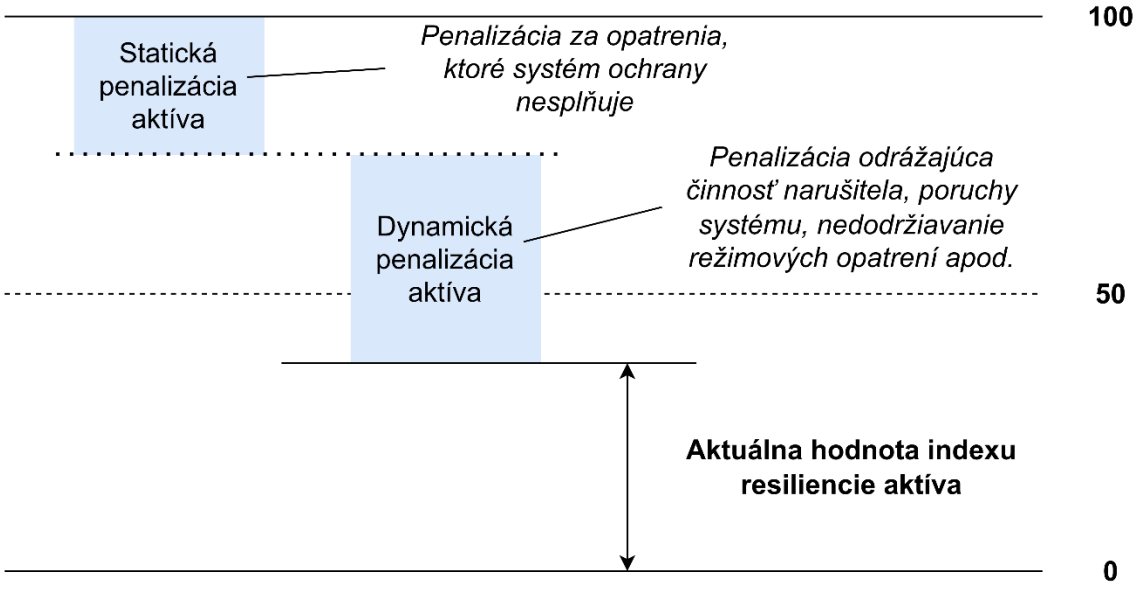
Na základe aktuálnych požiadaviek a potrieb reflexie aktuálnych bezpečnostných výziev kritickej infraštruktúry, bola autorom vytvorená metóda **Converged Resilience Assessment (CRA)**. Táto umožňuje posudzovanie resiliencie z pohľadu konvergovanej bezpečnosti. Konvergovaná bezpečnosť v tomto prípade zlučuje (konverguje) fyzickú, kybernetickú a prevádzkovú bezpečnosť do jedného celku. Zameriava sa najmä na informačný a situačný manažment, ktorý integruje a koreluje systémové a senzorické informácie za účelom získania prehľadu o danej situácii a následného efektívneho zvládnutia jej riešenia. Posudzovanie resiliencie je možné realizovať pre jednotlivé aktíva prvku kritickej infraštruktúry ako celku. V prípade, že je potrebné objekt tohto prvku dekomponovať na časti, je možné hodnotiť resilienciu po jednotlivých častiach a výslednú úroveň resiliencie prvku získať agregáciou jednotlivých čiastkových resiliencií.

Podstatou metódy CRA je určovanie resiliencie systému ochrany prvkov kritickej infraštruktúry z pohľadu konvergovanej bezpečnosti, a to prostredníctvom indexu resiliencie referenčného objektu. Tento index vyjadruje, do akej miery sú v danom časovom okamihu chránené aktíva referenčného objektu voči hrozbám, ktoré spadajú do pôsobnosti vybraných druhov bezpečnosti zahrnutých do konvergovanej bezpečnosti.

Vzhľadom na to, že konvergovaná bezpečnosť obsahuje viacero druhov bezpečnosti a referenčný objekt zahŕňa spravidla viac aktív, musia byť pre každý druh bezpečnosti najprv stanovené indexy resiliencie jednotlivých aktív. Z týchto hodnôt sa následne agregáciou stanoví výsledný index

resiliencie referenčného objektu pre daný druh bezpečnosti, to jest fyzická, kybernetická a prevádzková.

Index konvergovanej resiliencie aktíva je teda agregáciou indexov resiliencie aktíva pre jednotlivé druhy bezpečnosti. Samotný výpočet indexu resiliencie sa realizuje s využitím penalizačných faktorov tak, že od počiatočnej hodnoty sa odpočíta zníženie resiliencie spôsobené penalizačnými faktormi. Penalizačné faktory sú rozdelené na statické a dynamické. Tieto faktory závisia od dvoch častí systému ochrany, od statickej časti a od dynamickej časti. Statická časť odráža získanú penalizáciu za opatrenia, ktoré by mal systém ochrany mať a v danom časovom okamihu ich nemá. Obvykle sa pri tom vychádza zo štandardu, ktorý definuje štruktúru a opatrenia systému ochrany v danom druhu bezpečnosti. Medzi kľúčové opatrenia patrí bezpečnostná politika, fyzická ostraha, mechanické zábranné systémy, poplachové systémy, antivírusová ochrana atď. Dynamická časť vzorca potom odráža penalizáciu získanú činnosťou narušiteľa, poruchami, nedodržiavaním režimových opatrení a dynamicky koriguje hodnotu statickej penalizácie (viď obrázok 13).



Obrázok 13: Podstata výpočtu resiliencie pre jednotlivé druhy bezpečnosti (Hromada et al., 2021)

Penalizačný údaj (penalizácia) je hodnota vygenerovaná staticky alebo dynamicky na základe určitého zistenia alebo zmeny sledovaného faktora (činiteľa), majúca alebo odrážajúca podstatný vplyv na resilienciu. Výška veľkosti penalizácie je priamo úmerná miere vplyvu zmeny alebo zistenia na resilienciu.

V rámci procesu hodnotenia resiliencie sú detekované problémy (napr. absencia bezpečnostnej dokumentácie, poruchy poplachových zariadení, detekcia vniknutia do objektu atď.) považované za penalizačné faktory, ktoré túto hodnotu znižujú. Tak ako bolo už konštatované, penalizačné faktory je možné klasifikovať na statické a dynamické.

Statické faktory sú také vplyvy, ktoré pôsobia na systém ochrany do okamihu, kým sú odstránené. Ide ale o dlhodobé pôsobenie. V oblasti statickej penalizácie sú obsiahnuté problémy/incidenty, ktoré vychádzajú väčšinou z neexistencie procesov nutných pre zvládnutie bezpečnosti, neexistencie prvkov fyzickej bezpečnosti, nesúladu s platnou legislatívou, neuskutočnenej kontroly, revízie atď.

Dynamické faktory predstavujú faktory, ktoré sa samy v čase menia na základe zmien bezpečnostnej situácie, a doba ich pôsobenia nie je presne odhadnuteľná. Patrí sem napr. detekcia pohybu

pomocou kamerového systému, narušenie bezpečnosti hlásené detektormi narušenia, poruchy zabezpečovacích systémov či výpadky dodávky elektrickej energie. U týchto faktorov je nutné stanovenie sledovaného časového pôsobenia faktora. Počas pôsobenia je faktor identifikovaný ako incident a podieľa sa na znížení resiliencie objektu. Po uplynutí doby je faktor archivovaný a resiliencia objektu sa opäť zvýši.

Na základe uvedeného bol stanovený postup a procesný model posudzovania resiliencie referenčného objektu (viď obrázok 14).

Obrázok 14: Postup posudzovania resiliencie referenčného objektu (Hromada et al., 2021)

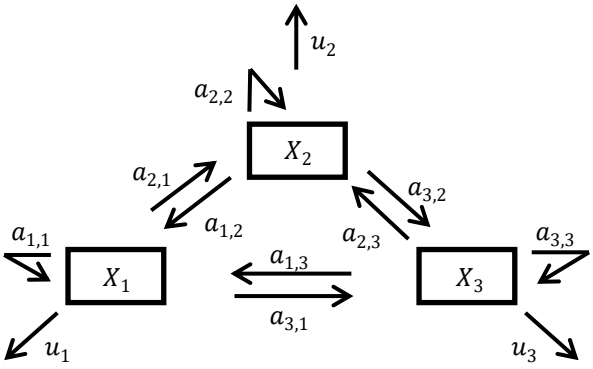
Prínosom metódy CRA je reflexia vplyvu všetkých udalostí do konvergovanej resiliencie systému. Metóda sa zameriava najmä na informačný a situačný manažment, ktorý integruje a koreluje informácie zo systémov a senzorov za účelom získania prehľadu o danej situácii a následného efektívneho zvládnutia jej riešenia. Aplikačným prínosom metódy je predikčné posudzovanie resiliencie prvkov, ktoré poskytuje manažmentu organizácie informácie o schopnosti prvkov odolávať pôsobeniu hrozieb s multispektrálnym dopadom do viacerých oblastí bezpečnosti.

Z prezentovaného je zrejmé, že dávanie ochrany prvkov kritickej infraštruktúry do kontextu resiliencie je vhodným a očakávaným vývojovým krokom zaistenia funkčnosti základného systému štátu. Rozšírenie chápania resiliencie o aspekt multispektrálneho hodnotenia dopadu do viacerých oblastí bezpečnosti prostredníctvom konvergencie, vytvára hmatateľný predpoklad predikcie vývoja bezpečnostnej situácie.

4.2 Výskum v oblasti vonkajších bezpečnostných hrozieb

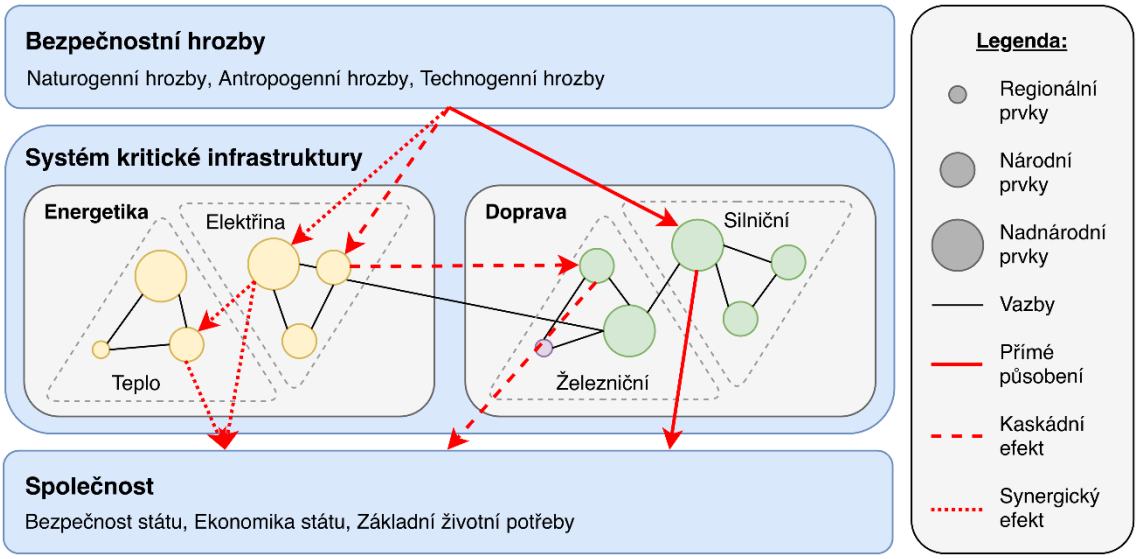
Chápanie a význam minimalizácie narušenia funkcie kritickej infraštruktúry (ako výskumu v oblasti vonkajších bezpečnostných hrozieb) vychádza z celého spektra možných prístupov, modelov a oblastí. Vzhľadom na výskumné zameranie projektu VI20152019049 "RESILIENCE 2015: Dynamické hodnocení odolnosti souvztažných subsystémů kritické infrastruktury" sa primárnou oblasťou výskumu stalo hodnotenie kaskádových a synergických efektov.

Východiskom bola aplikácia Leontievovho ekonomického modelu zameraného na popis rovnovážneho stavu produkcie (viď obrázok 15).



Obrázok 15: Diagram pre tri subjekty (Hromada et al., 2013)

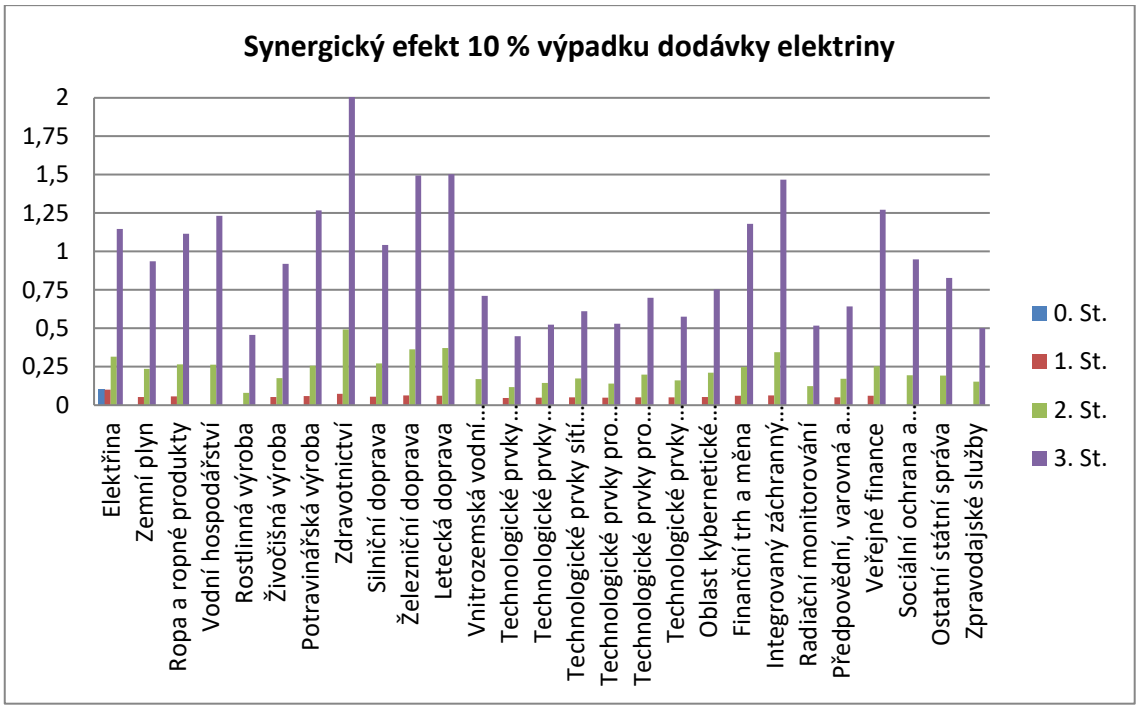
Následne bol spomínaný model transformovaný do oblasti kritickej infraštruktúry, kde došlo k hodnoteniu spôsobu a rozsahu šírenia priamych, kaskádových a synergických dopadov (viď obrázok 16).



