TECHNOLOGICKÁ PLATFORMA
ENERGETICKÁ BEZPEČNOST ČR

Strategická výzkumná agenda

Technologická platforma „Energetická bezpečnost ČR“

Obsah

Strategická výzkumná agenda TPEB – shrnutí

SVA TPEB vychází z aktuálních technologických priorit, které byly definovány v rámci analytických dokumentů EK zabývajících se problematikou ochrany kritické infrastruktury. Současně reflektuje potřeby domácího trhu pro zajištění bezpečnosti a stability v této oblasti.

SVA TPEB navazuje na předchozí strategické dokumenty, které byly aktualizovány v rámci úspěšně vyřešených projektů Energetická a kybernetická bezpečnost (OPPI) a Ochrana kritické infrastruktury (OPPIK) a jsou dále průběžně doplňovány.

SVA TPEB je taktéž připravována v souladu s podpůrnými studiemi a analýzami EK (DG Research and Innovation), které souvisejí zejména s hodnocení programu Horizon 2020 a přípravami navazujícího programu Horizon Europe. Zejména se zde jedná o tzv. Lamyho zprávu, která se stala základem sdělení EK COM(2018) 2 z 11. ledna 2018 týkající se vyhodnocení programu H2020 a zejména doporučení pro formování následného programu Horizon Europe.

SVA TPEB odráží i priority konkurenčních světových entit, zejména USA. V mnoha případech zde existují dohody o spolupráci a výměně informací. Tento přístup by měl členským státům EU zajistit, aby se v příštích letech mohly stát nezastupitelným spolutvůrcem nových technologií a souvisejících legislativně procesních postupů.

Klíčovou oblastí zájmu TPEB je zprostředkování příležitostí pro aplikovaný výzkum a vývoj v oblasti ochrany kritické infrastruktury. Vzhledem ke značné provázanosti jednotlivých sektorů kritické infrastruktury a technologickým řešením jdoucím napříč, bude TPEB iniciovat a podporovat VaVaI projekty zaměřené také na oblasti komunikačních technologií, kybernetické bezpečnosti či fyzické bezpečnosti.

Aktivity TPEB jsou a budou zaměřeny primárně na stimulaci zapojování českých firem a VaVaI institucí do mezinárodních projektových konsorcií v rámci programu H2020. TPEB pak hodlá využít stávající národní programy na podporu vědy a výzkumu, zejména programu Bezpečnostního výzkumu České republiky a projektových výzev TAČRu.

Představení TPEB

Technologická platforma „Energetická bezpečnost ČR“ (dále jen TPEB) vznikla z iniciativy Hospodářského výboru Poslanecké sněmovny ČR a MPO ČR na konci roku 2011. Jedná se o unikátní projekt partnerství veřejného a soukromého sektoru (PPP projekt), a to jak v českém, tak i evropském kontextu. TPEB se zaměřuje na v současnosti velmi dynamickou problematiku ochrany kritické infrastruktury v energetickém sektoru s přesahy do dalších sektorů kritické infrastruktury. V duchu PPP tvoří členskou základnu významné infrastrukturní společnosti, utilitní firmy, orgány státní správy a samosprávy a vědecké a výzkumné organizace.

TPEB reprezentuje a podporuje oprávněné a společné zájmy svých členů v oblasti výzkumu, vývoje a aplikace moderních technologií zvyšujících úroveň bezpečnosti, resilience a stability infrastrukturních systémů v ČR. Dále přispívá ke vzájemné koordinaci aktivit a informovanosti subjektů státní správy, subjektů výzkumu a vývoje a dodavatelů bezpečnostních technologií, a to v návaznosti na výzkumné a vývojové programy EU, NATO a ČR. V rámci velkých evropských projektů také napomáhá formulování a naplňování českých zájmů v procesech normotvorby a formulování politik, které jsou významnou součástí evropských projektů. Ve zmíněném duchu TPEB spolupracuje i s řadou subjektů, které nejsou členy platformy. Podle jejich odbornosti je přizývá do společných programů a projektů.

Ve své činnosti se TPEB soustředí především na podporu podávání projektů v oblasti aplikovaného výzkumu a vývoje, expertní aktivity v oblasti strategií, normotvorby a standardizace a osvětovou činnost propojující znalosti a schopnosti jednotlivých pilířů PPP projektu. Všechny tyto aktivity vykonává v národním i evropském kontextu, často v úzké součinnosti s institucemi a orgány EK.

Aktivity TPEB:

- Reprezentuje a podporuje oprávněné a společné zájmy svých členů v oblasti výzkumu, vývoje a aplikace moderních technologií zvyšujících úroveň ochrany kritické infrastruktury v ČR a EU
- Přispívá k vzájemné koordinaci aktivit a informovanosti subjektů státní správy, subjektů výzkumu a vývoje a dodavatelů bezpečnostních technologií, a to v návaznosti na programy EU, NATO, ČR a související finanční zdroje
- Usiluje o zapojení svých členů do evropských struktur, projektů a platforem, které se zabývají koordinovaným zvyšováním úrovně ochrany kritické infrastruktury
- Usiluje o využití vědeckých, výzkumných a technologických schopností svých členů a jejich zapojení do projektů EU s cílem zvyšovat konkurenceschopnost ČR
- Systematicky mapuje celosvětovou situaci a vývoj v oblasti vědy, výzkumu a trendů v zavádění moderních technologií v oblasti ochrany kritické infrastruktury
- Aktivně se podílí na vytváření souvisejících standardů a metodik pro nastavení závazné certifikace pro oblast energetické a kybernetické bezpečnosti.
- Poskytuje expertízy a konzultace pro orgány státní správy a samosprávy v oblastech souvisejících s ochranou kritické infrastruktury s důrazem na vyhodnocení

míry ohrozitelnosti a zranitelnosti krizových míst

- Zpracovává a realizuje projekty v oblasti vědy, výzkumu a zavádění moderních bezpečnostních technologií, žádosti o jejich financování a poskytuje související poradenský servis
- Vhodnou formou propaguje související aktivity a technologie českých subjektů v zahraničí s cílem podpory konkurenceschopnosti a exportu ČR a zapojení do zahraničních struktur a aktivit

Členové TPEB:

1.IČO: 61989100 Centrum ENET, Ostrava – Poruba, 17. listopadu 15/2172

2.IČO: 26129558 CNS a.s., Mělník Nad Šafranicí 574

3. IČO: 25702556 ČEPS a.s., Praha 10, Elektrárenská 774/2

4.IČO: 06578705 Česká agentura pro standardizaci, Praha 1, Biskupský dvůr 1148/5

5. IČO: 68407700 ČVUT Praha řádný člen, Praha 6, Zikova 4

6. IČO: 45274649 ČEZ, a.s. Praha 4, Duhová 2

7. IČO: 29040639 DOSTAV ENERGO, s.r.o., Praha 2, Na Moráni 1750/4

8. IČO: 60916427 ERA a.s., Pardubice, Průmyslová 387

9. IČO: 00007064 Hasičský záchranný sbor ČR -MV ČR Praha 7, Nad Štolou 936/3

10.IČO: 00216224 Masarykova univerzita Brno Žerotínovo nám.617/9

11.IČO: 70890692 Moravskoslezský kraj Ostrava 28. října 117

12. IČO: 48591254 TTC MARCONI s.r.o., Praha 10, Třebohostická 987/5

13.IČO: 70883521 Univerzita Tomáše Bati ve Zlíně, Zlín Nad Stráněmi 4511

14. IČO: 24272523 Vojenský technický ústav s.p. Praha 9, Mladoboleslavská 944

15. IČO: 61989100 VŠB – TUO, Ostrava -Výškovice , Lumírova 630/13

16.IČO: 00216305 Vysoké učení technické v Brně, Brno Antonínská 548/1

17. IČO: 397563 Žilinská univerzita v Žilině, Žilina, Univerzitná 8215/1

Úvod

Světový bezpečnostní průmysl je jedním z mála sektorů, který vykazuje velmi výrazný potenciál růstu a zaměstnanosti, a to především s ohledem na obecně zhoršující se bezpečnostní situaci ve světě a na skutečnost, že výkonné orgány výrazně preferují technologické odpovědi na existující hrozby. V rámci EU pracuje v bezpečnostním sektoru 180,000 lidí, přičemž obrat dosahuje 30 mld. €. Nehledě na velkou segmentaci tohoto trhu tvoří evropské firmy 25% z celkového světového objemu, a to díky vyspělým technologiím, které vlastní a vyvíjejí. Podle provedených analýz výkonnosti a konkurenceschopnosti evropských firem se však odhaduje pokles tohoto podílu na 20% do roku 2020. Pro udržení zmíněného podílu a jeho dalšího růstu provádí EK řadu legislativních opatření a stimulačních kroků, které mají vést k harmonizaci a rozvoji odvětví, podobně jak tomu je v USA, které je světovým technologickým vůdcem v uvedené oblasti.

Mezi hlavní segmenty evropského bezpečnostního průmyslu patří letecká bezpečnost, námořní bezpečnost, ochrana hranic, ochrana kritické infrastruktury včetně energetiky, kybernetická bezpečnost a komunikace a fyzické zabezpečení ochrany. Oblast ochrany kritické infrastruktury a energetiky představuje na světovém trhu 12,6 mld. € a v Evropě 3,5 mld €.

Analýzy stavu bezpečnostního průmyslu v EU prováděné EK uvádí dva základní závěry:

1) Evropský bezpečnostní trh je velmi fragmentovaný. Je to dáno tím, že průmysl v každém členském státu vyvíjí a aplikuje produkty a systémy, které nejsou kompatibilní s ostatními a tudíž v případě ohrožení systému (např. distribuční sítě), který je na území několika států, není možné aplikovat jednotné standardizované postupy přes jednotné standardizované systémy a řešit tak případné mimořádné situace. S tím souvisí i rozdílná legislativa pro krizové řízení v členských státech.

2) V EU existuje „propast“ mezi výzkumem a trhem jako výsledek chybějící efektivní koordinace při podpoře výzkumu a aplikace následných výstupů tohoto výzkumu do praxe. Tato skutečnost má dva základní negativní důsledky, které představuje neefektivní nakládání s prostředky a technologické zaostávání (primárně za USA, ale i nastupujícími technologickými velmocemi).

V reflexi těchto skutečností EU přeformulovala svoji politiku VaV, kdy výzvy programu

H2020 mnohem více než původní Rámcové programy akcentují uvedení technologií do praxe, na trh či minimálně její pilotní odzkoušení. Zároveň značná část výzev obsahuje i požadavky na návrhy společných evropských standardů v daných oblastech. Současně se tyto priority odrážejí i ve strategických dokumentech (např. Bezpečnostní průmyslová strategie COM (2012) 417 apod.) a politikách (např. Industry for Security – DG Migration and Home Affairs). Výše zmíněné dokumenty hodnotící H2020 naznačují, že v rámci programu Horizon Europe budou tyto trendy ještě zvýrazněny.

TPEB ČR svojí dosavadní činností vstupuje do evropských debat, a to prostřednictvím spolupráce s platformami či účastí v projektových konsorciích H2020.