Obrázok 16: Spôsoby šírenia dopadu v systéme kritickej infraštruktúry (Řehák a Hromada, 2018)

Obecne je možné konštatovať, že priame dopady vyjadrujú konkrétne pôsobenie hrozby na funkčné parametre vybraného prvku, kaskádové dopady vyjadrujú určitú eskaláciu šírenia obmedzenia alebo zlyhania funkčného parametra jedného prvku do ostatných závislých (dependentných) systémov kritickej infraštruktúry. Synergické dopady sú dopady spôsobené narušením alebo zlyhaním dvoch a viacerých subsystémov kritickej infraštruktúry, ku ktorým dochádza v rovnakom čase, čím sa zosilňujú dopady týchto udalostí na spoločnosť.

Príkladom synergického efektu môže byť modelovania 10 % výpadku dodávky elektrickej energie na ostatné subsektory kritickej infraštruktúry (viď obrázok 17).



Obrázok 4: Synergický efekt výpadku dodávky elektrickej energie (Hromada, 2016)

Zhmotnením vytvoreného modelu bol vývoj metódy **Cascading Impact Assessment – CIA** (Řehák et al., 2018a). Základom procesu hodnotenia je formulácia statického stochastického modelu subsystémov kritickej infraštruktúry a závislostí medzi nimi. Tento model je založený na percentuálnom predpoklade hodnoty pravdepodobnosti a intenzity dopadu. Podstatou tejto metódy je posúdenie všetkých sektorov nachádzajúcich sa vo vybranom území, zhodnotenie ich resiliencie a väzieb a následné vytvorenie štrukturálnej mapy rizika šírenia kaskádových dopadov.

Na účely hodnotenia synergických efektov v systéme kritickej infraštruktúry bola vyvinutá metóda **SYNergstic EFfect Impact Assessment – SYNEFIA** (Řehák et al., 2016). Podstatou metódy je hodnotenie medzisektorových synergických dopadov, ktoré je založené na stanovení súvzťažnosti a resiliencie záujmových sektorov. Hodnotenie súvzťažnosti vychádza z posúdenia miery vzájomnej aktivity a pasivity medzi týmito sektormi. Na základe toho dochádza k stanoveniu miery dopadov každého sektora na spoločnosť. V záverečnej fáze metódy dochádza k stanoveniu synergického efektu pri zlyhaní dvoch a viacerých sektorov v dôsledku kaskádového efektu.

Vzhľadom k prezentovanému je prínos a výskum v oblasti vonkajších bezpečnostných hrozieb dávaný do kontextu identifikácie, hodnotenia a modelovania kaskádových a synergických efektov, ktoré zásadným spôsobom ovplyvňujú úroveň resiliencie a to aj v kontexte konvergovanej bezpečnosti kritickej infraštruktúry. Vzhľadom na filozofiu konvergencie bezpečnosti je to o prepojení aspektov zabezpečenia (Security) s aspektom bezpečnosti (Safety).

4.3 Využiteľnosť výsledkov v praxi

Prezentované výsledky vedecko-výskumnej činnosti a to aj vzhľadom k potrebám projektov bezpečnostného výskumu Ministerstva vnitra ČR boli testované a súčasne aplikované do praxe. V oblasti Security sa jedná primárne o aplikáciu metód Critical Infrastructure Elements Resilience Assessment (CIERA) a Converged Resilience Assessment (CRA). Vznik oboch menovaných metód bol podmienený tvorbou „Metodiky zajištění ochrany kritické infrastruktury v oblasti výroby, přenosu a distribuce elektrické energie“. Je preto zrejmé, že užívateľskou skupinou sú subjekty kritickej infraštruktúry v sektoroch energetiky, dopravy, informačných a komunikačných technológií a ostatnej štátnej správy. Na testovaní predmetných metód sa v Českej republike podieľali subjekty ČEPS, a.s., České dráhy, a.s., ČEZ, a.s. a Pre, a.s.. V Slovenskej republike Stredoslovenská distribučná, a.s., Západoslovenská distribučná, a.s. a Železnice Slovenskej republiky. Motiváciou tvorby metodických nástrojov bola do určitej miery absencia argumentačného potenciálu styčných bezpečnostných zamestnancov vo vzťahu k štandardizácii bezpečnostných opatrení s preneseným významom na konvergenciu bezpečnosti a resilienciu prvkov kritickej infraštruktúry.

5 Koncepcia pedagogickej práce

Je zrejmé, a to vzhľadom na vedecko-výskumnú činnosť akademického pracovníka a jeho spoluprácu s praxou, že pedagogická činnosť musí byť významne formovaná výstupmi a výsledkami vedeckej práce a praktickými poznatkami. To je svojím spôsobom potvrdené faktom, že rozvoj bezpečnostného vzdelávania môže byť považovaný za významný pilier zvyšovania úrovne ochrany a resiliencie kritickej infraštruktúry. Toto tvrdenie bolo detailne rozpracované v publikácii (Hromada a Lukáš, 2014), kde zvolená štruktúra bezpečnostných oborov má významný vplyv na kvalitu jednotlivých atribútov resiliencie.

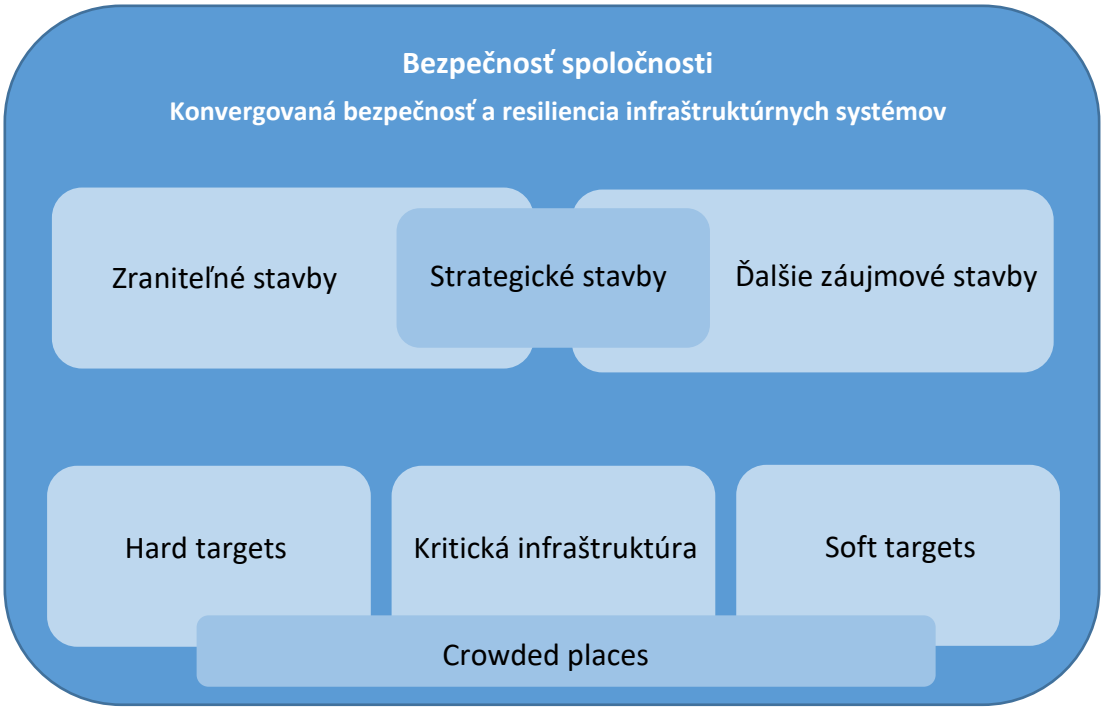
Koncepcia rozvoja pedagogickej práce by mala vychádzať a napĺňať nasledujúce ciele:

- V rámci mnou garantovaného bakalárskeho študijného programu „Bezpečnostní technologie systémy a management“ včasne a objektívne reflektovať aktuálne potreby praxe vzhľadom na meniace sa bezpečnostné prostredie, podmienky a požiadavky a integráciu problematiky konvergovanej bezpečnosti a resiliencie do bežnej praxe bezpečnostného manažmentu a inžinierstva.
- Logickou ambíciou je kontinuálne zvyšovanie kvality mnou garantovaných predmetov a to predovšetkým Krizové řízení a ochrana obyvatelstva, Ochrana kritické infrastruktury a měkkých cílů v doktorskom študijnom programe a Management bezpečnostního inženýrství, Technologie krizového řízení a Ochrana obyvatelstva v magisterskom študijnom programe a to predovšetkým implementáciou aktuálneho stavu poznania a nových poznatkov a to i nad rámec konvergovanej bezpečnosti a resiliencie kritickej infraštruktúry.
- Viesť a rozvíjať schopnosti študentov doktorského študijného programu k samostatnej vedeckej práci a to predovšetkým ich zapojením do riešenia výskumných úloh a projektov a publikovania odborných vedeckých prác v hodnotených časopisoch.
- Motivovať študentov k zahraničným mobilitám pre rozvoj medzinárodnej spolupráce a tvorbu medzinárodných konzorcií projektov typu H2020.

6 Koncepcia rozvoja vedného odboru

Ďalší rozvoj vedeckej práce je možné vnímať v detailnejšom a sektorovo orientovanom výskume konvergovanej resiliencie prvkov kritickej infraštruktúry. Súčasné prístupy konvergovanú resilienciu dávajú do kontextu konvergovanej bezpečnosti, a teda do kontextu spájania špecifických druhov bezpečnosti. Progresiou by v tomto smere mohla byť konvergencia atribútov resiliencie a teda atribútov robustnosti, obnoviteľnosti a adaptability prvku kritickej infraštruktúry. Ďalšou oblasťou rozvoja vedného odboru je problematika preventívnej indikácie narušenia resiliencie prvkov kritickej infraštruktúry. Indikančné parametre narušenia budú základom pre tvorbu prediktívnych modelov hodnotenia vývoja resiliencie v čase. V oboch menovaných prípadoch k pozitívnemu dopadu na úroveň ochrany kritickej infraštruktúry v rámci aspektov Security a súčasne k minimalizácii dopadov narušenia funkcie kritickej infraštruktúry a teda k funkčnej kontinuite spoločnosti (Safety).

Ďalšie výskumné aktivity budú do istej miery viazané na hierarchicky nižšiu úroveň konvergovanej bezpečnosti a resiliencie. Dôjde k rozpracovaniu a implementácii ďalších druhov bezpečnosti pre potreby ich konvergencie a súčasne rozšírenie atribútov konvergovanej resiliencie o rezistenciu. Výzvou bude formulácia penalizačných kritérií v rámci strategickej úrovne vnímania konvergovanej bezpečnosti (napr. energetická bezpečnosť, medzinárodná bezpečnosť). Vzhľadom na rozpracovanosť problematiky konvergovanej bezpečnosti a resiliencie kritickej infraštruktúry bude snahou vytvorené prístupy a metódy prispôsobiť podmienkam a špecifikám ďalších skupín významných infraštruktúrnych prvkov a systémov (viď obrázok 18).



Obrázok 18: Významné infraštruktúrne prvky

Vzhľadom na multispektrálnosť a medziodborovosť problematiky konvergovanej bezpečnosti a resiliencie významných infraštruktúrnych systémov je pragmatickým predpokladom spolupráca s významnými národnými a medzinárodnými výskumnými inštitúciami. Bude sa vzhľadom na predošlú históriu prípravy a realizácie zahraničných výskumných projektov a úloh jednať o spoluprácu s univerzitami v Miláne, Bologni, Budapešti, Varšave a Žiline. V kontexte medzinárodných projektov SecureGas, Stamina, S4AllCities sa bude jednať o rozvoj spolupráce s inštitúciami KEMEA (Grécko), APRE a RINA (Taliansko), EXUS Innovation (Spojené kráľovstvo) a Faruhofer Institute EMI (Nemecko). Potreba praktickej aplikácie výsledkov a výstupov súčasných a budúcich výsledkov a výstupov vedeckej práce bude naplňovaná prostredníctvom International Association of Critical Infrastructure Protection Professionals (Spojené kráľovstvo) a Technologickej platformy „Energetická bezpečnost ČR“.

7 Použitá literatúra

Alcaraz, C.; Zeadally, S. (2015). Critical Infrastructure Protection: Requirements and Challenges for the 21st century*. Int. J. Crit. Infrastruct.Prot.* 2015, 8, pp. 53–66.