Platformy:

- **ERNCIP (European Reference network for Critical Infrastructure Protection)**. Jedná se o poradní orgán EK (projekt iniciovaný DG Home), který analyzuje evropské laboratoře a zkušebny a doporučuje jejich využívání pro nové technologie z oblasti ochrany kritické infrastruktury, energetiky, komunikace, ICT apod.
- **Poradní orgány standardizačního úřadu EK CEN/CENELEC**
- **TPEB také dlouhodobě spolupracuje s European Organisation on Security (EOS).** EOS je bruselskou platformou sjednocující 43 špičkových výzkumných ústavů, firem a institucí z 13 evropských států a představujících cca 65% průmyslového bezpečnostního trhu. Jedná se o nejvýznamnější uskupení tohoto druhu v EU.
- TPEB rozvíjí své projektové aktivity také prostřednictvím navazováním spolupráce s evropskými technologickými platformami (ETP). Výsledné projekty vycházejí mimojiné ze struktur ETP NETWORLD 2020 (https://www.networld2020.eu/), se kterou platforma navázala hlubší vztahy během projektové cesty do Atén prostřednictvím firem, které jsou součástí této ETP. Dlouhodobě kooperativní vztahy lze vysledovat také s ETP Artemis, ve které působí dvě největší české technické školy, které jsou zároveň součástí platformy. Prospektivně se také jeví platforma Sustainable Nuclear Energy Platform (SNETP) ze sekce Energy, která pořádala výroční konferenci Nuclear Days 2018 v Praze. V této ETP již působí zástupci Centra jaderného výzkumu Řež a Ústavu jaderného výzkumu Řež, které dlouhodobě představují jedny z nejúspěšnějších českých institucí v kontextu rámcových programů a H2020.

Projekty

H2020 (ÚSPĚŠNĚ PODANÉ ČI ZÍSKANÉ):

CySmart – Adaptive Cyber Security for Low Resource Wireless Communications Systems.

Projekt přijat do výzvy H2020 ICT-32-2014: Cybersecurity, Trustworthy ICT

V čele projektového konsorcia stála University of Sheffield a jeho součástí byly výzkumné organizace a firmy ze Spojeného království, Německa, Rakouska, Francie a České Republiky. Z české strany na projektu kromě TPEB participovaly i VUT Brno a společnost Monet+. Cílem projektu bylo představit adaptivní řešení kybernetické bezpečnosti wireless ICT systémů kombinujících inovativní zabezpečení na úrovni kryptografické bezpečnosti i fyzické bezpečnosti. Součástí projektu je i ověření konceptu adaptivní bezpečnosti v reálném prostředí. TPEB v projektové konsorciu zastávala roli diseminačního a exploitačního aktéra a zároveň přijala odpovědnost za práce v oblasti standardizace.

OPTIMUS – Bringing Order to Chaos during MassiveVictim CBRN Incidents

Projekt přijat do výzvy H2020 DRS-2-2014 Crisis management topic 2: Tools for detection, traceability, triage and individual monitoring of victims after a mass CBRN contamination and/or exposure

Projekt směřoval do oblasti ochrany v případech CBRN incidentů. V kontextu přípravy tohoto projektu TPEB navázala spolupráci s Fakultou vojenského zdravotnictví Univerzity obrany, Vojenským výzkumným ústavem, Centrem biologické ochrany Těchonín a Státním ústavem jaderné, chemické a biologické ochrany. Konsorcium vedla řecká odnož britské společnosti EXUS, která má s evropskými projekty velmi bohaté zkušenosti. Cílem projektu bylo vytvořit UAV/UGV technologicko-informační ekosystém, který by efektivně asistovala záchranným složkám v případech CBRN incidentů.

Projektové konsorcium mělo celkem 27 členů, kteří pocházeli z Řecka, Francie, Španělska, Norska. Itálie, Nizozemí, Kypru a České republiky. Početné konsorcium reflektovalo skutečnost, že jeho součástí jsou vývojářské firmy, výzkumné instituce, ale i záchranářské

struktury. Součástí projektu jsou i demonstrační piloty, v rámci kterých měla proběhnout simulace C/B/R/N incidentu a následný zásah profesionálních záchranných složek, které měly být vyškoleny k využití technologie OPTIMUS. V ČR měla proběhnout simulace biologického incidentu v Centru biologické ochrany v Těchoníně, které představuje v této oblasti špičkovou infrastrukturu. Podporu projektu z české strany vyjádřily i Generální ředitelství hasičského záchranného sboru, Fakultní nemocnice v Hradci Králové (spádová fakultní nemocnice pro Těchonín) či město Hradec Králové. Zájem o demonstrační workshop projevila také Evropská obranná agentura, mezi jejíž priority oblast CBRN dlouhodobě patří.

Kromě koordinace českých zástupců měla role TPEB spočívat v exploatační a diseminační roli spojené s iniciativami na úrovni koncových uživatelů, přičemž důraz byl kladen i na workshopy uspořádané v institucích EU a NATO. Podobně jako v předchozím projektu byl využit expertní potenciál UNMZ v oblasti standardizace a certifikace, ke kterému byla připojena expertíza v oblasti vojenských standardů, kterou dodali experti z Úřadu pro obrannou standardizaci, katalogizaci a státní ověřování jakosti.

NOSBAT - Not Only Smart But Also Trusted

Projekt přijat do výzvy H2020-DRS-2015: Critical Infrastructure Protection topic 1: Critical Infrastructure "smart grid" protection and resilience under "smart meters" threats

Projektové konsorcium vedla společnost Atos (Spain). Projektové konsorcium dále zahrnovalo partnery z Itálie, Řecka, Polska, Turecka a Izraele, přičemž izraelské partnery (The Israeli Electric Corporation ((IEC)) a Powercom) zprostředkovala TPEB. Projekt se zaměřuje na bezpečnost smartgridových řešení v energetice a je postaven na konkrétních testovacích případech (Başkent Electricity Distribution Company, Tauron, IEC, CEZ/NESS). Český „used-case" se zaměřuje na souvztažnost smartgridů a kolísajícího napětí elektrické sítě. Kromě zabezpečení tohoto případu TPEB zajišťuje diseminační a exploitační aktivity a má na starosti oblast standardizace. Projekt je v současné době v evaluaci.

RESIXT! - Advanced Resilience Assessment for inter sector Critical Infrastructure Protection

Projekt přijat do výzvy H2020 DRS-14 2015: Critical Infrastructure Protection topic 3: Critical Infrastructure resilience indicator - analysis and development of methods for assessing resilience

Projektové konsorcium vedla španělská společnost INDRA a jeho dalšími členy jsou například A-CING, Canal de Isabel II, AENOR, EXUS, Ramphos Dynamics, NTUA, UNIMORE, ISIG, University of Trento, Immersion, Blue DotCINSIDE, KU Leuven, HKV. Projekt se zaměřuje na indikátory resilience (odolnosti) jednotlivých sektorů kritické infrastruktury. TPEB se v projektu soustředí na sektor energetiky a zároveň zprostředkovala analýzu v sektoru zdravotnictví, když prostřednictvím TPEB do projektu vstoupila i Fakultní nemocnice Hradec Králové. Projekt je v současné době v evaluaci.

PMOPaaS - Production and Manufacturing Open Platform as a Service
Projekt přijat do výzvy H2020 FOF-11-2016: Digital Automation

Projekt se soustředil na zefektivnění managementu kompletních výrobních řetězců. TPEB by v konsorciu, které vede britská společnost EXUS, měla převzít diseminační a exploitační aktivity a dále problematiku standardizace. V současnosti se jedná o vstupu dalších českých partnerů.

ADWICE- Advanced Wireless Technologies for Clever Engineering
Úspěšný projekt v rámci výzvy H2020 WIDESPREAD-2014-1 Teaming (COST)

TPEB podpořila úspěšný projekt ADWICE postavený na spolupráci mezi Centrem SIX při VUT v Brně a Technische Universität Wien. Cílem spolupráce je špičkový mezinárodní výzkum a prohloubení spolupráce mezi vědeckými centry a firmami. Klíčovými oblastmi projektu jsou: Smart sensor systems, Networked signal processing, Smart transport, High mobility communications, Advanced cybersecurity, Advanced antennas and circuits, Awareness in cyber-physical systems.

BehavVer: Video Surveillance of Physical Behavioural Patterns for Prevention of Identity Theft

Projekt směřovaný do výzvy Technologies for prevention, investigation, and mitigation in the context of fight against crime and terrorism

Primárním cílem projektu je vyvinout software BehavVer (název je zkratka pro ověřování behaviorálních vzorů), pro minimalizaci krádeží identity, založený na sledování fyzických modelů chování (tj. jak se člověk obvykle chová), zejména pokud jsou jiné mechanismy kontroly totožnosti útočníkem vyřazeny nebo nepoužitelné. Projekt navrhne novou technologii,

která může být použita ke kontrole fyzické identity oprávněných osob založené na vzorcích chování, které všichni máme jako zaměstnanci, jako například – jak zaparkujeme auto na parkovišti – jak ukážeme náš odznak nebo – jaké dveře obvykle používáme atd. V případě odcizení identity autorizované osoby v strategickém objektu bychom mohli poznat, že se tyto obvyklé vzory změnily a upozorňovaly ostrahu v reálném čase. Na základě rozsáhlé analýzy dat monitorování denních behaviorálních vzorců oprávněných osob bude projekt BehavVer vyvíjet nové technologie, které jsou velmi obtížné potlačit, a to i v kombinaci s dalšími kontrolami totožnosti a vstupu. Tato technologie je v strategických objektech levná a snadno implementovatelná, protože využívá již existující infrastrukturu CCTV kamer, které jsou povinně instalovány na přeplněných místech, ale dosud neúčinně používané.

Participant No	**Participant organization name**	**Acronym**	**Country**
1	Zilinska Univerzita v Ziline	UNIZA	Slovak Republic
2	Software Competence Center Hagenberg GMBH	SCCH	Austria
3	Fraunhofer-Institute for Production Systems and Design Technology (IPK) – Automation Department	FH	Germany
4	Universita Catolica del Sacro Cuore	UCSC	Italy
5	University of Ulster	UU	United Kingdom
6	General Tadeusz Kosciuzsko Military Academy of Land Forces in Wroclaw	MALF	Poland
7	Technology Platform Energy Security	TPEB	Czech Republic
8	ISEMI – International Security and Emergency Management Insititute, n.p.o.	ISEMI	Slovak Republic
9	The Polish Police	LEA1	Poland
10	Municipal Police Zlin	LEA2	Czech Republic
11	Israel National Police	LEA3	Israel
12	Lancashire Constabulary	LEA4	United Kingdom
13	Hampshire Constabulary	LEA5	United Kingdom
14	Sustainable Criminal Justice Solutions	SCJS	United Kingdom
15	Virte, a.s.	VIRTE	Slovakia

PRED-ICT (PRotect Energy Domain Infrastructures from Heterogeneous Cyber-Threats)

Projekt byl přijat v rámci výzvy DS-04-2018-2020: Cybersecurity in the Electrical Power and Energy System (EPES): an armour against cyber and privacy attacks and data breaches

Potenciální role TPEB byla v projektu velmi významná a bude se tak jednat o jedno z největších (plánovaných) zapojení TPEB v rámci projektu H2020. Vzhledem ke své unikátní podobě bude TPEB zodpovědná za WP soustředící se na oblast standardizace a vytváření politik. Dále pak platforma povede piloty zaměřující se na spolupráci operátorů a distributorů v ČR i na Slovensku v oblasti zabezpečení datového přenosu a kybernetické bezpečnosti obecně. V rámci druhé aktivity a také v souvislosti se standardizací a vytvářením politik budce TPEB úzce spolupracovat s dalším českým členem, kterým bude Masarykova univerzita, resp. její Centrum excelence pro kyberkriminalitu, kyberbezpečnost a ochranu kritických informačních infrastruktur, které je napojeno i na kybernetický polygon.