Serre, D., Heinzlef Ch., (2018*).* Assessing and Mapping Urban Resilience to Floods with Respect to Cascading Effects Through Critical Infrastructure Networks, *International Journal of Disaster Risk Reduction*, Volume 30, Part B, 2018, pp. 235-243, ISSN 2212-4209, https://doi.org/10.1016/j.ijdrr.2018.02.018.

European Council. (2008). *Council Directive 2008/114/EC of 8 December 2008 on the Identification and Designation of European Critical Infrastructures and the Assessment of the Need to Improve their Protection*.

ČR. (2010), *Nařízení vlády č. 432 ze dne 22. 12. 2010 o kritériích pro určení prvku kritické infrastruktury*. In Sbírka zákonů České republiky. 2010, částka 149.

Rinaldi, S.M., Peerenboom, J.P., Kelly, T.K. (2001). Identifying, Understanding, and Analyzing Critical Infrastructure Interdependencies. *IEEE Control Systems*, Vol. 21, pp. 11-25. DOI: 10.1109/37.969131

Hába, S. (2010). *Síťová odvětví v EU:* Hodnocení regulace elektroenergetiky v ČR. Dipl. práce. Praha: *Vysoká škola ekonomická v Praze, Fakulta mezinárodních vztahů*, 107 s. Dostupné z http://www.vse.cz/vskp/24775_sitova_odvetvi_v%C2%A0eu.

Murray, Alan T.; Grubesic, T., (2010). Critical Infrastructure: Reliability and Vulnerability. 1. USA: Springer, 2010. 311 p. ISBN 978-3642087738.

Máchek, O., Hnilica, J., (2013). Metody regulace síťových odvětví. 9 s. Dostupné z www.ekonomikaamanagement.cz/getFile.php?fileKey...lang=cz.

Chen, P., Kataria, G., Krishnan, R. (2011). Correlated Failures, Diversification, and Information Security Risk Management. MIS Quarterly, 35(2): 397-422. DOI: 10.2307/23044049.

Tyson, D. (2011). Security Convergence: Managing Enterprise Security Risk. Oxford: Butterworth Heinemann.

Anderson, K. (2007). Convergence: A Holistic Approach to Risk Management. *Network Security*, 2007(5): pp. 4-7. DOI: 10.1016/S1353-4858(07)70033-8.

Hromada, M., Řehák D., Lukáš L., (2021). Resilience Assessment in Electricity Critical Infrastructure From the Point of View of Converged Security. *Energies* 2021; https://doi.org/10.3390/en14061624.

Řehák, D., (2012). Úvod do problematiky řízení rizik. In Lukáš, L.. et al. Bezpečnostní technologie, systémy a management II. 1. vyd. – Zlín: VeRBuM, pp. 74-95. ISBN 978-80-87500-19-4.

Hromada, M., Lukáš, L.,. (2015) Modely zajištění bezpečnosti. In Lukáš, L.. et al. Teorie bezpečnosti. 1. vydání. -- Zlín: Radim Bačuvčík – VeRBuM. pp. 72-85. ISBN 978-80-87500-67-5.

Lukáš, L., Urbančoková, H., (2019). Druhy bezpečnosti a jejich konvergence. In *Lukáš, L.. et al. Konvergovaná bezpečnost.* 1. vydání. – Zlín : Radim Bačuvčík - VeRBuM, pp. 26-42. ISBN 978-80-87500-99-6.

Řehák, D., Hromada, M., (2018). Failures in a Critical Infrastructure System. In T. Nakamura (Ed.), *System of System Failures*. London: IntechOpen, pp. 75-93. DOI: 10.5772/intechopen.70446

Contos, B.T., Derodeff, C., Crowell, W.P., Dunkel, D. (2007). Physical and Logical Security Convergence: Powered by Enterprise Security Management. *Burlington*, MA: Syngress. DOI: 10.1016/B978-1-59749-122-8.X5001-.

Dunn Cavelty, M., Kaufmann, M., Soby Kristensen, K. (2015). Resilience and (in)Security: Practices, Subjects, Temporalities. *Security Dialogue*, 46(1): 3-14. DOI: 10.1177/0967010614559637.

Králík, L., Malaník, D., Matýsek, M. (2018). Cyber Security Resilience Based on Static Factors as a Part of Converged Security. *In 5th International Conference on Mathematics and Computers in Sciences and Industry (MCSI)*, Corfu, Greece, pp. 114-117. DOI: 10.1109/MCSI.2018.00035.

Řehák, D., Šenovský, P., Slivková, S. (2018). Resilience of Critical Infrastructure Elements and its Main Ffactors. *Systems*, 6(2): Article No. 21. DOI: 10.3390/systems6020021.

Hess, J.J., Lm, S., Knowlton, K., Saha, S., Dutta, P., Ganguly, P., Tiwari, A., Jaiswal, A., Sheffield, P., Sarkar, J., Vhan, S.C., Begda, A., Shah, T., Solanski, B., Mavalankar, D. (2018). Building Resilience to Climate Change: Pilot Evaluation of the Impact of India's First Heat Action Plan on All-cause Mortality. *Journal of Environmental and Public Health*, 2018: 7973519. DOI: 10.1155/2018/7973519.

Fath, B.D., Dean, C.A., Katzmair, H. (2015). Navigating the Adaptive Cycle: An Approach to Managing the Resilience of Social Systems*. Ecology and Society*, 20(2): 24. DOI: 10.5751/ES-07467-200224.

Coaffe, J., Fussey, P. (2015). Constructing Resilience Through Security and Surveillance: The Politics, Practices and Tensions of Security-driven Resilience. *Security Dialogue*, 46 (1): 86-105. DOI: 10.1177/0967010614557884.

Argyroudis, S.A., Mitoulis, S.S., Hofer, L., Zanini, M.A., Tubaldi, E., Frangopol, D.M. (2020). Resilience Assessment Framework for Critical Infrastructure in a Multi-hazard Environment: Case study on Transport Assets. *Science of the Total Environment*, 714: 136854. DOI: 10.1016/j.scitotenv.2020.136854.

Lukáš, L., Hromada, M. (2011). Utilization of the EASI Model in the Matters of Critical Infrastructure Protection and its Verification via the OTB SAF Simulation Tool. In *Recent Researches in Automatic Control - 13th WSEAS International Conference on Automatic Control, Modelling and Simulation, ACMOS'11*, pp. 131-136. Cited 8 times. ISBN: 978-161804004-6

DELOITTE ADVISORY s.r.o., (2012). *Metodika zajištění ochrany kritické infrastruktury v oblasti výroby, přenosu a distribuce elektrické energie*. Praha.

Hromada, M., Lukáš, L., Matejdes, M., Valouch, J., Nečesal, L., Richter, R., Kovářík, F.,. (2013). Systém a způsob hodnocení odolnosti kritické infrastruktury. 1 vyd. Ostrava: *Sdružení požárního a bezpečnostního inženýrství*, 177s. Neuveden. ISBN 978-80-7385-140-8.

Hromada, M., Lukáš, L.,. (2013) The Status and Importance of Robustness in the Process of Critical Infrastructure Resilience Evaluation. In: *2013 IEEE International Conference on Technologies for Homeland Security (HST)* [online]. Waltham, MA: The Institute of Electrical and Electronics Engineers (IEEE), 2013, s. 589-594. [cit. 2022-07-25]. Dostupné z: http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=6699070&tag=1.

Řehák, D., Hromada, M., Loveček, T. 2020b. Personnel Threats in an Electric Power Critical Infrastructure Sector and Their Impacts on Dependent Sectors. *Safety Science*, Vol. 127, Article No. 104698. DOI: 10.1016/j.ssci.2020.104698

Hromada, M., Řehák, D., Walker, N., (2020) Electricity Infrastructure Technical Security: Practical Application and Best Practices of Risk Assessment. In ŘEHÁK, David, BERNATÍK, Aleš, DVOŘÁK, Zdeněk, HROMADA, Martin (Eds.), *Safety and Security Issues in Technical Infrastructures*. Hershey, PA: IGI Global, 2020, pp. 1-30. ISBN 978-1-7998-3059-7. DOI: 10.4018/978-1-7998-3059-7.ch001

Řehák, D., Šenovský, P., Hromada, M., Pidhaniuk, L., Dvořák, Z., Loveček, T., Ristvej, J., Leitner, B., Sventeková, E., Mariš, L., (2018). *Metodika hodnocení resilience prvků kritické infrastruktury (CIERA)*. [Certifikovaná metodika]. Ostrava: VŠB-TUO, 2018. 90 s. ISBN 978-80-248-4164-9. Ev.č.: CERO 2/2018.

Řehák, D., Šenovský, P., Hromada, M., Loveček, T., (2019). Complex Approach to Assessing Resilience of Critical Infrastructure Elements. *International Journal of Critical Infrastructure Protection*, Vol. 25, pp. 125-138. DOI: 10.1016/j.ijcip.2019.03.003

Hromada, M. (2016) *Modelovanie kaskádového a synergického efektu súvzťažných pododvetví kritickej infraštruktúry*. [Habilitačná práca]. Ostrava: VŠB – Technická univerzita, 148 s.

Řehák, D., Šenovský, P., Hromada, M., Loveček, T., Novotný, P. (2018a). Cascading Impact Assessment in a Critical Infrastructure System. *International Journal of Critical Infrastructure Protection*, Vol. 22, pp. 125-138. DOI: 10.1016/j.ijcip.2018.06.004

Řehák, D., Markuci, J., Hromada, M., Barčová, K. (2016). Quantitative Evaluation of the Synergistic Effects of Failures in a Critical Infrastructure System. *International Journal of Critical Infrastructure Protection*, Vol. 14, pp. 3-17. DOI: 10.1016/j.ijcip.2016.06.002

Hromada, M., Lukas, L., (2014). Security Education as a Fundamental Pillar of Critical Infrastructure Protection and Resilience. *International Journal of Education and Information Technologies* [online]. 2014, vol. 8, s. 294-303. [cit. 2022-07-26]. ISSN 2074-1316. Dostupné z: https://www.naun.org/main/NAUN/educationinformation/2014/a062008-145.pdf.

8 Skrátený odborný životopis

OSOBNÉ ÚDAJE

Meno, priezvisko, tituly doc. Ing. Martin Hromada, Ph.D.

PRACOVNÉ SKÚSENOSTI

2022 – doteraz	Fakulta aplikované informatiky UTB ve Zlíně, Proděkan pro mezinárodní vztahy
2022 – doteraz	Fakulta bezpečnostního inženýrství VŠB-TUO, Riešiteľ projektu CK03000182.
2022 – doteraz	Vysoké učení technické v Brně, Fakulta stavební, Riešiteľ projektu – VB01000034.
2022 – doteraz	Fakulta aplikované informatiky UTB ve Zlíně, Manažér projektu – VB01000008.
2021 – doteraz	Fakulta aplikované informatiky UTB ve Zlíně, Riešiteľ projektu VI04000080.
2020 – 2021	Mezinárodní bezpečnostní institut, z. ú., Riešiteľ projektu VH20202021056.
2020 – 2022	Technologická platforma energetická bezpečnost ČR, Riešiteľ projektu S4AllCities – H2020 Project at European Commission, H2020, EU
2020 – 2022	MV ČR, GŘ HZS ČR, Institut ochrany obyvatelstva Lázně Bohdaneč, Riešiteľ projektu STAMINA – H2020 Project at European Commission, H2020, EU
2019 – 2022	Fakulta bezpečnostního inženýrství VŠB-TUO, Řešitel projektu VI20192022151.
2019 – 2021	Technologická platforma energetická bezpečnost ČR, Riešiteľ projektu SECUREGAS – Securing The European Gas Network, H2020, EU
2019 – 2022	Fakulta aplikované informatiky UTB ve Zlíně, Riešiteľ projektu VI20192022118.
2019 – 2022	Fakulta aplikované informatiky UTB ve Zlíně, Riešiteľ projektu VI20192022134.
2018 – 2021	Univerzita Karlova, Fakulta sociálních věd, Riešiteľ projektu TL02000352.
2018 – doteraz	Fakulta aplikované informatiky UTB ve Zlíně, garant predmetov: Fyzická ostraha, Bezpečnostní inženýrství, Bakalářská práce, Požární ochrana, Ochrana obyvatelstva, Management bezpečnostního inženýrství, Bezpečnost a ochrana zdraví při práci, Technologie krizového řízení
2018 – doteraz	Fakulta aplikované informatiky UTB ve Zlíně, garant bakalářského studijního programu: Bezpečnostní technologie, systémy a management
2018 – 2021	Technologická platforma energetická bezpečnost ČR, Riešiteľ projektu TK01010146.
2017 – 2019	Fakulta aplikované informatiky UTB ve Zlíně, Riešiteľ projektu VI20172019073.
2017 – 2019	Fakulta aplikované informatiky UTB ve Zlíně, Riešiteľ projektu VI20172019054.
2016 – 2016	Fakulta bezpečnostního inženýrství VŠB-TUO, Riešiteľ I veřejné zakázky úřadu vlády Zpracování studie „Souhrn způsobů hodnocení kvality a odolnosti infrastruktury“ – odborné zaměření na oblast energetické infrastruktury.
2015 – 2019	Fakulta aplikované informatiky UTB ve Zlíně, Riešiteľ a manažer projektu VI20152019049.
2014 – 2015	K2 connect solution s.r.o., Riešiteľ projektu 5.1 SPK 02/026 - CKI Centrum kritické infrastruktury.
2014 – 2015	Deloitte Advisory s.r.o., Riešitel veřejné zakázky MV- 38918/VZ-2012 – VF20142015035.

2011 – 2014 Fakulta aplikované informatiky UTB ve Zlíně, Koordinátor a riešitel projektu VG20112014067.