Participant No.	Participant organisation name	Acronym	Country
Technology Providers – Academic Institutions – Security Experts & Consulting Organizations			
1 (Coordinator)	INNOVATION SERVICES, S.A.	INOVA	PT
2	ATOS SPAIN S.A.	ATOS	ES
3	INTRASOFT INTERNATIONAL S.A.	INTRA	LU
4	EXUS SOFTWARE LTD.	EXUS	UK
5	CYBERLENS B.V	CLS	NL
6	NORGES TEKNISK -NATURVITENSKAPELIGE UNIVERSITET	NTNU	NO
7	EULAMBIA ADVANCED TECHNOLOGIES LTD.	EUL	EL
8	CENTRO REGIONALE INFORMATION COMMUNICATION TECHNOLOGY SCRL	CERICT	IT
9	UNIVERSITY OF AEGEAN	UOA	EL
10	GAP ANALYSIS S.A	GAP	EL
11	BUSINESS UPPER AUSTRIA – OÖ WIRTSCHAFTSAGENTUR GmbH	BIZ	AT
12	MASARYK UNIVERSITY	MUNI	CZ
13	GEIE ERCIM EEIG	W3C	FR
End Users (Pilots)			
14	MAGTEL OPERACIONES S.L.U	MAG	ES
15	TPEB	TPEB	CZ
16	GREENFLUX ASSETS BV	GFX	NL
17	INDEPENDENT POWER TRANSMISSION OPERATOR S.A.	IPTO	EL
18	MEAZON ELECTRONICS S.A	MEA	EL
19	PUBLIC POWER CORPORATION S.A.	PPA	EL

CYBER-REACT

Projekt byl přijat do výzvy SU-ICT-01-2018 (Dynamic countering of cyber-attacks) Subtopic: b) Cyber-attacks management – advanced response and recovery

TPEB v projektu měla působit v oblasti standardizační expertízy a v rámci diseminace výstupů v komunitě end-userů a relevantních institucí státní správy.

Participant No	Participant organisation name	Short name	Country
1 (Coordinator)	EXODUS ANONYMOS ETAIREIA PLIROFORIKIS	EXODUS	GR
2	Centro Regionale Information Communication Technology scrl	CeRICT	IT
3	Salzburg Research Forschungsgesellschaft M.B.H.	SRFG	AT
4	FernUniversitat in Hagen	FernUni	DE
5	ITTI SP ZOO	ITTI	PL
6	Factor Social-Consultoria Em Psico-Sociologia E Ambiente LDA	Factor Soc	PT
7	Eulambia Advanced Technologies LTD	EULAMB	GR
8	Krakowski Szpital Specjalistyczny IM. Jana Pawla II	JPII	PL
9	Engineering - Ingegneria Informatica SPA	ENG	IT
10	ETHNIKO DIKTYO EREVNAS TECHNOLOGIAS AE	GRNET	GR
11	Poste Italiane - SOCIETA PER AZIONI	PI	IT
12	Technologická platforma "Energeticka bezpecnost CR"	TPEB CR	CZ
13	Hellenic Telecommunications Organization S.A. - OTE AE	OTE	GR
14	ACTA Ltd	ACTA	GR

EU-CIRP: Practitioners Network

Projekt byl přijat do výzvy Pan European Networks of practitioners and other actors in the field of security

Plánovaný projekt představoval typ projektu CSA (Coordinated Support Action) a TPEB v něm měla hrát roli významného partnera etablovaného v oblasti Ochrany kritické infrastruktury. Projekt usiloval o vytvoření panevropské sítě klíčových aktérů ve specifické oblasti ochrany kritické infrastruktury (OKI). Cílem projektu je zintenzivnit komunikaci a interakci relevantních aktérů prostřednictvím čtyř typů aktivit:

1. Analýza výsledků evropských výzkumných a inovačních projektů v oblasti OKI s cílem zvážit jejich relativní potenciál a posunutí do další fáze průmyslového uplatnění;
2. Identifikace nedostatků v oblasti OKI a společných výzev mezi sektory a aktéry;
3. Zhodnocení se RDI řešení, které by mohly řešit identifikované nedostatky, včetně jejich výhledů do budoucnosti;
4. Indikace standardizačních požadavků a priorit, které by posílily transfer RDI do polohy konkrétních řešení;

Obecný cíl projektu představovala snaha vyvinout aktivní interakci mezi RDI komunitou reprezentovanou akademií, výzkumnými organizacemi a evropským bezpečnostním průmyslem

na jedné straně a operátory a regulátory kritické infrastruktury na straně druhé. Tato interakce by měla přinést efektivnější spolupráci při identifikaci klíčových problémů a následně řešení v oblasti ochrany a odolnosti systémů kritické infrastruktury. Dalším cílem projektu je posílit společnou bezpečnostní kulturu, což umožní účinnější přípravu a potenciální reakci na vážné poškození systémů kritické infrastruktury.

Participant No *	Participant organisation name	Country
1 (Koordinátor)	Center for Security Studies (KEMEA)	GR
2	Croatian Network of Urban Security Stakeholders (CIC)	CR
3	European Organization for Security (EOS)	B
4	European University of Cyprus (EUC)	CY
5	European Hospital and Healthcare Federation (HOPE)	B
6	Ministry of Interior (MoI)	BG
7	Spanish Technology Platform on Industrial Safety & Security (PESI)	ES
8	Scottish Government (Critical Infrastructure Resilience Unit)	UK
9	Technology Platform Energy Security (TPEB)	CZ
10	International Union of Railways (UIC)	F
11	Ente Nazionale Energia Atomica (ENEA)	I
12	Romanian Association for CIP and Related Services (ARPIC)	RO
13	Polícia Judiciária of Portugal (PJ)	PT

SecureGas – Securing the European Gas Network

Projekt financovaný EU za účelem zvýšení bezpečnosti a odolnosti evropské plynárenské sítě vede společnost RINA. Byl podpořen v rámci výzvy SU-INFRA01-2018-2019-2020 „Prevention, detection, response and mitigation of combined physical and cyber threats to critical infrastructure in Europe“.

Evropská plynárenská síť tvoří nedílnou součást energetických potřeb EU, včetně plánů na snížení emisí CO2, které jsou stanoveny v Pařížské dohodě. Již nyní představuje významný podíl v energetickém mixu, který tvoří 22 % spotřeby energie, přičemž lze vzhledem k různým technologickým iniciativám očekávat jeho další nárůst.

Plynárenská síť je svým charakterem složitá a vysoce propojená. Překračuje hranice, využívá nejrůznějších dopravních plynovodů a je obsluhována řadou různých skladovacích zařízení. Tato složitost z ní činí důležitý prvek kritické infrastruktury (CI), která může být narušena

přírodními katastrofami, nehodami, kybernetickými útoky, škodlivým jednáním, trestnou činností nebo terorismem. Jakékoli výpadky nebo nedostatek v dodávkách mohou mít nepříznivý dopad na bezpečnost EU a blahobyt jejích občanů.

Zajištění bezpečnosti a odolnosti tohoto životně důležitého zdroje a jeho infrastruktury má proto mimořádný význam. Vzhledem k propojené povaze infrastruktury a potenciálním kaskádovým efektům však zajištění bezpečnosti vyžaduje komplexní přístup. Plynárenská síť a infrastruktura představují složité systémy, u kterých je třeba zajistit, aby byly zabezpečeny a schopny odolávat jak fyzickým, tak kybernetickým útokům, a jejich kombinaci v kontextu všudypřítomných, řízených a dlouhotrvajících hrozeb.

Co se týče fyzických hrozeb, EGIG (European Gas pipeline Incident data Group) eviduje celkem 1366 incidentů mezi roky 1970 až 2016, přičemž většina incidentů byla způsobena třetími stranami v rámci pozemních prací, nepřátelských aktů či sabotáží. Počet dosud hlášených kybernetických incidentů je menší, nicméně důsledky mohou být podobně zničující. Útoky jako Night Dragon a Shamoon způsobily značné finanční škody ropným a plynárenským společnostem. Podle globálních odhadů náklady na kybernetickou bezpečnost provozovatelů ropy a zemního plynu a elektrické energie činí do roku 2018 1,87 miliardy dolarů.

V této souvislosti, s cílem zajistit bezpečnost a odolnost plynárenské sítě EU, RINA koordinuje zásadní projekt spolupráce EU v oblasti výzkumu a vývoje, SecureGas. V souladu s Evropskou strategií pro energetickou bezpečnost, s Evropským programem na ochranu evropské kritické infrastruktury (EPCIP), se závislostí EU na dovozu plynu a s nařízením EU 2017/1938 o bezpečnosti dodávek zemního plynu, se projekt zaměřuje na 140 000 km evropské plynárenské sítě pokrývající celý řetězec od výroby až po distribuci, poskytování metod, nástrojů a pokynů pro zabezpečení stávajících i nových instalací a jejich odolnosti vůči kybernetickým fyzickým hrozbám.

V průběhu projektu budou definovány návrhy plánování, navržení, vybudování, provozování a udržování kritické plynárenské infrastruktury tak, aby bylo možné se vyrovnat s kybernetickými a fyzickými bezpečnostními hrozbami. Tyto budou sloužit jako základ pro definování referenční vysokoúrovňové architektury (HLRA), která bude sloužit jako vodítko pro adaptaci, přizpůsobení, integraci technologických komponent, které budou nakonec demonstrovány v rámci aplikačních případů. Výsledky poté budou nabízeny jako služby pro bezpečnost a

odolnost plynárenské sítě EU prostřednictvím modelu PaaS (Platform as a Service), který umožňuje modularitu, flexibilitu, spolupráci a interoperabilitu třetích stran.

Projekt se může pochlubit multidisciplinárním konsorciem 21 mezinárodních partnerů. Skládá se z integrované energetické společnosti (ENI S.p.A), plynárenské korporace (Public Gas Corporation of Greece S.A.), TSO – Transmission system operator (provozovatele přenosové soustavy AB Amber Grid) a provozovatele distribuční soustavy DSO – Distribution system operator (Attiki Natural Gas Distribution Company SA), spravující dohromady + 15000 km plynovodů; poskytovatelů technologií působících v oblasti bezpečnosti a kritické infrastruktury (Leonardo S.p.A, Guardtime A.S., Elbit Systems Ltd., WINGS ICT Solutions, IDEMIA Identity & Security Germany AG, EXUS, GAP Analysis S.A., Innov-Acts Ltd. a Disaster Management, Advice and Training Consulting KG), výzkumných a akademických institucí v oblasti energetiky, bezpečnosti a odolnosti (Fraunhofer-Gesellschaft zur Förderung der angewandten Forschung, Kentro Meleton Asfaleias, Joint Research Centre Ispra, Technická univerzita v Rize, Technologická platforma Energetická bezpečnost ČR). Platforma zúčastněných stran (Stakeholder Platforrm), vedená Agenzia per la Promozione della Ricerca Europea, bude poskytovat zázemí k zajištění dlouhodobého šíření výstupů projektu.

Tento projekt je financován z programu výzkumu a inovací programu Horizont 2020 Evropské unie v rámci grantové dohody č. 833017.

OPPI A OPPIK

Energetická a kybernetická bezpečnost
Projekt řešen v letech 2012-2014

TPEB jak příjemce úspěšně vyřešila projekt Energetická a kybernetická bezpečnost, který jí umožnil zásadním způsobem stimulovat aktivity, které by TPEB chtěla prostřednictvím stávající výzvy dále efektivně rozvíjet.