2012 - 2018 Fakulta aplikované informatiky UTB ve Zlíně, garant předmětů: Modelování krizových situací, Speciální technologie komerční bezpečnosti.

2010 - 2012 Deloitte Advisory s.r.o., Riešiteľ projektu VG20102012025.

UNIVERZITNÉ VZDELANIE

2017 doc.

Vysoká škola báňská – Technická univerzita Ostrava, Fakulta bezpečnostního inženýrství

Obor: Bezpečnost a požární ochrana

2011 Ph.D.

Univerzita Tomáše Bati ve Zlíně, Fakulta aplikované informatiky

Obor: Inženýrská informatika

2008 Ing.

Univerzita Tomáše Bati ve Zlíně, Fakulta aplikované informatiky

Obor: Bezpečnostní technologie, systémy a management

ČLENSTVO V ORGÁNOCH UNIVERZÍT

2023 – doteraz Člen Vedeckej rady Fakulty bezpečnostného inžinierstva Žilinskej univerzity v Žiline

2020 – doteraz Člen Vedeckej rady Policejní akademie České republiky v Praze

2018 – doteraz Člen Vedeckej rady Fakulty vojenského leadershipu Univerzity obrany

2016 – doteraz Člen odborovej komise 3. stupně vysokoškolského studia v studijním odboru 8.3.7 občianska bezpečnosť v študijnom programe krízový manažment na Fakulte bezpečnostného inžinierstva ŽU v Žiline.

ČLENSTVO V ORGANIZÁCIÁCH

2020 – doteraz Člen odborového panelu TAČR programu Doprava 2020+.

2018 – doteraz Člen International Association of CIP Professionals.

2018 – doteraz Člen odborového panelu TAČR programu THÉTA.

2016 – doteraz Člen vědeckého výboru aktivity „Mladá věda“.

2015 – doteraz Člen European Association for Security.

2013 – doteraz UTB ve Zlíně: z zastupujúci člen Technologické platformy „energetická bezpečnost“, TPEB – člen správní rady

2013 – doteraz univerzitu zastupujúci člen bezpečnostně technologického klastru v Ostravě, BTklastr.

2012 – doteraz UTB ve Zlíně: zastupujúci člen v European Reference Network for Critical Infrastructure Protection, EU ERNCIP.

2012 – doteraz	UTB ve Zlíně: zastupujúci člen v Critical Infrastructure Warning Information Network, EU CIWIN.
2011 – doteraz	člen odbornej platformy ochrany obyvatestva Generálního ředitelství Hasičského Záchranného Sboru ČR, OPOO.
2011 – doteraz	člen Českej asociácie bezpečnostných manažérov.
2010 – doteraz	člen expertnej skupiny pre posudzovanie a oponovánie návrhov projektov bezpečnostného výskumu, MVČR.
2008 – doteraz	člen Mezirezortnej skupiny pre prípravu zákona o ochrane KI, MV SR.

ODBORNÉ ZAMERANIE ----------

Kritická infraštruktúra	Resiliencia a ochrana prvkov kritickej infraštruktúry; Kaskádové a synergické efekty v systéme kritickej infraštruktúry; Hodnotenie statickej a dynamickej resiliencie; Prediktívne indikácie narušenia resiliencie; Konvergovaná bezpečnosť a resiliencia kritickej infraštruktúry
Ochrana mäkkých cieľov	Fyzická ochrana mäkkých cieľov; Tvorba koordiančných plánov; Konvergovaná bezpečnosť mäkkých cieľov
Management rizik	Metódy posudzovania rizík; Opatrenia na zvládanie rizík; Aktuálne bezpečnostné hrozby

IDENTIFIKAČNÉ ÚDAJE AUTORA ----------

ResearcherID	GXM-8666-2022
Scopus Author ID	55246365500
ORCID	0000-0003-0347-7528

9 Prehľad publikačnej, vedecko-výskumnej a pedagogickej činnosti

9.1 Výsledky publikačnej činnosti a aplikovaného výskumu

Články v časopisech indexovaných v databázi Web of Science	12
Články v časopisech indexovaných v databázi Scopus (bez duplicit ve WoS)	10
Příspěvky z konferencí indexovaných v databázi Web of Science	38
Příspěvky z konferencí indexovaných v databázi Scopus (bez duplicit ve WoS)	46
Odborné knihy a kapitoly v anglickém jazyce	10
Odborné knihy a kapitoly v českém jazyce	11
Certifikované metodiky a softwarové nástroje	10

Články v časopisoch indexovaných v databáze Web of Science

Q1	Q2	Q3	Q4	ESCI
2	4	4	-	2

1. VICHOVA, K., HROMADA, M., DZERMANSKY, M., SNOPEK, L., PEKAJ, R. Solving Power Outages in Healthcare Facilities: Algorithmisation and Assessment of Preparedness. *Energies*. 2023, 16(1), 1-14. ISSN 1996-1073 (**Q3; IF 3.004; autorský podíl 10 %)**
2. ŘEHÁK, David, Simona SLIVKOVÁ, Heidi JANEČKOVÁ, Dominika ŠTUBEROVÁ a Martin HROMADA. Strengthening resilience in the energy critical infrastructure: Methodological overview. *Energies* [online]. 2022, vol. 15, iss. 14 [cit. 2023-02-09]. ISSN 1996-1073. Dostupné z: https://www.mdpi.com/1996-1073/15/14/5276. (**Q3; IF 3.004; autorský podíl 10 %)**
3. ŘEHÁK, David, HROMADA, Martin, ONDERKOVÁ, Vendula, WALKER, Neil, FUGGINI, Clemente. Dynamic robustness modelling of electricity critical infrastructure elements as a part of energy security. *International Journal of Electrical Power & Energy Systems*, 2022, Vol. 136, Article No. 107700. ISSN 0142-0615. DOI: 10.1016/j.ijepes.2021.107700 **(Q1; IF 4.630; autorský podíl 20 %)**
4. DVOŘÁK, Zdeněk, CHOVANČÍKOVÁ, Nikola, BRUK, Jozef, HROMADA, Martin. Methodological framework for resilience assessment of electricity infrastructure in conditions of Slovak Republic. *International Journal of Environmental Research and Public Health*, 2021, Vol. 18, No. 16, pp. 1-29. ISSN 1661-7827. DOI: 10.3390/ijerph18168286 **(Q3; IF 3.390; autorský podíl 10 %)**
5. VÁVRA, Jan, HROMADA, Martin, LUKÁŠ, Luděk, DWORZECKI, Jacek. Adaptive anomaly detection system based on machine learning algorithms in an industrial control environment.

International Journal of Critical Infrastructure Protection, 2021, Vol. 34, Article No. 100446. ISSN 1874-5482. DOI: 10.1016/j.ijcip.2021.100446 **(Q2; IF 2.225; autorský podíl 40 %)**

6. HROMADA, Martin, ŘEHÁK, David, LUKÁŠ, Luděk. Resilience assessment in electricity critical infrastructure from the point of view of converged security. *Energies*, 2021, roč. 14, č. 6. ISSN 1996-1073. DOI: 10.3390/en14061624 **(Q3; IF 3.004; autorský podíl 60 %)**
7. ŠPLÍCHALOVÁ, Alena, PATRMAN, David, KOTALOVÁ, Nikol, HROMADA, Martin. Managerial Decision-Making in Indicating a Disruption of Critical Infrastructure Element Resilience. *Administrative Sciences*, Vol. 10, Iss. 3, Article No. 75. ISSN 2076-3387. 2020. DOI: 10.3390/admsci10030075, **(ESCI; autorský podíl 10 %)**
8. ŘEHÁK, David, HROMADA, Martin, LOVEČEK, Tomáš. Personnel Threats in an Electric Power Critical Infrastructure Sector and Their Impacts on Dependent Sectors. *Safety Science*, 2020, Vol. 127, Article No. 104698. ISSN 0925-7535. DOI: 10.1016/j.ssci.2020.104698 **(Q1; IF 4.105; autorský podíl 30 %)**
9. ŘEHÁK, David, ŠENOVSKÝ, Pavel, HROMADA, Martin, LOVEČEK, Tomáš. Complex Approach to Assessing Resilience of Critical Infrastructure Elements. *International Journal of Critical Infrastructure Protection*, 2019, Vol. 25, pp. 125-138. ISSN 1874-5482. DOI: 10.1016/j.ijcip.2019.03.003 **(Q2; IF 2.164; autorský podíl 15 %)**
10. ŘEHÁK, David, RADIMSKÝ, Michal, HROMADA, Martin, DVOŘÁK, Zdeněk. Dynamic Impact Modeling as a Road Transport Crisis Management Support Tool. *Administrative Sciences (Special Issue: Rational Decision Making in Risk Management)*, 2019, Vol. 9, Iss. 2, Article No. 29. ISSN 2076-3387. DOI: 10.3390/admsci9020029 **(ESCI; autorský podíl 20 %)**
11. ŘEHÁK, David, ŠENOVSKÝ, Pavel, HROMADA, Martin, LOVEČEK, Tomáš, NOVOTNÝ, Petr. Cascading Impact Assessment in a Critical Infrastructure System. *International Journal of Critical Infrastructure Protection*, 2018, Vol. 22, pp. 125-138. ISSN 1874-5482. DOI: 10.1016/j.ijcip.2018.06.004 **(Q2; IF 2.225; autorský podíl 5 %)**
12. ŘEHÁK, David, MARKUCI, Jiří, HROMADA, Martin, BARČOVÁ, Karla. Quantitative Evaluation of the Synergistic Effects of Failures in a Critical Infrastructure System. *International Journal of Critical Infrastructure Protection*, 2016, Vol. 14, pp. 3-17. ISSN 1874-5482. DOI: 10.1016/j.ijcip.2016.06.002 **(Q2; IF 1.500; autorský podíl 15 %)**

Články v časopisech indexovaných v databázi Scopus (bez duplicit ve WoS)

Q1	Q2	Q3	Q4	Nezařazené
-	1	2	7	-

1. VÍCHOVÁ, Kateřina, HROMADA, Martin. The risk mapping for hospitals and the impact for the transport in the Zlín Region. *Journal of Emergency Management*, 2020, Vol. 18, No. 2, pp. 131-140. ISSN 1543-5865. **(Q3; Autorský podíl 10 %)**

2. ZIMEK, Ondřej, MACH, Václav, VALOUCH, Jan, ADÁMEK, Milan, HROMADA, Martin. Integrated Alarm System with the access system for Kindergartens. *Przeglad Elektrotechniczny*, 2020, Vol. 96, No. 4, pp. 28-32. ISSN 0033-2097. **(Q4; Autorský podíl 5 %)**
3. VÍCHOVÁ, Kateřina, HROMADA, Martin. The Evaluation Module of the Crisis Preparedness for the Hospitals. *International Journal of Biology and Biomedical Engineering*, 2018, Vol. 2018, No. 12, pp. 178-185. ISSN 1998-4510. **(Q4; Autorský podíl 10 %)**
4. VÍCHOVÁ, Kateřina, HROMADA, Martin. The Use of Information Systems in the Hospital in Times of Crisis. *International Journal of Biology and Biomedical Engineering*, 2018, Vol. 2018, No. 12, pp. 170-177. ISSN 1998-4510. **(Q4; Autorský podíl 10 %)**
5. VÍCHOVÁ, Kateřina, HROMADA, Martin. The Comparative Analysis of Information, Communication and Warning Systems. *International Journal of Circuits, Systems and Signal Processing*, 2018, Vol. 2018, No. 12, pp. 736-741. ISSN 1998-4464. **(Q4; Autorský podíl 10 %)**
6. VÁVRA, Jan, HROMADA, Martin, JAŠEK, Roman. Specification of the Current State Vulnerabilities Related to Industrial Control Systems. *International Journal of Online Engineering*, 2015, Vol. 2015, No. 5, pp. 64-68. ISSN 1868-1646. **(Q4; Autorský podíl 10 %)**
7. LUKÁŠ, Luděk, HROMADA, Martin. Resilience as main part of protection of critical infrastructure. *International Journal of Mathematical Models and Methods in Applied Science*, 2011, Vol. 5, No. 6, pp. 1135-1142. ISSN 1998-0140. **(Q4; Autorský podíl 50 %)**
8. LUKÁŠ, Luděk, HROMADA, Martin. Simulation and modelling in critical infrastructure protection. *International Journal of Mathematics and Computers in Simulations*, 2011, Vol. 5, No. 4, pp. 386-394. ISSN 1998-0159. **(Q4; Autorský podíl 50 %)**
9. HROMADA, Martin, LUKÁŠ, Luděk. Security Education as a Fundamental Pillar of Critical Infrastructure Protection and Resilience. *International Journal of Education and Information Technologies*, 2014, Vol. 2014, No. 8, pp. 294-303. ISSN 2074-1316. **(Q2; Autorský podíl 80 %)**
10. HROMADA, Martin, LUKÁŠ, Luděk. Critical Infrastructure Protection and the Evaluation Process. *International Journal of Disaster Recovery and Business Continuity*, 2012, Vol. 3, No. 3, pp. 37-46. ISSN 2005-4289. **(Q3; Autorský podíl 50 %).**

Príspevky z konferencií indexovaných v databáze Web of Science

1. KOTEK, Lukáš, HROMADA, Martin, KOTKOVÁ, Dora. Educational Platform for Personal and Community Protection Situations From the Perspective of Soft Targets. In *Iberian Conference on Information Systems and Technologies, CISTI. Los Alamitors: IEEE Computer Society*, 2020, pp. 1-4. ISSN 21660727. ISBN 978-989546590-3.
2. VÁVRA, Jan, HROMADA, Martin. Optimization of the Novelty Detection Model Based on LSTM Autoencoder for ICS Environment. In *Advances in Intelligent Systems and Computing (Vol. 1)*. Berlín: Springer Verlag, 2019, pp. 306-319. ISSN 2194-5357. ISBN 978-3-030-30328-0.

3. VÍCHOVÁ, Kateřina, HROMADA, Martin. Power Outage in the Hospitals. In *ACM International Conference Proceeding Series*. New York: Association for Computing Machinery, 2019, pp. 304-309. ISBN 978-1-4503-6269-6.
4. BLAHOVÁ, Marta, HROMADA, Martin. Epidemiological Threats and Preparedness of the Selected CFAs for the Transport of Infectious Patients. In *ACM International Conference Proceeding Series*. New York: Association for Computing Machinery, 2019, pp. 10-14. ISBN 978-1-4503-6269-6.
5. BLAHOVÁ, Marta, HROMADA, Martin. Assessment of the Emergency Preparedness of the Patient to Move from the Airport with Suspicion of Ebola. In *ACM International Conference Proceeding Series*. New York: Association for Computing Machinery, 2019, pp. 6-9. ISBN 978-1-4503-6269-6.
6. VÍCHOVÁ, Kateřina, HROMADA, Martin, VISKUP, Pavel. The Simulation of Hospital Supply in case of Emergency Deliveries. In *Proceedings of the International Conference Transport Means*. Kaunas: Kaunas University of Technology, 2018, pp. 601-605. ISSN 1822296X.
7. VÍCHOVÁ, Kateřina, HROMADA, Martin. The Evaluation System to Ensure the Transport of Emergency Supplies of Fuel to the Hospitals. In *Transportation Research Procedia*. Amsterdam: Elsevier B.V., 2019, pp. 1618–1624. ISSN 2352-1457.
8. ĎURICOVÁ, Lucia, HROMADA, Martin, MRÁZEK, Jan. The Mathematical Modelling of the Soft Targets Assessment. In *ACM International Conference Proceeding Series*. New York: Association for Computing Machinery, 2019, pp. 35-39. ISBN 978-1-4503-7181-0.
9. MRÁZEK, Jan, ĎURICOVÁ, Lucia, HROMADA, Martin. The Design Solution for Dynamic Material Transportation Management. In *ACM International Conference Proceeding Series*. New York: Association for Computing Machinery, 2019, pp. 76-80. ISBN 978-1-4503-7181-0.
10. MRÁZEK, Jan, MRÁZKOVÁ, Lucia, HROMADA, Martin, Traffic Control Through Traffic Density, Traffic Control Through Traffic Density," In *3rd European Conference on Electrical Engineering and Computer Science (EECS)*, 2019, pp. 19-21, doi: 10.1109/EECS49779.2019.00017.
11. VÍCHOVÁ, Kateřina, HROMADA, Martin. The Use of Simulation Software for Emergency Supply Transport to the Hospital. *ACM International Conference Proceeding Series*. New York: Association for Computing Machinery, 2019, pp. 96-101. ISBN 978-1-4503-6106-4.
12. VÍCHOVÁ, Kateřina, HROMADA, Martin. Assessment of Emergency Supply of Healthcare Facilities as a Module of the Crisis Management Information System. In *MATEC Web of Conferences*. Les Ulis: EDP Sciences, 2018, ISSN 2261-236X
13. VÍCHOVÁ, Kateřina, HROMADA, Martin. The Analysis of Crisis Management Information System in the Selected States. In *MATEC Web of Conferences*. Les Ulis: EDP Sciences, 2018, ISSN 2261-236X.

14. VÍCHOVÁ, Kateřina, HROMADA, Martin. The Analysis of Communication in Times of Crisis at the Hospitals in the Czech Republic. In *MARKETING IDENTITY: DIGITAL MIRRORS*, PT II. Trnava: UNIV SS CYRIL & METHODIUS TRNAVA-UCM TRNAVA, 2019, pp. 325-330. ISSN 1339-5726. ISBN 978-80-8105-984-1.
15. ĎURICOVÁ, Lucia, HROMADA, Martin, MRÁZEK, Jan. The Soft Target Assessment and Software Tool. In *Proceedings - 2018 3rd International Conference on System Reliability and Safety, ICSRS 2018.* Piscataway, New Jersey: Institute of Electrical and Electronics Engineers Inc., 2019, pp. 30-34. ISBN 978-1-72810-238-2.
16. VÍCHOVÁ, Kateřina, HROMADA, Martin. The Analysis of Health Information System. In *Proceedings - 2018 International Conference on Control, Artificial Intelligence, Robotics and Optimization, ICCAIRO 2018*. Piscataway, New Jersey: Institute of Electrical and Electronics Engineers Inc., 2019, pp. 271-276. ISBN 978-1-5386-9576-0.
17. VÍCHOVÁ, Kateřina, HROMADA, Martin, VISKUP, Pavel. The Simulation of Hospital Supply in case of Emergency Deliveries. In *Transport Means - Proceedings of the International Conference*. Kaunas: Kaunas University of Technology, 2018, pp. 601-605. ISSN 1822296X.
18. ĎURICOVÁ, Lucia, HROMADA, Martin. The Proposal of Software for Transport Infrastructure Management. In *8th International Conference on Information, Intelligence, Systems and Applications*, IISA 2017. Piscataway, New Jersey: Institute of Electrical and Electronics Engineers Inc., 2017, ISBN 978-1-5386-3731-9.
19. VÍCHOVÁ, Kateřina, HROMADA, Martin. The comparative analysis of crisis management information systems in the Czech Republic. In *8th International Conference on Information, Intelligence, Systems and Applications*, IISA 2017. Piscataway, New Jersey: Institute of Electrical and Electronics Engineers Inc., 2017, pp. 1-5. ISBN 978-1-5386-3731-9.
20. VÍCHOVÁ, Kateřina, HROMADA, Martin, LUKÁŠ, Luděk. The Proposal of United Crisis Management Information Systems of the Czech Republic. In *Proceedings 2017 International Conference on Soft Computing, Intelligent System and Information Technology*. Washington, DC: IEEE Computer Society Conference Publishing Services (CPS), 2017, pp. 190-195. ISBN 978-1-4673-9899-2.
21. VÁVRA, Jan, HROMADA, Martin. Anomaly Detection System Based on Classifier Fusion in ICS Environment. In *Proceedings 2017 International Conference on Soft Computing, Intelligent System and Information Technology*. Washington, DC: IEEE Computer Society Conference Publishing Services (CPS), 2017, pp. 32-38. ISBN 978-1-4673-9899-2.
22. MRÁZEK, Jan, ĎURICOVÁ, Lucia, HROMADA, Martin. The Software Proposes for Management and Decision Making at Process Transportation. In *Proceedings 2017 International Conference on Soft Computing, Intelligent System and Information Technology*. Washington, DC: IEEE

Computer Society Conference Publishing Services (CPS), 2017, pp. 120-123. ISBN 978-1-4673-9899-2.

23. VÍCHOVÁ, Kateřina, HROMADA, Martin, ŘEHÁK, David. The Use of Crisis Management Information Systems in Rescue Operations of Fire and Rescue System in the Czech Republic. In *12th International Scientific Conference on Sustainable, Modern and Safe Transport (TRANSCOM 2017)*, Procedia Engineering, 2017, Vol. 192, pp. 947-952. ISSN 1877-7058. DOI: 10.1016/j.proeng.2017.06.163
24. ĎURICOVÁ, Lucia, HROMADA, Martin. The Proposal of Security and Safety Solution to the Soft Targets. In *8th International Conference on Information, Intelligence, Systems and Applications, IISA 2017*. Piscataway, New Jersey: Institute of Electrical and Electronics Engineers Inc., 2017, ISBN 978-1-5386-3731-9.
25. ĎURICOVÁ, Lucia, HROMADA, Martin. The Proposal of Software for Transport Infrastructure Management. In *8th International Conference on Information, Intelligence, Systems and Applications, IISA 2017*. Piscataway, New Jersey: Institute of Electrical and Electronics Engineers Inc., 2017, ISBN 978-1-5386-3731-9.
26. LEITNER, Bohuš, MÔCOVÁ, Lenka, HROMADA, Martin. A New Approach to Identification of Critical Elements in Railway Infrastructure. In *Procedia Engineering. Amsterdam*: Elsevier BV, 2017, pp. 143-149. ISSN 1877-7058.
27. VÍCHOVÁ, Kateřina, HROMADA, Martin, LUKÁŠ, Luděk. The Proposal of United Crisis Management Information Systems of the Czech Republic. In *Proceedings 2017 International Conference on Soft Computing, Intelligent System and Information Technology*. Washington, DC: IEEE Computer Society Conference Publishing Services (CPS), 2017, pp. 190-195. ISBN 978-1-4673-9899-2.
28. VÁVRA, Jan, HROMADA, Martin. Comparison of the Intrusion Detection System Rules in Relation with the SCADA systems. In Software Engineering Perspectives and Application in Intelligent Systems: *Proceedings of the 5th computer science on-line conference 2016*, Vol. 2. Heidelberg: Springer-Verlag Berlin, 2016, pp. 159-169. ISSN 2194-5357. ISBN 978-3-319-33620-6.
29. ĎURICOVÁ, Lucia, HROMADA, Martin. The Proposal of the Soft Targets Security. In Automation Control Theory Perspectives in Intelligent Systems*: Proceedings of the 5th computer science on-line conference 2016*. Vol. 3. Heidelberg: Springer-Verlag Berlin, 2016, pp. 337-345. ISSN 2194-5357. ISBN 978-3-319-33387-8.
30. ĎURICOVÁ, Lucia, HROMADA, Martin. Fuzzy Logic as Support for Security and Safety Solution in Soft Targets. In *MATEC Web of Conferences*. Les Ulis: EDP Sciences, 2016, ISSN 2261-236X.
31. ŘEHÁK, David, HROMADA, Martin, NOVOTNÝ, Petr. European Critical Infrastructure Risk and Safety Management: Directive Implementation in Practice. In *Chemical Engineering*

Transactions, 2016, Vol. 48, pp. 943-948. ISBN 978-88-95608-39-6. ISSN 2283-9216. DOI: 10.3303/CET1648158

32. LUKÁŠ, Luděk, HROMADA, Martin, PAVLÍK, Lukáš. The Key Theoretical Models for the Safety and Security Ensuring. In Proceedings - 2016 *3rd International Conference on Mathematics and Computers in Sciences and in Industry, MCSI 2016*. Piscataway, New Jersey: Institute of Electrical and Electronics Engineers Inc., 2016, pp. 61-65. ISBN 978-1-5090-0972-5.
33. VÁVRA, Jan, HROMADA, Martin. An Evaluation of Cyber Threats to Industrial Control Systems. In *International conference on Military Technologies - ICMT 2015. Piscataway: Institute of Electrical and Electronics Engineer*, Inc., 2015, pp. 369-373. ISBN 978-80-7231-976-3.
34. PROCHÁZKOVÁ, Lucia, HROMADA, Martin. The Security Risks Associated with Attacks on Soft Targets of State. In *ICMT 2015*. Piscataway: Institute of Electrical and Electronics Engineer, Inc., 2015, p. 307. ISBN 978-80-7231-976-3.
35. HROMADA, Martin, LUKÁŠ, Luděk. The Status and Importance of Robustness in the Process of Critical Infrastructure Resilience Evaluation. In *Proceedings of the 13th annual IEEE Conference on Technologies for Homeland Security (HST '13)*. Boston: IEEE, 2013, pp. 589-594. ISBN 978-1-4799-1533-0.
36. HROMADA, Martin, LUKÁŠ, Luděk. Multicriterial Evaluation of Critical Infrastructure Element Protection in Czech Republic. In *Computer Applications for Software Engineering, Disaster Recovery, and business Continuity*, 2012, roč. 2012, č. 340, pp. 361-368. ISSN 1865-0929.
37. HROMADA, Martin, LUKÁŠ, Luděk. Conceptual Design of the Resilience Evaluation System of the Critical Infrastructure Elements and Networks in Selected Areas in Czech Republic. In *2012 IEEE International Conference.* Boston: IEEE, 2012, pp. 353-358. ISBN 978-1-4673-2707-7.
38. BLAHOVÁ, Marta, HROMADA, Martin. Simulation of Chemical Attack on the Population and its Protection. In *ACM International Conference Proceeding Series*. New York: Association for Computing Machinery, 2021, pp. 93-100. ISBN 978-145039005-7.

Príspevky z konferencií indexovaných v databáze Scopus (bez duplicít vo WoS)

1. VÍCHOVÁ, Kateřina, Martin HROMADA, František PAULUS a Jarmil VALÁŠEK. CBRN weapons as a threat to critical infrastructure elements. In: *ACM International Conference Proceeding Series* [online]. online: Association for Computing Machinery, 2022, s. 253-257. [cit. 2023-02-09]. Dostupné z: https://dl.acm.org/doi/10.1145/3545729.3545780.
2. MUHAMMAD, Hemin Akram a Martin HROMADA. Proposing an e-government stage model in terms of personal information security in developing countries. In: *Proceedings - International Carnahan Conference on Security Technology* [online]. Valeč u Hrotovic: Institute of Electrical and Electronics Engineers Inc., 2022 [cit. 2023-02-09]. ISSN 1071-6572. Dostupné z: https://ieeexplore.ieee.org/document/9896521.