Projekt Energetická a kybernetická bezpečnost úspěšně prošel všemi čtyřmi etapami, ve kterých řešitelský tým dokázal identifikovat klíčové problémy a potřeby ve všech čtyřech technologických sektorech. V první etapě se podařilo aktualizovat strategickou a výzkumnou agendu a upřesnit směřování projektu ve vztahu k dalším etapám, které se zabývaly

standardizací, projektovou aplikací a legislativou. Kromě identifikace projektových a výzkumných témat, která byla následně využita ve třetí etapě, první etapa kontextualizovala celou problematiku s vývojem evropských iniciativ v této oblasti. V této souvislosti bylo zdůrazněno, že i na evropské úrovni lze vysledovat poměrně značnou dynamiku v oblasti ochrany kritické infrastruktury, která bude nadále do značné míry ovlivňovat situaci v ČR.
Druhá etapa projektu se zabývala problematikou standardů, jejichž formování a aplikace představuje významnou problematiku, a to jak z hlediska bezpečnosti, tak i navázaných příležitostí v oblastech výzkumu, vývoje, inovací a stejně tak i samotného byznysu. Procesy standardizace navíc z definice představují interdisciplinární aktivity, což vedlo TPEB i k expanzi její odborné báze. Jako velmi zásadní a do budoucna významné téma se objevila problematika vztahu mezi právní regulací a standardy, kterou lze vnímat z mnoha perspektiv, a která je různým způsobem ošetřována v jiných technologických odvětvích.

Ve třetí etapě činnost řešitelského týmu vyústila v účast hned v několika projektových konsorciích, která usilují o podporu v rámci programu Horizont2020 a zároveň ve stimulaci a formulaci dalších projektových žádostí. V rámci procesu přípravy projektů byly reflektovány závěry z prvních dvou etap týkající se významu evropského kontextu a standardizačních procesů. Ve většině projektů byl vytvořen prostor pro aktivity odborníků z ÚNMZ a Úř OSK SOJ. Zároveň došlo k zásadní expanzi institucí spolupracujících s TPEB, a to jak z akademické a výzkumné, tak i firemní oblasti.

Čtvrtá etapa uzavírající projekt se soustředila na legislativu, nicméně jako nečekaně silné téma se objevila související problematika rámce institucionální spolupráce při zvyšování společenské resilience v této oblasti. Ve čtvrté etapě zároveň pokračovaly projektové aktivity představující jeden z primárních cílů strategické a výzkumné agendy, které přestavují cestu k dlouhodobé udržitelnosti fungování TPEB.

Ochrana kritické infrastruktury
Projekt řešen v letech 2017-2018

Projekt Ochrana kritické infrastruktury TPEB pokračoval v naplňování cílů uvedených ve Strategické výzkumné agendě a Implementačním akčním plánu. Zásadní pozornost byla věnována úspěšné výstavbě projektových konsorcií žádajících o podporu v rámci výzev programu H2020. Vstupem do projektových konsorcií v oblasti výzkumu, vývoje a inovací a

jejich formováním TPEB naplňuje svůj nejvýznamnější dlouhodobý cíl, kterým je propojování výzkumné, vývojové a inovační základny s komerčním sektorem a koncovými uživateli, kteří většinou patří mezi státní instituce. V tomto smyslu činnost TPEB plně naplňuje poslání a charakteristiku public-private-partnership platformy.

Další aktivitu pak představovaly veřejné expertní akce, které směřovaly k agendám ochrany kritické infrastruktury a v neposlední řadě také k podpoře aktivit v programu H2020.

Třetí zásadní aktivita ukotvená ve Strategické a výzkumné agendě a Implementačním akčním plánu se týkala spolupráce s Evropskými technologickými platformami (ETP), které přispěly k vybudování konsorcií výše zmíněných projektů. V rámci projektu Ochrana kritické infrastruktury se TPEB stala součástí 5-ti konsorcií, jejichž projekty byly přijaty do výzev H2020. Svoji aktivitou také TPEB podpořila dalších 6 projektových žádostí, které do výzev programu poslali členové.

BEZPEČNOSTNÍ VÝZKUM MINISTERSTVA VNITRA

RESILIENCE 2015

TPEB je součástí úspěšného projektu Resilience 2015 který byl podpořen v rámci programu Bezpečnostního výzkumu MV. Hlavním cílem projektu je pokročilý výzkum problematiky kritické infrastruktury v oblasti hodnocení souvztažnosti a odolnosti evropsky významných sektorů (a jejich subsystémů), kterými jsou energetika, doprava a informační a komunikační technologie.

Výzkumný tým TPEB je primárně zodpovědný za řešení výše zmíněných témat v oblasti energetické infrastruktury.

Hlavním příjemcem projektu je Univerzita Tomáše Bati, Fakulta aplikované informatiky, kde projekt vede Ing. Martin Hromada, Ph.D., člen Správní rady Technologická platforma „Energetická bezpečnost ČR“. Dalšími partnery projektu jsou Vysoká škola báňská – Technická univerzita Ostrava, Fakulta bezpečnostního inženýrství; Vysoké učení technické v Brně, Fakulta stavební; Ministerstvo obrany – Univerzita obrany, Fakulta vojenského leadershipu; Technická univerzita v Liberci, Fakulta mechatroniky, informatiky a mezioborových studií a Centrum dopravního výzkumu.

CIRFI – Critical Infrastructure Resilience Failure Indicators

Projekt je zaměřen na problematiku indikace narušení resilience subsystémů kritické infrastruktury (KI) vlivem působení vnitřních a vnějších hrozeb. Za tímto účelem byl stanoven hlavní cíl projektu, kterým je determinování indikátorů narušení resilience subsystémů KI (tj. sektorů, subsektorů a prvků) a vyvinutí nástroje na identifikaci těchto indikátorů a posouzení jejich vhodnosti pro konkrétní subsystémy KI.

Při řízení provozu a bezpečnosti prvků KI je v současnosti využívána řada indikátorů. Tyto indikátory však dosud nejsou relevantně identifikovány a využívány pro účely hodnocení resilience infrastruktur. V průběhu výzkumu proto budou determinovány významné indikátory narušení resilience subsystémů u vybraných a úzce provázaných sektorů technické KI (tj. energetika, doprava a informační a komunikační technologie). Tyto indikátory budou determinovány pro všechny úrovně systému KI, kterými jsou elementární, subsektorová, sektorová a systémová. Na každé úrovni pak budou tyto indikátory determinovány v jednotlivých oblastech, ve kterých se mohou vyskytovat vnější i vnitřní hrozby negativně působící na resilienci subsystémů KI. Konkrétně se jedná o oblast politickou, ekonomickou, sociální, technologickou, legislativní a ekologickou.
Výstupem projektu tak bude specializovaná veřejná databáze indikátorů narušení resilience subsystémů KI (S), metodika identifikace vhodných indikátorů ve vztahu k analyzovanému narušení resilience zkoumaných subsystémů KI (Nmet) a online softwarový nástroj CIRFI Tool (R), který bude sloužit k propojení a implementaci obou výše uvedených výsledků řešení projektu pro potřeby praktické aplikace. Vlastníci a provozovatelé prvků KI tak získají k dispozici nástroj, který umožní zapojení indikátorů do procesu strategického plánování infrastruktur a výrazně tak zjednoduší zapojení úvah o budování resilience těchto infastruktur v dlouhodobém horizontu.

ISOLATOR - Detekce vad isolátorů energetických přenosových soustav
Cílem projektu je přispět k odblokování současné situace, kdy na trhu není poptávka po nákladních vozidlech na LNG z důvodu nedostatečně rozvinuté infrastruktury čerpacích stanic. Infrastruktura se nerozvíjí z důvodu chybějících informací astavebně technických předpisů pro výstavbu a provoz. Prosazení stavebních předpisů tak vytvoří základní impuls pro urychlení rozvoje a vytvoření nabídky, která povede k rozšíření LNG v nákladní přepravě i jinde. Proces bude také znamenat významný příspěvek pro naplnění směrnice Evropského
parlamentu 22/2014 o zavádění infrastruktury pro alternativní paliva. Stanoveného cíle bude dosaženo realizací navazujících etap: sestavení monografie (06/2019), uspořádání odborné

konference (05/2020), návrh příslušné ČSN (12/2020) a certifikace metodiky (08/2021).

TECHNOLOGICKÁ AGENTURA ČR

Projektování a bezpečné provozování LNG čerpacích stanic

Cílem projektu je přispět k odblokování současné situace, kdy na trhu není poptávka po nákladních vozidlech na LNG z důvodu nedostatečně rozvinuté infrastruktury čerpacích stanic. Infrastruktura se nerozvíjí z důvodu chybějících informací astavebně technických předpisů pro výstavbu a provoz. Prosazení stavebních předpisů tak vytvoří základní impuls pro urychlení rozvoje a vytvoření nabídky, která povede k rozšíření LNG v nákladní přepravě i jinde. Proces bude také znamenat významný příspěvek pro naplnění směrnice Evropského parlamentu 22/2014 o zavádění infrastruktury pro alternativní paliva. Stanoveného cíle bude dosaženo realizací navazujících etap: sestavení monografie (06/2019), uspořádání odborné konference (05/2020), návrh příslušné ČSN (12/2020) a certifikace metodiky (08/2021).

Oblasti výzkumu a vývoje

V rámci SVA je řešena široce pojímaná oblast ochrany kritické infrastruktury. Pro potřeby tohoto dokumentu bude níže rozpracována problematika resilience a souvztažnosti prvků kritické infrastruktury a související oblasti komunikačních technologií, kybernetické bezpečnosti a fyzické bezpečnosti, které představují klíčové agendy náplně projektových konsorcií.

Stimulace, koordinace a zapojování členské základny a dalších subjektů z vnějšího prostředí do projektů výzkumu a vývoje představuje nejvýznamnější aktivitu TPEB, přičemž důraz je v této souvislosti kladen na propojování schopností a potřeb firemní a výzkumné sféry reflektující strategické potřeby a zájmy infrastrukturních společností a orgánů státní správy. V návaznosti na vytvoření domácí a mezinárodní inovačně-kooperativní sítě TPEB úspěšně vyřešila projekt Energetická a kybernetická bezpečnost financovaný z programu OPPI, v současnosti jako člen konsorcia řeší projekt Resilience 2015 podpořený v rámci programu Bezpečnostního výzkumu MV a vstoupila do celkem 5 projektových konsorcií usilujících o projekty v rámci programu H2020.

VaVaI činnost TPEB je do značné míry ovlivňována konkrétními projektovými výzvami v národních a především nadnárodních programech. Níže uvedené oblasti naznačují inovačně-technologické směry v široce definované oblasti ochrany kritické infrastruktury, které TPEB vnímá jako progresivní ve vztahu ke společenským výzvám a přeneseně také očekávaným projektovým výzvám.

Resilience a souvztažnost subsystémů kritické infrastruktury

Problematika vzájemné závislosti v oblasti kritické infrastruktury je zejména v posledních letech dynamicky se rozvíjející oblastí. Tento dynamický rozvoj přispěl k vymezení rozličných druhů vazeb v systému kritické infrastruktury, obecných způsobů šíření nefunkčnosti, charakteru selhání a chování jednotlivých prvků systému. V posledních letech jsou pak patrné snahy o modelování systémů kritických infrastruktur. Takovýto systém se skládá z jednotlivých sektorů, příslušných prvků a vazeb nejen mezi prvky v sektoru, ale i napříč sektory. Každý prvek systému má pak určitý vliv na jiný prvek nebo společnost, která je na jeho funkci do určité míry závislá (zranitelná). Při narušení funkce jakéhokoli prvku systému pak dochází k negativním dopadům nejen v rámci samotnému systému, ale i dopadům mající vliv na

bezpečnost společnosti obecně, potažmo celou společnost. Míra těchto dopadů pak úzce souvisí s mírou kritičnosti jednotlivých prvků, které se v systému nacházejí a vykazují tak požadavek na zajištění ochrany a bezpečnosti.