3. OKA, Mimi Enakome a Martin HROMADA. Analysis of current preventive approaches in the context of cybersecurity. In: Proceedings - *International Carnahan Conference on Security Technology* [online]. Valeč u Hrotovic: Institute of Electrical and Electronics Engineers Inc., 2022 [cit. 2023-02-09]. ISSN 1071-6572. Dostupné z: https://ieeexplore.ieee.org/document/9896499.
4. MALATINSKÝ, Adam a Martin HROMADA. Evaluation of the most important fire threats of the building. In: *Proceedings - International Carnahan Conference on Security Technology* [online]. Valeč u Hrotovic: Institute of Electrical and Electronics Engineers Inc., 2022 [cit. 2023-02-09]. ISSN 1071-6572. Dostupné z: https://ieeexplore.ieee.org/document/9896486.
5. KOTKOVÁ, Dora, Lukáš KOTEK a Martin HROMADA. Educational platform for personal and community protection situations from the perspective of soft targets - Self-defense part. In: *Proceedings - International Carnahan Conference on Security Technology* [online]. Valeč u Hrotovic: Institute of Electrical and Electronics Engineers Inc., 2022 [cit. 2023-02-09]. ISSN 1071-6572. Dostupné z: https://ieeexplore.ieee.org/document/9896561.
6. L. Kotek, M. Hromada and D. Kotkova, "Online Interactive Education of People in the Field of Protection of Soft Targets," *2022 IEEE International Carnahan Conference on Security Technology (ICCST),* Valeč u Hrotovic, Czech Republic, 2022, pp. 1-5, doi: 10.1109/ICCST52959.2022.9896591.
7. KOTKOVÁ, Dora, HROMADA, Martin, MALANÍKOVÁ, Martina, KOVÁŘ, Stanislav. The Concept of a Software Tool with an Interactive Map for Identification and Determination of Soft Targets of Transport Infrastructure. In *IEEE 2021 International Carnahan Conference on Security Technology (ICCST)*. Manila: Institute of Electrical and Electronic Engineers (IEEE) Research Publishing, 2021, pp. 1-5. ISBN 978-1-66549-988-0.
8. BLAHOVÁ, Marta, HROMADA, Martin. Principles for Verification of Mathematical Fire Models. In *Proceedings - 25th International Conference on Circuits, Systems, Communications and Computers, CSCC 2021*. Los Alamitos: IEEE Computer Society, 2021, pp. 111-115. ISBN 978-166542749-4.
9. KOTKOVÁ, Barbora, HROMADA, Martin. The Threat of Social Engineering and the Safety of Companies. In *Proceedings - 25th International Conference on Circuits, Systems, Communications and Computers*, *CSCC 2021*. Los Alamitors: IEEE Computer Society, 2021, pp. 126-133. ISBN 978-166542749-4.
10. KOTKOVÁ, Barbora, HROMADA, Martin. Cyber Security and Social Engineering. In Proceedings - 25th *International Conference on Circuits, Systems, Communications and Computers, CSCC 2021*. Los Alamitors: IEEE Computer Society, 2021, pp. 134-140. ISBN 978-166542749-4.
11. BLAHOVÁ, Marta, HROMADA, Martin. Modeling the development of fire unconventional methodology. In *Proceedings - 25th International Conference on Circuits, Systems,*

Communications and Computers, CSCC 2021. Los Alamitors: IEEE Computer Society, 2021, ISBN 978-166542749-4.

12. MALATINSKÝ, Adam, DROFOVÁ, Irena, SOUSEDÍKOVÁ, Lucie, HROMADA, Martin. Fire Safety Threat Risk Analysis for Soft Target. *Annals of DAAAM and Proceedings of the International DAAAM Symposium*. Vienna: DAAAM International Vienna, 2021, pp. 586-592. ISSN 1726-9679. ISBN 978-3-902734-33-4.
13. KOTKOVÁ, Barbora, HROMADA, Martin. Benefits and Risks of Multimodal Transport with a Main Focus on the EU. In *Annals of DAAAM and Proceedings of the International DAAAM Symposium*. Vienna: DAAAM International Vienna, 2021, pp. 306-310. ISSN 1726-9679. ISBN 978-3-902734-33-4.
14. KOTKOVÁ, Dora, HROMADA, Martin, ŠTERNOVÁ, Tereza, LJUBYMENKO, Krystyna. Methodology of Identification and Protection of Soft Targets of Transport Infrastructure – initial study. In *Transport Means - Proceedings of the International Conference*. Kaunas: Kaunas University of Technology, 2021, pp. 1107-1112. ISSN 1822-296X.
15. VÍCHOVA, Katerina, HROMADA, Martin, VALÁŠEK, Jarmil, PAULUS, František, Integrated Rescue System and the Use of Unmanned Aerial Vehicle Not Only for the Population Protection, In *ACM International Conference Proceeding Series, 4th International Conference on Medical and Health Informatics, ICMHI 2020*, Code 163980, pp. 180–185, ISBN 978-145037776-8, DOI: 10.1145/3418094.3418112.
16. BLAHOVÁ, Marta, HROMADA, Martin, Chemical Situation Modeling Software to Protect Soft Targets, In *Proceedings - 24th International Conference on Circuits, Systems, Communications and Computers, CSCC 2020*, Pages 270 – 277, July 2020, Platanias, Chania, Crete Island, ISBN 978-172816503-5, DOI: 10.1109/CSCC49995.2020.00056
17. KOTKOVÁ, Barbora, HROMADA, Martin. Blackout Measures in Hospitals – Use of Alternative Sources of Electricity. In *Proceedings - 24th International Conference on Circuits, Systems, Communications and Computers, CSCC 2020*. Piscataway, New Jersey: Institute of Electrical and Electronics Engineers Inc., 2020, pp. 195 - 200. ISBN 978-1-72816-503-5.
18. BLAHOVÁ, Marta, HROMADA, Martin. Vacuum Ambulance for Transporting Accessible Patient. In *ACM International Conference Proceeding Series*. New York: Association for Computing Machinery, 2020, pp. 94-97. ISBN 978-1-4503-7779-9.
19. BLAHOVÁ, Marta, HROMADA, Martin. Modeling and Visualization of Environmental Data in Space and Time Use of Gisv. In *International Multidisciplinary Scientific GeoConference Surveying Geology and Mining Ecology Management, SGEM* (Book No 2.1). Sofia: International Multidisciplinary Scientific Geoconference, 2020, pp. 523-530. ISSN 13142704. ISBN 978-619-7603-06-4.

20. KOTKOVÁ, Barbora, HROMADA, Martin. Comparsion of the Resulting Models of Dispersion of Hazardous Substances Created in the Software Aloha and Terex, In *International Multidisciplinary Scientific GeoConference Surveying Geology and Mining Ecology Management, SGEM* (Book No 2.1). Sofia: International Multidisciplinary Scientific Geoconference, 2020, pp. 73-80. ISSN 13142704. ISBN 978-619-7603-06-4.
21. ZIMEK, Ondřej, HROMADA, Martin. Risk Analysis of Selected Soft Target. In *International Multidisciplinary Scientific GeoConference Surveying Geology and Mining Ecology Management, SGEM* (Book No 2.1). Sofia: International Multidisciplinary Scientific Geoconference, 2020, pp. 283-290. ISSN 13142704. ISBN 978-619-7603-06-4.
22. KOTKOVÁ, Barbora, HROMADA, Martin. The Use of RFID Technology in Hospital. In *Annals of DAAAM and Proceedings of the International DAAAM Symposium*. Vienna: DAAAM International Vienna, 2020, s. 638-643. ISSN 17269679. ISBN 978-390273429-7.
23. BLAHOVÁ, Marta, HROMADA, Martin, MIKULIČOVÁ, Michaela. Utilization of Fractal Geometry Possibilities for Information Systems Security. In *Annals of DAAAM and Proceedings of the International DAAAM Symposium. Vienna: DAAAM International Vienna*, 2020, pp. 619-625. ISSN 17269679. ISBN 978-390273429-7.
24. VÍCHOVÁ, Kateřina, HROMADA, Martin, VALÁŠEK, Jarmil, PAULUS, František, Comparison Analysis the Use of Modern Technologies by Fire Rescue Service, In *Annals of DAAAM and Proceedings of the International DAAAM Symposium*, Volume 31, Issue 1, pp. 535 - 5412020 31st International DAAAM Virtual Symposium "Intelligent Manufacturing and Automation “, ISBN 978-390273429-7, DOI 10.2507/31st.daaam.proceedings.074.
25. KOTEK, Lukáš, HROMADA, Martin, LAPKOVÁ, Dora. Protection of Soft Targets from Terrorism. In *roceedings of the 2019 IEEE 6th Asian Conference on Defence Technology, ACDT 2019*. Piscataway, New Jersey: Institute of Electrical and Electronics Engineers Inc., 2019, pp. 71-78. ISBN 978-172811766-9.
26. VÁVRA, Jan, HROMADA, Martin. Evaluation of Data Preprocessing Techniques for Anomaly Detection Systems in Industrial Control System. In *Annals of DAAAM and Proceedings of the International DAAAM Symposium*. Vídeň: Danube Adria Association for Automation and Manufacturing (DAAAM), 2019, pp. 738-745. ISSN 17269679.
27. KOTKOVÁ, Barbora, HROMADA, Martin, MACH, Václav, BLAHOVÁ, Marta. Detection and Face Recignition of People by Camera for Security Applications. In *Annals of DAAAM and Proceedings of the International DAAAM Symposium*. Vídeň: Danube Adria Association for Automation and Manufacturing (DAAAM), 2019, pp. 610-614. ISSN 17269679.
28. BLAHOVÁ, Marta, MACH, Václav, PAVLÍK, Lukáš, FICEK, Martin, HROMADA, Martin. The Information Security to Software of Crisis Management. In *Annals of DAAAM*

and Proceedings of the International DAAAM Symposium. Vídeň: Danube Adria Association for Automation and Manufacturing (DAAAM), 2019, pp. 1019-1025. ISSN 17269679.

29. MRÁZEK, Jan, HROMADA, Martin, ĎURICOVÁ, Lucia. Reactivity to Crisis Situations in the Transport Sector. In *9th International Defense and Homeland Security Simulation Workshop, DHSS 2019*. Genoa: Dime University of Genoa, 2019, pp. 47-50. ISBN 978-88-85741-34-8.
30. ĎURICOVÁ, Lucia, JAŠEK, Roman, MRÁZEK, Jan, HROMADA, Martin. Soft Target Assessment Software. In *9th International Defense and Homeland Security Simulation Workshop, DHSS 2019*. Genoa: Dime University of Genoa, 2019, pp. 29-32. ISBN 978-88-85741-34-8.
31. VÁVRA, Jan, HROMADA, Martin. Novelty Detection System Based on Multi-Criteria Evaluation in Respect of Industrial Control System. In *Advances in Intelligent Systems and Computing*, Volume 765. Berlín: Springer Verlag, 2018, s. 280-289. ISSN 2194-5357. ISBN 978-331991191-5.
32. MRÁZEK, Jan, VÁVRA, Jan, HROMADA, Martin. The Evaluation Criteria in the Road Transported with Fuzzy Logic Support. In *Annals of DAAAM and Proceedings of the International DAAAM Symposium*. Vienna: DAAAM International Vienna, 2018, pp. 1187-1190. ISSN 1726-9679. ISBN 978-3-902734-20-4.
33. VÍCHOVÁ, Kateřina, HROMADA, Martin, FICEK, Martin, GRACLA, Michal. The Comparative Analysis of Safety in th Czech Republic and in Abroad. In *Annals of DAAAM and Proceedings of the International DAAAM Symposium*. Vienna: DAAAM International Vienna, 2018, pp. 1181-1186. ISSN 1726-9679. ISBN 978-3-902734-20-4.
34. VÁVRA, Jan, HROMADA, Martin. Evaluation of Anomaly Detection Based on Classification in Relation to SCADA. In *ICMT 2017 - 6th International Conference on Military Technologies. Brno: University of Defence*, 2017, pp. 330-334. ISBN 978-1-5386-1988-9.
35. ĎURICOVÁ, Lucia, HROMADA, Martin. The Proposal of the Analytical Tool for the Soft Targets Assessment. In *ICMT 2017 - 6th International Conference on Military Technologies. Brno: University of Defence*, 2017, pp. 387-391. ISBN 978-1-5386-1988-9.
36. ĎURICOVÁ, Lucia, HROMADA, Martin, MRÁZEK, Jan. The Proposal of the Software for the Soft Targets Assessment. In *Proceedings 2017 International Conference on Soft Computing, Intelligent System and Information Technology*. Washington, DC: IEEE Computer Society Conference Publishing Services (CPS), 2017, pp. 90-95. ISBN 978-1-4673-9899-2.
37. ĎURICOVÁ, Lucia, HROMADA, Martin, MRÁZEK, Jan. The Comparison Security Coefficient between University and Shopping Center. In *Safety and Reliability - Theory and Applications*. Leiden: CRC Press Balkema publishers, 2017, pp. 1485-1489. ISBN 978-1-138-62937-0.
38. MRÁZEK, Jan, ĎURICOVÁ, Lucia, HROMADA, Martin. The Proposal of Evaluation Criteria for Recoverability of Road Transport. In *Safety and Reliability - Theory and Applications*. Leiden: CRC Press Balkema publishers, 2017, pp. 133-137. ISBN 978-1-138-62937-0.