V odborné literatuře se můžeme čím dál tím častěji setkat s mnoha přístupy používanými k modelování vzájemných závislostí v systému kritické infrastruktury a simulaci šíření následků nefunkčnosti jednoho či více prvků v takovém systému. Jedná se o přístupy založené na metodách a simulaci vycházející z různých principů, jakými jsou např. Markovovy procesy, Petriho sítě, metoda Monte Carlo, Leontiefův vstupně-výstupní model, diferenciální rovnice a dynamické simulace. Mnoho autorů se také zaměřuje na modely založené na agregované poptávce a nabídce prvků v rámci systému infrastruktur, agentních modelech atd. Všechny tyto přístupy na různém principu simulují, modelují, popř. vyhodnocují nebo oceňují chování vzájemně více či méně propojených prvků infrastruktur a jejich reakci na různá selhání, či narušení jejich funkce. Cílem těchto přístupů je vytvořit systém hodnocení dopadů způsobených prostřednictvím vzájemné provázanosti mezi a napříč prvky kritické infrastruktury a identifikovat kritické prvky systému. Provedením těchto simulací, lze následně efektivněji realizovat opatření směrem k zabránění šíření těchto nefunkčností napříč systémem a tím docílit komplexního zvýšení odolnosti posuzovaného systému a v konečném důsledku i společnosti.
Snaha o modelování a simulaci komplexních systémů v oblasti kritické infrastruktury začíná být v poslední době patrná i v rámci Evropské unie. Tato snaha je zřejmá zejména z uvědomění si značné provázanosti jednotlivých prvků kritické infrastruktury jak v rámci jednoho sektoru (např. energetice, informačních a komunikačních technologiích nebo dopravě), tak i v mezisektorové rovině (tj. např. mezi energetikou, informačními a telekomunikačními systémy a dopravou). Tato signifikantní provázanost daná vazbami mezi jednotlivými prvky jak v rámci jednotlivých sektorů tak i napříč mezi nimi, umožňuje prostřednictvím vazeb šíření dopadu poruchy jednoho prvku napříč celým systémem. To v konečném důsledku znamená, že při poruše prvku v jednom sektoru může dojít vlivem vazeb k narušení prvku v sektoru jiném. Takováto kaskádní selhání vedou ke zvyšování dopadu na společnost s následným projevem v oblasti ekonomických a bezpečnostních hodnot.

V České republice byla kritické infrastruktuře v posledních letech věnována velká pozornost. Tato pozornost však brala v úvahu vždy jen jeden sektor a to jak z pohledu dopadů na společnost, residenci nebo určování kritických prvků. Dopadům vykazujících provázanosti v mezisektorové rovině však doposud pozornost věnována nebyla vůbec, a to i přes skutečnost, že

právě vazby nejen mezi prvky jednoho sektoru, ale zejména v mezisektorové rovině, mohou způsobovat významný negativní dopad. V současné době, v souladu se současným stavem poznání a technologickými možnostmi, je nezbytné se zabývat i vazbami a dopady v mezisektorové rovině a posuzovat systém kritické infrastruktury jako komplexní systém.

Výhledové směry VaVaI

Základním způsobem komplexního zkoumání vazeb a dopadů v rámci KI je systémový přístup tzn., že k dané problematice je nutné přistupovat jako k systému systémů, tedy k systému s vysokou mírou komplexity. To znamená, že KI jako komplexní systém tvořený základními subsystémy (tj. sektory, odvětvími a prvky), které mají mezi sebou specifické typy vazeb od jednoduchých (vliv a závislost) až po složité (vzájemná závislost).

Počáteční výzkum dopadů KI byl v Evropě veden formou tzv. sektorového přístupu, který nahlíží na jednotlivé sektory KI jako na samostatné celky. Tento způsob výzkumu jednotlivých subsystémů je realizován hloubkově a ohraničeně bez respektování mezisektorových vazeb ovlivňujících chování celého systému. Postupem času byly zjištěny značně limitované možnosti tohoto přístupu, a proto od roku 2013 začíná Evropská unie po vzoru USA a Kanady prosazovat tzv. systémový přístup spočívající v mezisektorovém hodnocení založeném na zkoumání vzájemných vazeb jednotlivých sektorů KI. Na základě toho je nutné konstatovat, že ambicí výzkumného záměru je tudíž systémový přístup. Zmiňované systémové řešení bude v rámci realizace projektu aplikováno progresivním přístupem „bottom-up“, který je založen na hodnocení KI od nejnižší úrovně (obec) směrem nahoru a v současné době je již realizován v některých vyspělých zemích (např. Švýcarsko či Nizozemsko).

Stanovení souvztažnosti vybraných sektorů KI umožní identifkovat a stanovit faktory, které mají zásadní vliv na zajištění minimální dostupnosti funkcí v rámci specifikovaných subsystémů KI. Na základě určení statických a dynamických atributů bude posléze možné analyzovat a modelovat vliv vzájemných závislostí (interdependencies) s cílem zvýšení dostupnosti a odolnosti dodávky vybraných funkcí. Tyto poznatky budou znalostním základem pro výzkum vlivu a dopadů synergického jevu a domino efektu na dynamické hodnocení souvztažnosti a odolnosti (resilience) KI.

Na základě formulace znalostního základu synergického efektu a jeho vlivu na dynamické hodnocení souvztažnosti, dopadů a následně i odolnosti a dostupnosti vybraných funkcí je z pohledu dynamického hodnocení možné definovat koeficient souvztažnosti vyjadřující závislost (fyzickou, územní, informační, logickou a společenskou) a vazby mezi jednotlivými subsystémy KI. Taková analýza vychází a rozšiřuje problematiku a proces statického hodnocení odolnosti KI.

Vymezení atributů dynamického hodnocení úrovně synergického efektu lze také vnímat i z pohledu dynamického hodnocení dalšího atributu metodiky, a to koeficientu rizikovosti vyjadřujícího pravděpodobnost dopadu hrozby na funkčnost KI, což je možné vnímat i z perspektivy hodnocení zranitelnosti KI. Pravděpodobnost dopadu hrozby je třeba pro účely dynamického modelování kvantifikovat. V tomto ohledu lze pro hrozby stanovit vhodné ukazatele pravděpodobnosti jejich výskytu a následků. K těmto ukazatelům lze vztáhnout rozsah jejich možných hodnot a souvisejících nejistot.

V další fázi zkoumání bude možné stanovit dynamické atributy pro hodnocení robustnosti, a to z pohledu strukturální robustnosti, vyjadřující schopnost KI ustát působení negativních vlivů ve vztahu k jeho struktuře, systémovým a technologickým vlastnostem a z pohledu robustnosti zabezpečení, která vyjadřuje stav a úroveň bezpečnostních opatření zajišťujících efektivní minimalizaci působení rizik. Pro koeficient strukturální odolnosti budou popsány dynamické atributy ve vztahu k typu topologické struktury KI, její složitosti, počtu klíčových technologií, flexibilitě, možnosti redundance a dalších ukazatelů. Koeficient robustnosti zabezpečení bude následně dynamicky hodnocen z pohledu vybraných aspektů bezpečnosti a zabezpečení, a to i v kontextu měnících se vah (významnosti) těchto aspektů. Dalším významným aspektem výzkumu dynamického hodnocení odolnosti souvztažných subsystému KI je koeficient připravenosti, který zohledňuje schopnost reakce, odezvy a obnovy funkce KI.

Naplnění všech skutečností následně umožní dynamické hodnocení odolnosti KI v rámci vymezeného území, jehož výstupem bude stanovení dopadů. Dalším přínosem bude objektivní výběr preventivných opatření k minimalizaci dopadu hrozeb pro zvolené oblasti KI, a to v oblasti bezpečnosti (safety), v oblasti zabezpečení (security) a oblasti připravenosti (preparedness).

Na základě dynamického hodnocení a modelování KI prostřednictvím vhodné informační podpory je možné následně upravit postup určování a seznam prvků pozemní (silniční a

železniční) dopravní KI. Výhodou dynamického hodnocení odolnosti bude v této souvislosti v závislosti na čase i možná detekce těch negativních faktorů, které mají zásadní vliv na funkčnost KI na vymezeném území. Výsledky podobných analýz mohou být například základem pro optimalizaci plánovacího procesu ve vztahu k postupům a opatřením při řešení vybraných krizových situací a tím i plány krizové připravenosti subjektů KI. Současně podobné výzkumy mohou podpořit vytvoření a zavedení systémů, které umožní hodnotit v čase úroveň souvztažnosti a tím i integrální odolnosti. Tím se významně rozšíří a doplní aktuální stav poznání a možností statického hodnocení odolnosti ve prospěch dynamického hodnocení odolnosti KI v čase.

Komunikační technologie v oblasti kritické infrastruktury

Komunikační technologie jsou typickou oblastí s dynamickým rozvojem, kde se ve velmi krátkých časových intervalech objevují nová řešení a služby. Objevy nových materiálových možností zejména v nano a mikroelektronice způsobují vývoj nových komponent, produktů a služeb. Změny probíhají tak rychle, že odhadnout technologie a jejich vlastnosti používané v horizontu deseti a více let je téměř nemožné. V současné době se všeobecně zaměřují vývojové trendy v komunikačních technologiích na zkvalitnění přenosu informací v digitální podobě:

- Zvýšení kapacity a přenosové rychlosti
- Zjednodušení architektury komunikačních systémů, tj. minimalizace HW komponent s možností změny jejich vlastností použitím rozdílného SW vybavení (SDR – Software Define Radio)
- Standardizace jednotlivých rozhraní, a to jak z hlediska HW komponent, tak i vzhledem k jednotnému formátu distribuovaných dat

Rozvoj komunikačních technologií a nárůst přenášených informací se projevuje ve všech směrech. Zasáhl jak oblast komunikace (převážně hlasové) využívané především složkami IZS, tak i oblast datových přenosů v rámci zavádění SMART technologií v energetice. Komunikační systémy využívané složkami Integrovaného záchranného systému jsou nedílnou součástí zajištění ochrany prvků kritické infrastruktury.

V uplynulých několika letech došlo ve světě k několika mimořádným přírodním katastrofám, v průběhu kterých se projevila technologická vyspělost použitého záchranného systému. Dnes

již můžeme srovnat následky ničivých vln tsunami v Malajsii a Japonsku, které způsobily rozsáhlé škody na majetku i na životech. V Japonsku se díky vyspělým komunikačním technologiím (zejména za využití mobilních operátorů) podařilo organizovat evakuační a následně i záchranné práce mnohem úspěšněji. Přesto po výpadku proudu v jednotlivých oblastech se objevila kritika týkající se včasné informovanosti obyvatelstva v postižených oblastech.

V ČR se v posledních letech stále častěji setkáváme se stejným problémem v důsledku povodní. Sítě mobilních operátorů pokud nepřestanou fungovat úplně, jsou často přetížené a výsledek je vždy stejný. Včasná informovanost obyvatelstva je velmi omezena a v případě výpadků elektrické energie nelze ani použít klasické TV a rádio přijímače.

V oblasti datových přenosů dochází k propojení koncových účastníků energetických sítí s dodavateli cestou páteřních sítí

Připojení koncových uživatelů

Pro připojení koncových uživatelů lze obecně využít systémů bezdrátových, metalických a optických.

Metalické a optické systémy se využívají pro kritické části infrastruktury, ve srovnání s bezdrátovými systémy mají zpravidla vyšší spolehlivost a dosahují vyšších přenosových rychlostí. Typickým představitelem metalické sítě je v Ethernet standardu 100Base-TX a 1000Base-T. Systémy metalické s vyššími přenosovými rychlostmi a optické linky bývají nasazovány na páteřních spojích.

Současné bezdrátové systémy lze rozdělit na úzkopásmové a širokopásmové. Úzkopásmové dosahují nízkých komunikačních rychlostí, využívají se zejména pro přenos telemetrie, měřených dat a povelů. Mezi základní požadavky úzkopásmových komunikačních systémů patří vysoká odolnost a spolehlivost přenosu, v řadě aplikací pak také energetická nenáročnost. Komunikační rychlost zde není zásadním parametrem.

Úzkopásmové systémy používané v domácnostech komunikují zpravidla ve volných kmitočtových pásmech, přidělených generálním povolením ČTÚ. Nejpoužívanější pásmo 433 MHz je v současné době již extrémně zaplněno množstvím zařízení, jako jsou bezdrátové teploměry, dálkově řízené hračky, meteostanice apod. Vzhledem k rušení je nasazování nových zařízení problematické. Lepší situace je v pásmu 868 MHz, do kterého se přesouvá většina

důležitějších aplikací, např. termostaty, komunikace s vodoměry a měřiči tepla apod. Pro profesionální telemetrické aplikace, např. monitorování a řízení místních vodáren, se používají přenosy na licencovaných kmitočtových pásmech. Tato pásma mají zajištěnou zákonnou ochranu proti rušení, pokud ale není rádiová linka zálohovaná jiným systémem, nemůže být zcela odolná proti úmyslnému rušení a útokům.

Samostatnou kapitolou je úzkopásmové připojení mobilních stanic a terminálů. Kromě systémů používaných mobilními operátory, které jsou implementovány v GSM a 3G sítích, existuje v ČR několik neveřejných sítí. Tou nejrozsáhlejší je digitální převaděčová síť integrovaného záchranného systému MATRA – Pegas. Řada dalších převáděčových systémů zejména ve větších městech je pak využívána dopravními podniky, městskou policií i komerčními zákazníky. Všechny převaděčové systémy pracují v licencovaných pásmech.

Širokopásmové systémy zpravidla kladou důraz na přenosovou rychlost, pohybující se od stovek kilobitů do stovek megabitů za sekundu. Patří mezi ně i systémy s rozprostřeným spektrem, používané zejména pro svou bezpečnost a odolnost proti rušení. Nejznámějším systémem současnosti je WiFi, tj. standardy 802.11b/g/n pro bez licenční pásmo 2,4 GHz a 802.11a/n pro 5 GHz. Systémy WiFi umožňují různé metody zabezpečení – od zcela otevřených systémů přes symetrické šifrování WEP klíčem (nyní již snadno prolomitelným) po WPA2 s AES šifrou. Původní nasazení systémů WiFi cílilo na vnitřní sítě, tj. pokrytí bytu nebo domu. Současné časté nasazení ve vnějším prostředí je nevhodné, navíc pásmo 2,4 GHz je výrazně přeplněné, což se projevuje nízkou kvalitou WiFi spojů. Jako doplněk k systémům WiFi vznikl standard WiMAX, zaměřený právě na venkovní sítě. Rozšíření tohoto systému je ale v ČR zatím poměrně nízké, zejména kvůli vyšším pořizovacím nákladům ve srovnání se systémy WiFi.

Zvláštní kapitolou jsou komunikační systémy, které využívají jako přenosového média elektrickou síť, nazývané souhrnně Power Line Communication (PLC). Jejich rozšíření mezi uživateli v ČR je poměrně nízké, tvoří však zásadní prvek infrastruktury pro chytré domy a chytré distribuční sítě, protože je jimi často realizován tzv. úsek poslední míle. Jednou z překážek většího rozšíření těchto systémů je standardizace, řada výrobců má svá proprietální, navzájem nekompatibilní řešení. Při návrhu sítě je třeba věnovat pozornost množstvím omezení – pro vícefázové systémy je třeba instalovat vysokofrekvenční přemostění, signál neprojde přes neupravený distribuční transformátor apod.

PLC sítě dělíme podle pracovního kmitočtového pásma na tři základní systémy. Zařízení

pracující v pásmu do 500 kHz s vysílacím výkonem až stovek wattů se používají zejména pro pomalou komunikaci na velkou vzdálenost, např. po distribučních linkách vysokého napětí. Pro domácí využití se v tomto pásmu rozšířily zejména systémy LonWorks a Universal Powerline Bus. PLC v kmitočtovém pásmu nad 1 MHz lze již používat pro širokopásmový přenos, nejrozšířenějšími jsou zde systémy HomePlug a Broadband over Power Lines. Problémem je rušení jiných služeb, zejména radioamatérských pásem v oblasti 10-30 MHz, protože elektrická síť funguje jako rozlehlá drátová anténa. Výzkum se v současnosti zaměřuje také na PLC komunikaci v pásmu UHF (nad 100 MHz). Je možné využít extrémně širokopásmové systémy pro vysoké přenosové rychlosti na krátké vzdálenosti.

Domácí sítě

Domácí sítě jsou komunikační sítě, pokrývající oblast jednoho bytu nebo domu. Kromě dnes již běžné lokální datové sítě, založené zpravidla na některém ze standardů Ethernetu, se můžeme setkat s řadou systémů, využívaných pro tzv. domácí automatizaci, tj. realizaci koncepce chytrého domu. Ta zabezpečuje především automatiku pro vytápění, ventilaci a klimatizaci, řízení osvětlení, audiovizuální a zabezpečovací techniky, interkomy. Důležitým prvkem je také automatický sběr dat z různých měřičů – kromě elektroměru je dům obvykle vybaven vodoměry, plynoměrem, měřidlem odebraného tepla atd.

Sítě lze opět rozdělit, v tomto případě především na bezdrátové a metalické. Instalace metalických sítí musí být projektována při stavbě nebo rekonstrukci domu, sítě domácí automatizace mají totiž zpravidla celou řadu koncových bodů, které prakticky znemožňují dodatečnou instalaci. Mezi nejrozšířenější sítě patří již zmíněný Ethernet a dále zejména protokoly, postavené na průmyslových diferenčních sběrnicích, jako je např. RS485/ModBus, OpenTherm nebo M-BUS.

Bezdrátové technologie pro pokrytí malého území bytu nebo domu zpravidla spadají do bez licenčních pásem, uvolněných na základě generálního povolení. Kromě již popsané technologie WiFi a spíše výjimečného nasazení BlueTooth jsou využívány zejména systémy ZigBee a proprietární úzko pásmová komunikace v ISM pásmech (433 MHz, 868 MHz a 2,4 GHz). Výhodou posledních dvou jmenovaných technologií je možnost dosáhnutí velmi úsporného provozu, který je v těchto případech kritický – řada koncových zařízení je bateriově napájena.

Výhledové směry VaVaI

Výše uvedené systémy a technologie jsou v současné době již zralé a široce nasazované v nejrůznějších realizacích. Aplikovaný výzkum v těchto oblastech je věnován zejména otázkám zlepšení základních parametrů těchto technologií, jako je jejich spolehlivost, bezpečnost a efektivita. U standardizovaných systémů se lze navíc pohybovat pouze v oblasti vytyčené a definované daným standardem, aby byla zajištěna vzájemná spolupráce různých zařízení.

Z hardwarového hlediska je kladen důraz na snižování ceny systému. Toho lze docílit především vyšší integrací, kdy je značná část analogového zpracování signálu a veškeré digitální často integrováno na jediném čipu. Takové řešení plní zpravidla i další zásadní cíl, kterým je snižování energetické náročnosti daného obvodu. Řada aplikací je bateriově napájená a např. u systémů pro sběr dat je často požadována jejich životnost v řádu jednotek let.

Limitním případem přístupu ke snižování spotřeby je realizace systémů napájených sběrem energie z okolního prostředí – zejména energie rádiového pole, často ale i solární energie či využití piezoelektrického jevu. Mezi komunikační systémy napájené pouze energií vysílače patří pasivní tagy pro radiofrekvenční identifikaci (RFID). Prosazují se také komunikační systémy s extrémní šířkou pásma – ultra-wideband (UWB). Ty kromě efektivity a odolnosti proti rušení umožňují další zajímavé funkce, jako je přesná prostorová lokalizace vysílače s přesností až jednotek centimetrů. S vysokou integrací moderních systémů souvisí také návrh miniaturních či adaptivních antén na speciálních substrátech.

Softwarové hledisko je v současnosti čím dál více zaměřeno na problematiku zabezpečení a standardizace komunikace. Zabezpečení je řešeno symetrickým a asymetrickým šifrováním, vývoj v této oblasti je značný – teprve v nedávné době se například staly běžně dostupnými mikrokontroléry s integrovaným kryptografickým koprocesorem, který efektivně zajišťuje výpočetně vysoce náročné šifrovací operace. Zatímco šifrování v odborné veřejnosti snadno přístupných systémech osobních počítačů je poměrně známou záležitostí, v oblasti mikroprocesorové techniky a embedded systémů výrobci často spoléhají na uzavřenost systému a utajení firmwaru, v čemž lze spatřovat značné bezpečnostní riziko – analýzou jediného zařízení je pak možné získat přístup k interním údajům všech dalších zařízení stejného typu.

Dostupnost mikrokontrolérů s vysokým výkonem umožňuje dále snižovat energetickou náročnost komunikačních zařízení. Výkonné 32 - bitové mikrokontroléry sice zpravidla mají v aktivním režimu mírně vyšší spotřebu než starší typy, operace ale provádí řádově rychleji a ušetřený výpočetní čas mohou trávit v úsporných režimech – spánku. Tím je možné docílit

výrazného snížení průměrné spotřeby při zachování nebo zvýšení dostupného výpočetního výkonu.

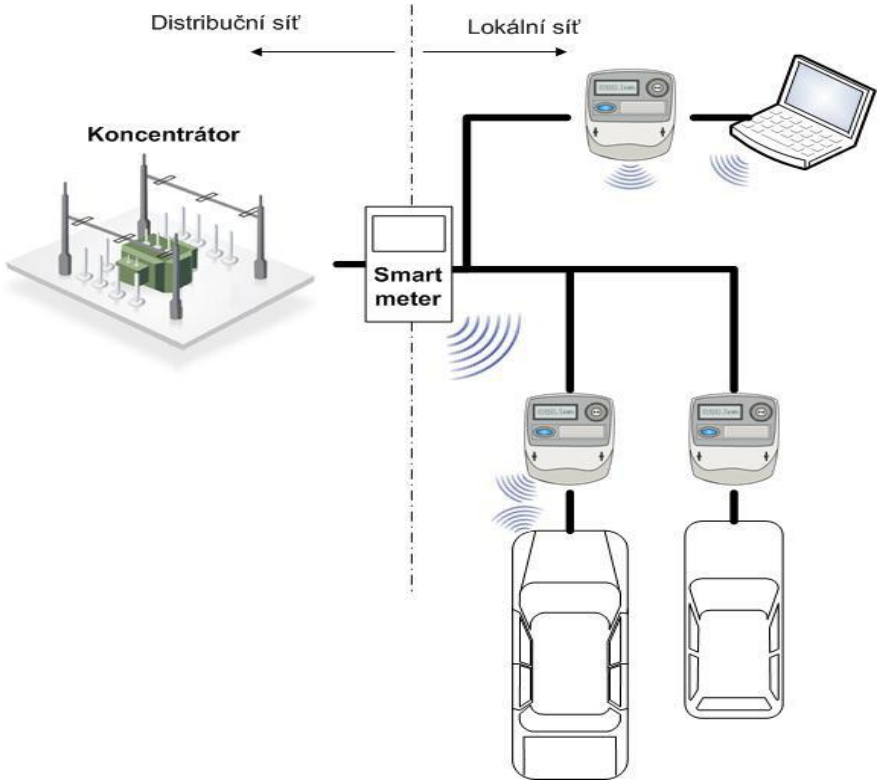
Standardizace v oblasti komunikace směřuje u komplexnějších sítí k nasazení IP protokolu. Aktuální situace s nedostatkem IPv4 adres je řešena přechodem na IPv6, který je již velmi dobře podporován v páteřních a akademických sítích, stejně jako u komerčních serverů. Jeho implementace v koncových uživatelských zařízeních je ale zatím málo rozšířená, stejně jako všeobecné znalosti uživatelů o možnostech zabezpečení IPv6 komunikace.