39. ŘEHÁK, David, HROMADA, Martin, RISTVEJ, Jozef. Indication of Critical Infrastructure Resilience Failure. In ČEPIN, M. and BRIŠ, R. (eds.), In *Safety and Reliability – Theory and Application (ESREL)*, 2017, pp. 963-970. ISBN 978-1-138-62937-0.
40. ĎURICOVÁ, Lucia, HROMADA, Martin, MRÁZEK, Jan. The Analytical Software Support for Evaluation to a Security and Safety Situation in the Soft Targets. In *Safety and Reliability - Theory and Applications*. Leiden: CRC Press Balkema publishers, 2017, pp. 1261-1268. ISBN 978-1-138-62937-0.
41. ĎURICOVÁ, Lucia, HROMADA, Martin, MRÁZEK, Jan. The Software for the Security Management in the Soft Targets. In *Proceedings of the International Defense and Homeland Security Simulation Workshop*, 2017. Genova: DIME University of Genova, 2017, pp. 61-67. ISBN 978-88-97999-98-0.
42. VÁVRA, Jan HROMADA, Martin. Determination of Optimal Cluster Number in Connection to SCADA. Sotware Engineering Trends and Techniques in Intelligent Systems, CSOC2017, VOL 3 Book Series: In *Advances in Intelligent Systems and Computing*. Cham: Springer International Publishing AG, 2017, pp. 136-147. ISSN 2194-5357. ISBN 978-3-319-57141-6.
43. MRÁZEK, Jan, ĎURICOVÁ, Lucia, HROMADA, Martin. Increased Safety Road Transporter. In *6th International Defense and Homeland Security Simulation Workshop, DHSS 2016*. Genoa: Dime University of Genoa, 2016, pp. 31-34. ISBN 978-88-97999-71-3.
44. HROMADA, Martin, LUKÁŠ, Luděk. Management of Protection of Czech Republic Critical Infrastructure Elements. In *Recent Researches in Automatic Control*. Montreux: WSEAS Press, 2011, s. 306-309. ISBN 978-1-61804-004-6.
45. LUKÁŠ, Luděk, HROMADA, Martin. Utilization of the EASI model in the matters of critical infrastructure protection and its verification via the OTB SAF simulation tool. In *Recent Researches in Automatic Control*. Montreux: WSEAS Press, 2011, pp. 131-136. ISBN 978-1-61804-004-6.
46. LUKÁŠ, Luděk, HROMADA, Martin. Risk analysis in context of Critical Infrastructure Protection. In *Annals of DAAAM for 2011 & Proceedings of the 22nd International DAAAM Symposium "Intelligent Manufacturing & Automation: Power of Knowledge and Creativity"*. Vienna: DAAAM International Vienna, 2011, pp. 1469-1470. ISSN 1726-9679. ISBN 978-3-901509-83-4.

Odborné knihy a kapitoly v anglickom jazyku

1. ĎURICOVÁ, Lucia, HROMADA, Martin. *The Assessment of the Soft Targets.* Advances in Networks, Security and Communications: Reviews. Barcelona: IFSA Publishing, S. L., 2017, pp. 201-2013. ISBN 978-84-697-8994-0.
2. ĎURICOVÁ, Lucia, HROMADA, Martin. *The Mathematical Modeling of Road Transport in Context of Critical Infrastructure Protection*. Advances in Networks, Security and Communications: Reviews. Barcelona: IFSA Publishing, S. L., 2018, pp. 187-199. ISBN 978-84-697-8994-0.

3. VÍCHOVÁ, Kateřina, HROMADA, Martin. *Information Support of Crisis Management*. Crisis Management: Theory and Practice. Londýn: IntechOpen, 2018, pp. 37-58. ISBN 978-1-78923-234-9.
4. ĎURICOVÁ, Lucia, HROMADA, Martin, MRÁZEK, Jan. *The Software to the Soft Target Assessment*. Software Design and Modelling. Londýn: IntechOpen, 2019, pp. 1-10. ISBN 978-1-78984-619-5.
5. MRAZEK J, HROMADA M AND DURICOVA MRAZKOVA L (2020) *The Methodological Standard to the Assessment of the Traffic Simulation in Real Time*. Introduction to Data Science and Machine Learning. IntechOpen. DOI: 10.5772/intechopen.86961.
6. KOTKOVÁ, Barbora, HROMADA, Martin, MACH, Václav. *Detection and Recognition of People by Camera – Reliability and Use*. DAAAM International Scientific Book 2019. Vienna: DAAAM International Vienna, 2020, pp. 233-240. ISBN 978-3-902734-24-2.
7. ŘEHÁK, David, HROMADA, Martin, GKOTSIS, Ilias, GAZI, Anna, AGRAFIOTI, Evita, CHALKIDOU, Anastasia, JURKIEWICZ, Karolina, BOLLETTA, Fabio, FUGGINI, Clemente. *Validation Strategy as a Part of the European Gas Network Protection*. In ROSATO, Vittorio, DI PIETRO, Antonio (Eds.), *Issues on Risk Analysis for Critical Infrastructure Protection*. London: IntechOpen, 2020. ISBN 978-1-83962-621-0.
8. HROMADA, Martin, ŘEHÁK, David, WALKER, Neil. *Electricity Infrastructure Technical Security: Practical Application and Best Practices of Risk Assessment*. In ŘEHÁK, David, BERNATÍK, Aleš, DVOŘÁK, Zdeněk, HROMADA, Martin (Eds.), Safety and Security Issues in Technical Infrastructures. Hershey, PA: IGI Global, 2020, pp. 1-30. ISBN 978-1-7998-3059-7. DOI: 10.4018/978-1-7998-3059-7.ch001
9. ŘEHÁK, David, ŠENOVSKÝ, Pavel, HROMADA, Martin. *Analysis of Critical Infrastructure Network.* In CHEN, Z., DEHMER, M., EMMERT-STREIB, F., SHI, Y. (eds.). Modern and Interdisciplinary Problems in Network Science: A Translational Research Perspective. Boca Raton, FL: CRC Press, 2018, pp. 143-171. ISBN 9780815376583.
10. ŘEHÁK, David, HROMADA, Martin. *Failures in a Critical Infrastructure System*. In NAKAMURA, Takafumi (ed.). System of System Failures. London: IntechOpen, 2018, pp. 75-93. ISBN 978-1-78923-047-5. DOI: 10.5772/intechopen.70446

Odborné knihy a kapitoly v českom jazyku

1. ŘEHÁK D., ŠPLÍCHALOVÁ A., HROMADA M., LOVEČEK T., HLAVATÝ R., 2022, *Využití indikátorů v ochraně kritické infrastruktury*, Sdružení požárního a bezpečnostního inženýrství, z.s. v Ostravě, 1. vydání, ISBN 978-80-7385-259-7.
2. HROMADA, Martin, LUKÁŠ, Luděk, MATEJDES, Milan, VALOUCH, Jan, NEČESAL, Luboš, RICHTER, Rostislav, KOVÁŘÍK, František. *Systém a způsob hodnocení odolnosti kritické infrastruktury*.

1 vyd. Ostrava: Sdružení požárního a bezpečnostního inženýrství, 2013. 177 s. Neuveden. ISBN 978-80-7385-140-8.

3. HROMADA, Martin, LUKÁŠ, Luděk, VALOUCH, Jan, RICHTER, Rostislav, KOVÁŘÍK, František. *Ochrana kritické infrastruktury ČR v odvětví energetiky*. 1 vyd. Ostrava: Sdružení požárního a bezpečnostního inženýrství, 2014. 272s. 1. ISBN 978-80-7385-144-6.
4. HROMADA, M., HRŮZA, P., KADERKA, J., LUŇÁČEK, O., NEČAS, M., PTÁČEK, B., SKORUŠA, L., SLOŽIL, R. (10), *Kybernetická bezpečnost - Teorie a praxe*, Vydavatelství Powerprint, Praha, 2015, 250s., ISBN 978-80-87994-72-6.
5. ŘEHÁK, David, HROMADA, Martin, ŠENOVSKÝ, Pavel. *Resilience kritické infrastruktury: Teorie, principy, metody.* 1. vyd. Ostrava: Sdružení požárního a bezpečnostního inženýrství, 2019. 107 s. ISBN 978-80-7385-224-5.
6. HROMADA, Martin. *Preprava peňažnej hotovosti a cenností – taktika a organizácia*. Bezpečnostní technologie, systémy a management III. Zlín: VeRBuM, 2013, s. 229-245. ISBN 978-80-87500-35-4.
7. HROMADA, Martin. *Inštitucionálizácia bezpečnosti v Egyptskej ríši*. Teorie bezpečnosti II. Zlín: Radim Bačuvčík – VeRBuM, 2020, s. 142-162. ISBN 978-80-88356-06-6.
8. LUKÁŠ, Luděk, HROMADA, Martin. *Modely zajištění bezpečnosti*. Teorie bezpečnosti I.. Zlín: Radim Bačuvčík - VeRBuM, 2017, s. 72-85. ISBN 978-80-87500-89-7.
9. HROMADA, Martin. *Energetická bezpečnosť*. Teorie bezpečnosti I.. Zlín: Radim Bačuvčík – VeRBuM, 2017, s. 111-122. ISBN 978-80-87500-89-7.
10. HROMADA, Martin. *Kybernetická bezpečnosť*. Teorie bezpečnosti I.. Zlín: Radim Bačuvčík – VeRBuM, 2017, s. 123-133. ISBN 978-80-87500-89-7.
11. HROMADA, Martin. *Odolnosť referenčného objektu*. Konvergovaná bezpečnost. Zlín: Radim Bačuvčík - VeRBuM, 2019, s. 98-112. ISBN 978-80-87500-99-6.

Certifikované metodiky a softwarové nástroje

1. HROMADA, Martin, FRÖHLICH, Tomáš. *Metodika zvyšování ochrany a odolnosti vybraných kategorií měkkých cílů*. Zlín: Univerzita Tomáše Bati ve Zlíně, 2021.
2. HROMADA, M., APELTAUER, T., KOTKOVÁ, D., *Metodika identifikace a ochrany objektů dopravní infrastruktury*, Brno, VUT v Brně, Fakulta stavební, 2021.
3. ŘEHÁK, D. a kolektiv. *Metodika identifikace indikátorů narušení resilience prvků kritické infrastruktury.* Ostrava: VŠB – Technická univerzita Ostrava, 2022. 29 s.
4. FUCHS, Pavel, HROMADA, Martin, KOUCKÝ, Miroslav. *Metodika určování semikvantitativních atributů dynamického modelování souvztažnosti v kritické infrastruktuře*. 2018, CERO 1/2018.
5. HROMADA, Martin, LUKÁŠ, Luděk. *Metodika hodnocení odolnosti vybraných prvků a systému prvků kritické infrastruktury*. 2013, MV-125879-1/PO-OKR-2013.

6. POKORNÝ, Jiří, ŘEHÁK, David, ADAMEC, Vilém, HROMADA, Martin, ROSENKRANZ, Jiří, HRUBÝ, Václav, BLAŽKOVÁ, Kateřina, PAULUS, František, MICHALCOVÁ, Lenka, FRÖHLICH, Tomáš, NOVOTNÝ, Petr, SLIVKOVÁ, Simona, MACHALOVÁ, Barbora. *Metodika pro ochranu obyvatelstva v územním plánování a ve stavebním řízení*. 2020, CERO 9/2020
7. HROMADA, Martin, FRÖHLICH, Tomáš. *Metodika kategorizace a prioritizace objektů nezbytných při obnově dodávek elektrické energie po blackoutu*. 2019, CERO 2/2019,
8. HROMADA, Martin, ŘEHÁK, David, FRÖHLICH, Tomáš, KOVÁŘÍK, František. *Metodika hodnocení krizové připravenosti územních celků s vazbou na vnější resilienci kritické infrastruktury.* [Certifikovaná metodika]. Zlín: Univerzita Tomáše Bati ve Zlíně, Fakulta aplikované informatiky, 2019. 40 s. Ev.č: CERO 9/2019. DOI: 10.13140/RG.2.2.16384.38409
9. ŘEHÁK, David, ŠENOVSKÝ, Pavel, HROMADA, Martin, PIDHANIUK, Lukáš, DVOŘÁK, Zdeněk, LOVEČEK, Tomáš, RISTVEJ, Jozef, LEITNER, Bohuš, SVENTEKOVÁ, Eva, MARIŠ, Ladislav. *Metodika hodnocení resilience prvků kritické infrastruktury (CIERA).* [Certifikovaná metodika]. Ostrava: VŠB-TUO, 2018. 90 s. ISBN 978-80-248-4164-9. Ev.č: CERO 2/2018.
10. HROMADA, Martin, ŘEHÁK, David, *Zásady pro projektování a bezpečné provozování LNG čerpacích stanic*, [Certifikovaná metodika]. Praha: Technologická platforma, energetická bezpečnost ČR, 2021, Č. j.: MD-634/2021-710/4.