SMART technologie a jejich zabezpečení

Problematika Smart grids těsně navazuje na oblast Smart home (chytrá domácnost). Výzkum a vývoj v oblasti Smart home se primárně soustředí na koncepty komunikace mezi jednotlivými spotřebiči v domácnosti a na uživatelská rozhraní, přičemž rozhraní k energetické síti tvoří jeden (nebo jen několik málo) bodů. Tyto body jsou vybavené smart meterem (chytrým elektroměrem).

Nutná je identifikace skupin spotřebičů vůči smart meteru z hlediska možnosti dálkového vypínání či zapínání spotřebičů. Jedná se o další rozvoj již používané funkce HDO (Hromadné Dálkové Ovládání), která se dnes používá typicky pro ohřev teplé vody v bojlerech. Dále se rozvíjí oblast smart spotřebičů (logo SG ready), které jsou schopny řídit svůj chod v závislosti na aktuálním tarifu, který se dozvídají právě ze smart-meteru. Tedy např. pračka se zapíná v době, kdy je elektřina levnější. Tato možnost vzdáleně ovládat spotřebiče je důležitá i z hlediska možnosti ostrovního provozu v mimořádných situacích, kdy umožní dálkově snižovat odběr nevýznamných skupin spotřebičů.

S očekávaným nárůstem spotřeby zejména elektrické energie u mobilních odběratelů (např. elektromobily) je potřeba řešit i otázku identifikace těchto odběratelů za účelem řízení distribuce energie tak, aby byla nejen optimalizována vytíženost sítě, předešlo se kolapsům (částí) energetické sítě kvůli dynamicky se měnící zátěži, ale aby byla i zajištěna bezpečnost přenosu informace o uživateli mezi spotřebičem a smart meterem. Podobně jako v oblasti telekomunikací se i v oblasti energetiky očekává vznik nových právních subjektů, obchodníků s energií.



Obr. 1 Napojení lokální sítě

V oblasti energetické bezpečnosti v návaznosti na lokální sítě odběrných míst pro mobilní odběratele je potřeba vyřešit:

- Návaznost existujících technologii pro identifikaci uživatelů na odběrné místo (rozhraní k primárnímu smart meteru)
- Bezpečnost komunikace při identifikaci (zamezeni zneužití/krádeže identity)
- Fyzické možnosti identifikace uživatelů
- Nezávislost komunikace na přístupovém mediu
- Komunikace mezi smart meterem a spotřebičem
- Zabezpečení komunikačního kanálu

Komunikační technologie pro složky IZS

Z hlediska komunikačních technologií lze pro účely této SVA rozdělit potřeby IZS na následující technologické oblasti:

- Komunikace mezi členy záchranných týmů navzájem
- Komunikace mezi členy záchranných týmů a obyvatelstvem v postižených oblastech

- Zajištění dostatečného množství elektrické energie pro provoz výše uvedených komunikačních systémů v případě blackoutu.

Komunikace mezi členy záchranných týmů navzájem se vyznačuje zaváděním nejmodernějších komunikačních technologií za využití autonomních komunikačních sítí s omezeným počtem účastníků.

Naproti tomu komunikace mezi členy záchranných týmů a obyvatelstvem v postižených oblastech představuje problematiku zajištění plošného šíření informací v přesně definovaných oblastech. Pro tyto účely je vhodnější využití masově rozšířených technologií s bateriovým napájením, než zavádění nejmodernějších technologií, které nejsou dostatečně zastoupeny ve vybavení domácností. Perspektivně se jeví vývoj v oblasti mobilních, energeticky autonomních komunikačních center umožňujících příjem informací dostatečně rozšířenými technologiemi.

Z hlediska zajištění dodávek potřebného množství elektrické energie lze předpokládat uplatnění nových technologií pro:

- Optimalizaci spotřeby komunikačních systémů
- Návrhy ostrovních systémů schopných udržet dodávky elektrické energie v postižených oblastech (buď v plném rozsahu, nebo v omezeném rozsahu s využitím inteligentního řízení spotřeby)
- Vývoj nových energetických zdrojů a zásobníků pro lokální použití

Kybernetická bezpečnost v oblasti ochrany kritické infrastruktury

Význam kybernetické bezpečnosti zásadně roste, což je to způsobeno především následujícími skutečnostmi:

- Významný nárůst objemu zpracovávaných a uchovávaných dat. Předpokládá se, že v období 2009 – 2020 dojde k nárůstu asi 44x. Tím se enormně zvýší nároky na kapacitu a bezpečnost úložišť
- Přesun většiny nebo všech aktivit subjektů provozujících prvky KI do kyberprostoru (aktivity řídící, transakční, komunikační, obchodní, PR atd.)
- Totální závislost subjektů KI na řídicích systémech založených na ICT

Vzhledem k těmto skutečnostem bude nezbytné vytvoření národního systému a jeho zapojení do mezinárodního systému informovanosti o hrozbách a zranitelnostech v rámci KI.

Technologie, které se dnes jeví jako perspektivní, jsou následující:

- Monitorování datového provozu z rozsáhlých IP sítí s důrazem na detekci útoků, anomálií, bezpečnostních incidentů, pokusů o průnik do systému atd.
- Bezpečnost dat a ochrana soukromí monitorovaných osob
- Kryptografie
- Real-time získávání informací a jejich real-time analýza

Výhledové směry VaVaI

Z hlediska bezpečného přístupu k datům pro jednotlivé účastníky je nutné problematiku řešit komplexně jak na úrovni technologické, tak na úrovni poskytovaných služeb (Service Oriented Architecture, SOA) datovou centrálou. Zejména problematika poskytovaných služeb není dosud uspokojivě řešena a je reálnou překážkou pro přijetí koncepce SG významnými hráči na trhu.

Centrální databáze SG bude obsahovat cenná data, které jsou velmi riziková pro jednotlivé provozovatele. Pouze zcela transparentní bezpečnostní mechanismy mohou významné aktéry přesvědčit o bezpečí jejich dat ve SG.

- Stanovení technických a procesních opatření s cílem minimalizovat dopady síťových útoků (Distributed Denial of Service) na klíčové body ICT infrastruktury.
- Analýza „metody pohyblivého cíle“. V takovém případě se klíčový počítač (server) v síti pohybuje, při zachování plné funkčnosti. Za takovéto situace je velmi obtížné vést útok, neboť se cíl může nacházet jinde, než zjistil předběžný průzkum útočníka.
- Vývoj metod, které budou schopny zaručit bezpečnost i za situace, kdy již došlo k narušení bezpečnostních pravidel. Např. budou-li počítače v chráněné síti infikovány malwarem, zamezit jim v komunikaci s řídícími stránkami, které bývají uvedeny na blacklistech.
- Rozvoj spolupráce s národním CERT (Computer Emergency Response Team) a CSIRT (Computer Security Incident Response Team) za účelem lepší koordinace při řešení bezpečnostních incidentů v počítačových sítích provozovaných v České

republice). Sdílení informací o aktuálních hrozbách a způsobech ochrany.

- Rozvoj koncepce spolupráce v oblasti ochrany ICT infrastruktury mezi veřejným a soukromým sektorem, neboť řada prvků kritické infrastruktury je ve vlastnictví soukromých společností. Jedním z cílů této spolupráce by mělo být stanovení jednotných bezpečnostních standardů, tak aby mohla probíhat bezpečná výměna dat mezi veřejným a soukromým sektorem.

Fyzická bezpečnost v oblasti ochrany kritické infrastruktury

Dynamický rozvoj v oblastech senzorů, čidel, informačních a komunikačních technologiích výrazně ovlivnil možnosti nových zabezpečovacích systémů zajišťujících fyzickou bezpečnost. Současně s neustále rostoucími kapacitními možnostmi řídících center dochází ke strukturálním změnám při návrhu jednotlivých systémů. Důraz je kladen na integraci s ostatními systémy řízení a organizaci provozu. Je to způsobeno tedy jednak technologickými možnostmi, ale tlak na integraci souvisí také s finanční stránkou, kdy dochází k propojení a návaznosti na další systémy v rámci optimalizace procesů a vyplývající ekonomické návratnosti takovýchto investic.

Vývojové trendy naznačují následující možnosti:

- Vytvoření nového technologického celku, který zvýší účinnost technologií nebo doplní jejich funkce.
- Rozvoj perimetrických poplachových systémů umožňujících:
  - obrazovou verifikaci;
  - preventivní funkce;
  - identifikaci potencionálního vznikajícího rizika už na samotném obvodu perimetru zájmových oblastí;
  - vytvoření podstatně lepších podmínek pro následné protiopatření s cílem předcházet škodám na majetku či proti útokům s cíli neautorizovaného přístupu k informacím;
  - schopnost vytvářet zcela automatizovaně záznamy o vzniklých incidentech k následnému rozboru a pro účely zpětných auditů účinnosti bezpečnostních opatření.

Vzhledem k výše uvedeným skutečnostem bude nezbytné při navrhování takovýchto systémů spolupracovat s bezpečnostními specialisty, kterých je však nyní, vzhledem k absenci

relevantních vzdělávacích programů, nedostatek.

Výhledové směry VaVaI

V oblasti fyzické bezpečnosti, resp. prostředků technické ochrany osob, informací a majetku je patrná tendence sjednocování normativních postupů a pravidel nejen v rámci evropské legislativy vyplývající z implementace harmonizovaných předpisů a norem v oblastech standardů, zkušebnictví, zřizování, provádění profylaktických zkoušek těchto systémů, ale i v rámci příbuzných oborů a specializací jako je např. informatika.

Je kladen čím dále vyšší důraz na unifikaci komunikačních rozhraní mezi technologiemi navzájem. Příkladem z poslední doby je např. vytvoření nových mezinárodních platforem v oblasti IP CCTV systémů ONVIF a PSIA.

K podobným tendencím dochází i v oblasti nadstavbových grafických monitorovacích a řídicích systémů, kde se začíná projevovat těžkopádnost úzkoprofilově vyvinutých platforem, které jen velmi těžko s podporou menších lokálních firem sledují neustále se zvyšující se trendy a požadavky na tyto systémy.

Dnes již nevystačíme jen s klasickými grafickými rozhraními, ale je cítit čím dále větší tlak uživatelů a investorů na propojení a návaznosti s dalšími systémy v rámci optimalizace procesů a vyplývající ekonomické návratnosti takovýchto investic.

Pod pojmem integrace bezpečnostních technologií rozumíme vytvoření nového technologického celku, který zvýší účinnost technologií nebo doplní jejich funkce. Předpokladem úspěšné integrace je znalost cílového stavu před začátkem prací a samozřejmě způsobilost zařízení.

Tak jak se vyvíjí bezpečnostní technologie, pokračuje i rozvoj softwarových nástrojů pro jejich integraci a vizualizaci. Uživatel se dnes vedle technických parametrů dívá na integrační nástroj jako na investici k dosažení budoucích úspor. Proto se dnes bezpečnostní software posouvá za cílem **minimalizace** počtu členů bezpečnostní služby, zastoupit je vždy odpovídající reakcí na incident a otrocky opakovat úlohy v režimu 24/7.

Propojení světa bezpečnosti a informačních technologií umožnila využít především přenosové trasy na bázi TCP/IP protokolu a tím zjednodušit instalace prvků bezpečnosti. Největší posun v tomto směru zaznamenala IP CCTV a to především:

- Analýza video obrazu (osoby, předměty, RZ vozidel …), která akusticky upozorní přítomnou obsluhu. Sledování obrazovek očima je u velkých kamerových systémů nemyslitelné až nesmyslné.
- Označování videozáznamu je nová a zásadní funkce integračních systémů. Díky vytváření časových značek s vazbou na videozáznam lze významně zkrátit dobu prohledávání videozáznamu. Uživatel zadá textově událost, kterou hledá a systém mu poskytne odkazy k odpovídajícímu záznamu kamer.