9.2 Vedecko-výskumná činnosť

Mezinárodní projekty (EU)	Národní projekty (TA ČR, GA AV ČR)	Resortní projekty
3	5	19

Medzinárodné a zahraničné granty:

2020 – 2022 *S4AllCities: Smart Spaces Safety and Security for All Cities* (883522), European Commission H2020-SU-INFRA-2019, Člen riešitelského tímu

2020 – 2022 *STAMINA: Demonstration of Intelligent Decision Support for Pandemic Crisis Prediction and Management within and Across European Borders* (883441), European Commission H2020-SUSEC-2019, Člen riešitelského tímu

2019 – 2021 *SecureGas: Securing The European Gas Network* (833017), European Commission H2020-SU-INFRA-2018, Člen riešitelského tímu

Projekty štátnych grantových agentúr:

2022 – 2025 *Výzkum stavebně-technických požadavků na využití národní pozemní infrastruktury TEN-T k řešení krizových situací velkého rozsahu* (CK03000182), Technologická agentura ČR, Riešiteľ projektu

2020 – 2023 *SECURAIL: Zvýšení odolnosti a bezpečnosti železniční infrastruktury a minimalizace dopadů na ostatní sektory dopravní infrastruktury* (CK01000015), Technologická agentura České republiky, Riešiteľ projektu

2019 – 2021 *Vývoj metod identifikace a ochrany měkkých cílů dopravní infrastruktury pro zvýšení jejich bezpečnosti a odolnosti před teroristickým útokem* (VB01000008), Technologická agentura ČR, Riešiteľ projektu

2019 – 2021 *Klasifikace sociálně-psychologických parametrů osob prostřednictvím umělé inteligence a strojového vidění pro potřeby ochrany osob v reálném čase* (TL02000352), Technologická agentura České republiky, Člen riešitelského týmu

2018 – 2021 *Projektování a bezpečné provozování LNG čerpacích stanic* (TK01010146), Technologická agentura České republiky, Člen riešitelského tímu

Rezortné ministerské granty:

2023 – doteraz *STRENGTH 2023: Posilování resilience subjektů pozemní dopravní kritické infrastruktury,* VK01030014, Ministerstvo vnitra České republiky, Člen riešitelského tímu

2022 – doteraz *Systém hodnocení bezpečnostních aspektů hromadných společenských akcí ve vztahu k vybraným bezpečnostním incidentům* (VB01000041), Ministerstvo vnitra České republiky, Člen riešitelského tímu

2022 – doteraz *Digitální modelování evakuačních plánů v zájmových stavbách a měkkých cílech s prvky umělé inteligence* (VB01000034), Ministerstvo vnitra České republiky, Člen riešitelského tímu

2022 – doteraz *FLAPRIS – Systém pro podporu zpřesněné a včasné předpovědi nebezpečí vzniku přívalových povodní a usnadnění činností krizových a povodňových orgánů kraje*, (VB01000008) Ministerstvo vnitra České republiky, Riešiteľ a manažér projektu

2021 – 2022 *Informační platforma krizové logistiky* (VI04000080), Ministerstvo vnitra České republiky, Člen riešitelského tímu

2020 – 2021 *Ochrana kritické infrastruktury II*, Ministerstvo průmyslu a obchodu ČR, OPPIK, Člen riešitelského tímu

2020 – 2021 *Minimalizace rizik vzniku událostí ve společensky významných objektech* (VH20202021056), Ministerstvo vnitra České republiky, Člen riešitelského tímu

2020 – 2022 *CIRFI 2019: Indikace narušení resilience kritické infrastruktury* (VI20192022151), Ministerstvo vnitra České republiky, Ministerstvo vnitra České republiky, Riešiteľ projektu

2019 – 2022 *Ochrana měkkých cílů v bezpečnostním prostředí ČR* (VI20192022118), Ministerstvo vnitra České republiky, Riešiteľ projektu

2019 – 2022 *Systém zpřesněné předpovědi konvektivních srážek pro krajský územní celek* (I20192022134), Ministerstvo vnitra České republiky, člen riešitelského tímu projektu

2018 – 2020 *Ochrana obyvatelstva v územním plánování a při stanovení technických podmínek pro navrhování staveb* (VH20182020042), Ministerstvo vnitra České republiky, Člen riešitelského týmu

2017 – 2019 *Analytický programový modul pro hodnocení odolnosti v reálném čase z hlediska konvergované bezpečnosti (RECOS)* (VI20172019054), Ministerstvo vnitra České republiky, Riešiteľ projektu

2017 – 2019 *Identifikace a metody ochrany měkkých cílů ČR před násilnými činy s rozpracováním systému včasného varování* (VI20172019073), Ministerstvo vnitra České republiky, Riešiteľ projektu

2018 – 2020 *Ochrana obyvatelstva v územním plánování a při stanovení technických podmínek pro navrhování staveb* (VH20182020042), Ministerstvo vnitra České republiky, Člen riešitelského tímu

2016 Souhrn způsobů hodnocení kvality a odolnosti infrastruktury (26432), Úřad vlády ČR, Člen riešitelského tímu

2015 – 2019 *RESILIENCE 2015: Dynamické hodnocení odolnosti souvztažných subsystémů kritické infrastruktury* (VI20152019049), Ministerstvo vnitra České republiky, Riešiteľ a manažér projektu

2014 – 2015 *Aktuální kybernetické hrozby v České republice a jejich eliminace* (VF20142015035), Ministerstvo vnitra České republiky, Řešitel projektu

2011 – 2014 *Systém hodnocení odolnosti prvků a sítí vybraných oblastí kritické infrastruktury* (VG20112014067) Fakulta aplikované informatiky UTB ve Zlíně, Ministerstvo vnitra České republiky, Riešiteľ projektu

2010 – 2012 *Metodika ochrany kritické infrastruktury (KI) v oblasti výroby, přenosu a distribuce elektrické energie* (VG20102012025), Ministerstvo vnitra České republiky, Riešiteľ projektu

9.3 Pedagogická činnosť

Disertační práce	Diplomové práce	Bakalářské práce
3	161	13

Výchova doktorandov

2016 – 2020 Ing. Kateřina Víchová, Ph.D.

Téma disertačnej práce: *Algoritmizace hodnocení připravenosti zdravotnických zařízení čelit výpadku dodávky elektrické energie*

2014 – 2020 Ing. Jan Vávra, Ph.D.

Téma disertačnej práce: *Návrh a ověření systému detekce anomálií založeného na strojovém učení v průmyslových řídicích systémech* – v rámci tejto dizertačnej

2014 – 2019 Ing. Lucia Mrázková, Ph.D.

Téma disertačnej práce: *Hodnotenie bezpečnosti mäkkých cieľov*

práce som bol vedený ako konzultant/školiteľ špecialista

Aktuálne študujúci:

2020 – doteraz Ing. Červený Vlastimil

Téma disertačnej práce: *Objektivizace metod a procesů řízení kybernetické bezpečnosti*

2020 – doteraz Ing. Dostálová Petra

Téma disertačnej práce: *Optimalizace procesního řízení rizik při vzniku pandemie v soukromých společnostech*

2020 – doteraz Ing. Malatinský Adam

Téma disertačnej práce: *Proaktívne spôsoby požiarnej bezpečnosti vybranej skupiny objektov vo vzťahu k aktívnej prevencii a represii*

2020 – doteraz Hemin Akram Muhammad. MSc.

Téma disertačnej práce: *Protection of Privacy Information in E-government*

2019 – doteraz Ing. Kalvach Zdeněk

Téma disertačnej práce: *Význam a efektivita technologií v bezpečnostních systémech měkkých cílů*

2019 – doteraz Ing. Blahová Marta

Téma disertačnej práce: *Zvyšování odolnosti měkkých cílů*

2019 – doteraz Ing. Čajková Nikola

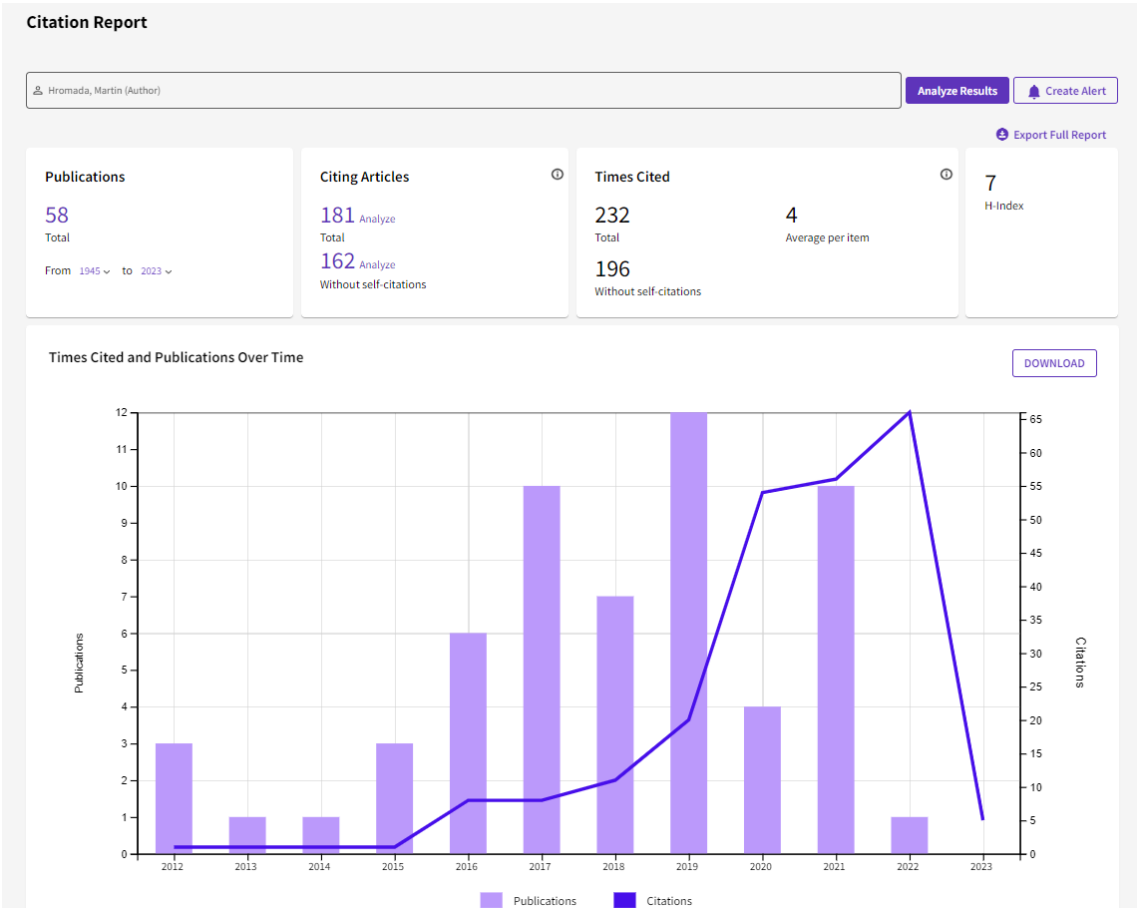
Téma disertačnej práce: *Technologické a procesní aspekty ochrany vybrané skupiny měkkých cílů*

Pedagogická činnost

2021– doteraz	Garancia a výuka predmetu „Technologie krizového řízení“ na Fakultě aplikované informatiky, UTB ve Zlíně
2021– doteraz	Garancia a výuka predmetu „Ochrana obyvatelstva“ na Fakultě aplikované informatiky, UTB ve Zlíně
2018 – doteraz	Garancia predmetu „Fyzická ostraha, Bezpečnostní inženýrství, Bakalářská práce, Požární ochrana,
2018 – doteraz	Garancia a výuka predmetu DSP Bezpečnostní technologie systémy a management „Ochrana kritické infrastruktury a měkkých cílů“ na Fakultě aplikované informatiky, UTB ve Zlíně
2018 – doteraz	Garancia a výuka predmetu DSP Bezpečnostní technologie systémy a management „Krizové řízení a ochrana obyvatelstva“ na Fakultě aplikované informatiky, UTB ve Zlíně
2018 – doteraz	Garancia a výuka predmetu DSP Bezpečnostní technologie systémy a management „Bezpečnostní prognostika“ na Fakultě aplikované informatiky, UTB ve Zlíně
2018 – doteraz	Garancia bakalárského študijného programu: Bezpečnostní technologie, systémy a management
2012 – doteraz	Garancia a výuka predmetu „Management bezpečnostního inženýrství“ na Fakultě aplikované informatiky, UTB ve Zlíně
2012 – 2021	Garancia a výuka predmetu „Speciální technologie komerční bezpečnosti“ na Fakultě aplikované informatiky, UTB ve Zlíně
2012 – 2021	Garancia a výuka predmetu „Modelování krizových situací“ na Fakultě aplikované informatiky, UTB ve Zlíně

9.4 H-index, citácie a oponentská činnosť

	H-index/počet citácií	**H-index/počet citácií (bez autocitacií)**
Web of Science	7/232	7/193
Scopus	10/345	9/298
Google Scholar	14/880	-


Citation Report
Hromada, Martin (Author)
Analyze Results
Create Alert
Export Full Report
Publications
58
Total
From 1945 to 2023
Citing Articles
181 Analyze
Total
162 Analyze
Without self-citations
Times Cited
232
Total
4
Average per item
196
Without self-citations
7
H-Index
Times Cited and Publications Over Time
DOWNLOAD
Publications
Citations
2012
2013
2014
2015
2016
2017
2018
2019
2020
2021
2022
2023
Publications
Citations


This author profile is generated by Scopus. Learn more
Hromada, Martin
Univerzita Tomáše Bati ve Zlíně, Zlin, Czech Republic
55246365500
https://orcid.org/0000-0003-0347-7528
View more
469
Citations by 354 documents
112
Documents
10
h-index View h-graph
Set alert
Save to list
Edit profile
More
Document & citation trends
Documents
Citations
2011
2023
Most contributed Topics 2017–2021
Attack; Supervisory Control; Intrusion Detection
7 documents
Radicalization; Attack; Counterterrorism
4 documents
Cascading Failure; Giant Component; Robustness
4 documents
Analyze author output
Citation overview
View all Topics
Documents
0 Preprints
60 Co-Authors
52 Topics
0 Awarded Grants
Beta
Documents (112)
Cited by (354)

Martin Hromada

SLEDOVAT

Univerzita Tomáše Bati ve Zlíně
E-mailová adresa ověřena na: fai.utb.cz - Domovská stránka
kritická infrastruktura bezpečnost analýza rizik fyzická bezpečnosť

NÁZEV	CITACE	ROK
Complex approach to assessing resilience of critical infrastructure elements D Rehak, P Senovsky, M Hromada, T Lovecek International journal of critical infrastructure protection 25, 125-138	167	2019
Cascading impact assessment in a critical infrastructure system D Rehak, P Senovsky, M Hromada, T Lovecek, P Novotny International Journal of Critical Infrastructure Protection 22, 125-138	81	2018
Quantitative evaluation of the synergistic effects of failures in a critical infrastructure system	80	2016

Citace ZOBRAZIT VŠECHNY

	Všechny	Od 2018
Citace	880	722
h-index	14	12
i10-index	18	15