Významným nástrojem, který se v poslední době rozvinul, jsou funkce simulací poplachů a poruch za účelem tréninku obsluhy. Zvyšování znalosti řešení postupů a připravenosti obsluhy je významný prvek pro minimalizaci počtů jejich členů.

IT svět se změnil a přináší možnosti různých prezentačních platforem. Zatímco nedávnou doménou klientského prostředí byl program běžící na PC s MS Windows, je dnes patrný posun k webovým technologiím a mobilním prostředků. Díky dobře dostupným datovým službám je prakticky všude zajištěna konektivita do internetu a tím i přístup k integračnímu systému. Bezpečnost řeší opět IT.

V posledním období dochází prudkému vývoji, zejména v oblasti CCTV systémů, kde nové analytické funkce systémů CCTV umožňují výrazně sofistikovanější vyhodnocování obrazových záznamů a s tím související možnost jejich využití i v ostatních oblastech bezpečnostních technologií. Odrazem této skutečnosti je situace v oblasti výstavnictví, kdy je na výstavách se zaměřením na bezpečnost věnována mimořádná pozornost právě novým trendům v oblasti CCTV a některých dalších technologií, které jsou ruku v ruce závislé na zpřístupnění kamerových systémů i pro jiné aplikace.

Markantním příkladem je např. výrazně zvýšená poptávka a s ní související rozvoj perimetrických poplachových systémů, jejichž nezbytnou součást v podobě verifikačního systému právě kamerové systémy tvoří. Tyto systémy získávají na oblibě zejména z důvodu, že vyjma své preventivní funkce dokáží identifikovat potencionální vznikající rizika už na samotném obvodu perimetru zájmových oblastí, čímž vytváří podstatně lepší podmínky pro následné protiopatření s cílem předcházet škodám na majetku či proti útokům s cíli neautorizovaného přístupu k informacím.

Nezanedbatelnou skutečností přitom je, že dnešní moderní technologie jsou schopny vytvářet zcela automatizovaně záznamy o vzniklých incidentech k následnému rozboru a pro účely

zpětných auditů účinnosti bezpečnostních opatření.

Ačkoli by se mohlo zdát, že z důvodu postupného prolínání bezpečnostních a IT technologií je výhledově možné aplikovat bezpečnostní systémy i znalými pracovníky z oblasti IT, tak skutečnost je zcela opačná a chyby, které dnes monitorujeme na poli takto dnes budovaných systémů, jednoznačně ukazují na nutnost řešení bezpečnostní problematiky právě bezpečnostními specialisty, kteří se budou profilovat na uzavřenou část IT systému, které zejména u vysoce zájmových objektů budou provozovány jako uzavřené systémy v rámci stávající datové sítě.

Úspěšná integrace

Předpokladem účinného spojení technologií a jejich plného využití je přítomnost integrátora nikoliv jen instalace software, který „umí“ komunikovat s technologií. Dobrá vůle provozovatele umožní snadno rozpoznat provozní potřeby objektu a vytvořit prostředí, které ocení nejen provozovatel, ale i koncový uživatel.

Naplňování SVA TPEB

TPEB byla založena jako odpověď na výzvy a příležitosti, které souvisejí s dynamickým odvětvím kritické infrastruktury v oblasti energetiky, ale i v dalších sektorech. Celá řada událostí z posledních let ukazuje na potenciální zranitelnost současných vyspělých společností, která odráží inherentní závislost těchto společností na vzájemně propojených infrastrukturních systémech. V oblasti energetiky navíc nejen v souvislosti s bezpečností dochází k zavádění nových technologií, které významně proměňují dosavadní fungování energetických sítí. Aktivity TPEB tak reflektují jednak potřebu hledat technologické, ale i strategické či politické odpovědi na celospolečenské hrozby, ale také zprostředkovat využití výzkumného a inovačního potenciálu českých vědeckých institucí a firem.

TPEB je od počátku koncipována jako otevřený PPP projekt, ve kterém hlavní pilíře představují energetické infrastrukturní firmy, utilitní firmy, orgány státní správy a výzkumné a vědecké organizace. Po pěti letech fungování se členská základna stabilizovala, přičemž zahrnuje významné infrastrukturní firmy (ČEPS, ČEZ), další společnosti (např. ERA, CNS, TTC Marconi, TTS Group), zástupce státní správy (Hasičský záchranný sbor ČR, Moravskoslezský kraj), nejvýznamnější české technické vysoké školy (ČVUT, VUT, UTB, VSB -TU Ostrava) a další výzkumné ústavy (Vojenský technický ústav).

Takto vystavěná organizace se jeví jako ideální instrument k naplňování aktivit v oblasti ochrany kritické infrastruktury. Konkrétní výkonná strategie TPEB bude založena na dvou pilířích:

Internacionalizace v rámci evropských platforem

TPEB se konkrétně účastní na aktivitách evropských platforem, které souvisí s předpokládáním a následnou realizací politik a programů EK.

Mnoha těchto aktivit se TPEB přímo účastní, ať již ve spolupráci s orgány státní správy, jak to procedura vyžaduje, nebo samostatně, neboť zastupuje zájmy české vědy a průmyslu, komunikuje, koordinuje své postoje se zmíněnými státními institucemi. Klíčová role pro danou problematiku ve státní správě v gesci Ministerstva vnitra ČR; respektive Hasičského záchranného sboru (HZS) a Ministerstva průmyslu a obchodu ČR.

Účast v platformě 3rd ERNCIP CIIP SCADA – Integrované kontrolní systémy a Smart Gridy (Integrated Control Systems a SmartGrids)

Směrnice o ochraně kritické infrastruktury a její transpozice do české legislativy a její další vývoj jsou v kompetenci HZS. S tím souvisí i společná účast zástupců HZS a TPEB v programu ERNCIP (European Reference network for Critical Infrastructure protection). Tento poradní orgán analyzuje evropské laboratoře a zkušebny a doporučuje EK jejich využívání pro nové technologie z oblasti ochrany kritické infrastruktury, energetiky, komunikace, ICT apod. TPEB byla zastoupena ve skupině ERNCIP Industrial Automated Control Systems and Smart Grids Thematic Group.

Posláním ERNCIP je podporovat vznik inovačních, kvalifikovaných, efektivních a konkurenceschopných bezpečnostních řešení, a to prostřednictvím sítě evropských experimentálních laboratoří a testovacích zařízení. ERNCIP řeší chybějící síť harmonizovaného celoevropské testování a certifikací za účelem zvýšení konkurenceschopnosti a inovace výrobků a služeb, což je překážkou pro další rozvoj a přijetí na trhu bezpečnostních řešení.

Účast v platformě úřadu EK CEN/CENELEC „Koordinační skupina kybernetická bezpečnost“ (Cyber Security Coordination Group CSCG) na základě mandátu EK M/487. Jednalo se o analýzu aktuální standardizace v oblasti bezpečnostních norem a požadavkem o následný návrh postupu pro jejich harmonizaci a případné vytvoření nových norem pro oblast ochrany kritické infrastruktury, včetně energetické a kybernetické bezpečnosti.

Byl vytvořen seznam národních norem v uvedené oblasti, dále byl vytvořen soupis mezinárodních norem poskytující přehled o evropských a světových standardech a existujících databázích.

Prvními závěry jsou, že bezpečnostní průmysl EU je rozdrobený, má výraznou potřebu standardizace nezbytné pro zvýšení evropské konkurenceschopnosti tohoto odvětví na světovém trhu.

Bylo analyzováno 78 projektů v rámci 7. rámcového programu EK výzkumu v oblasti bezpečnosti programu. Zjištěním je, že pouze čtyři projekty se zabývaly standardizací, což se odráží v projektových výzvách programu H2020.

V rámci uvedeného procesu TPEB spolupracovala s Úřadem pro normalizaci, metrologii a

zkušebnictví (ÚNMZ) při MPO ČR. Jedná se o společnou účast v poradním orgánu standardizačního úřadu EK CEN/CENELEC „Koordinační skupina kybernetická bezpečnost“. (Cyber Security Coordination Group - CSCG) Tento nový poradní orgán doporučuje EK úpravy a vytváření norem a standardů a následných certifikací v uvedené oblasti.

Spolupráce s platformou Evropská organizace bezpečnosti (European Organisation of Security)

TPEB dlouhodobě spolupracuje s evropskou institucí European Organisation of Security (EOS), která je bruselskou platformou sjednocující 43 špičkových výzkumných ústavů, firem a institucí zabývajících se otázkami bezpečnosti. Problematika, ve které spolupracuje, je zaměřena na otázky ochrany kritické infrastruktury v souvislosti s přípravou pokračování Bílé knihy „Bezpečnost energetické infrastruktury“ a „Postupy pro implementaci strategie evropské kybernetické bezpečnosti“. TPEB je pravidelně zvána na akce EOS a účastnila se výroční konference.

Spolupráce s DG Joint Research Centre

TPEB spolupracuje s Directorat General Joint Research Centre (DGJRC) – Institutem pro ochranu obyvatelstva v Ispře (Itálie). Tato instituce provádí řadu vědeckých úkolu a studií, které jí zadávají jednotlivá DG (Generální ředitelství) na základě mandátů EK. Prostřednictví DG JRC, ale i napřímo, TPEB komunikuje s DG Energy, DG Home, DG Enterprise and Industry, DG Research. Jde zde především o získávání informací, které souvisí s aktivitami ve výše uvedených poradních orgánech, o možnosti je připomínkovat, komentovat a spolupodílet se na jejich dalším řešení. V neposlední řadě jde také o strategické informace související s výzvami programu H2020.

Spolupráce s ETP ARTEMIS a ENIAC

rozvíjí své projektové aktivity také prostřednictvím navazováním spolupráce s evropskými technologickými platformami (ETP). Výsledné projekty vycházejí mimojiné ze struktur ETP NETWORLD 2020 (https://www.networld2020.eu/), se kterou platforma navázala hlubší vztahy během projektové cesty do Atén prostřednictvím firem, které jsou součástí této ETP. Dlouhodobě kooperativní vztahy lze vysledovat také s ETP Artemis, ve které působí dvě největší české technické školy, které jsou zároveň součástí platformy. Prospektivně se také jeví platforma Sustainable Nuclear Energy Platform (SNETP) ze sekce Energy, která pořádala

výroční konferenci Nuclear Days 2018 v Praze. V této ETP již působí zástupci Centra jaderného výzkumu Řež a Ústavu jaderného výzkumu Řež, které dlouhodobě představují jedny z nejúspěšnějších českých institucí v kontextu rámcových programů a H2020.

VUT v Brně, zakládající člen TPEB, je členem obou ETP a podílí se na řešení mezinárodních projektů jako součást konsorcia řešitelů. TPEB se zúčastnila v roce 2015 finální konference platformy ARTEMIS, kde se jí podařilo zahájit diskuzi o v budoucnosti podaném H2020 projektu. V ETP působí také klíčový partneři TPEB v inovačních konsorciích (např. společnost EXODUS).

TPEB bude i v dalším období využívat tyto a jiné platformy a jejich akce primárně k šíření vize platformy jako efektivního českého (potažmo) regionálního „inovačního hubu“. Cílem je získávat informace o připravovaných výzvách a konsorcií a představovat přidanou hodnotu se zapojování členů i nečlenů TPEB.

TPEB se bude také aktivně účastnit mezinárodních jednání výše uvedených pracovních skupin s cílem implementovat získané poznatky v podmínkách ČR. Získaný přehled o aktivitách EU v této oblasti umožní českým subjektům najít vhodnou dlouhodobou strategii vlastního rozvoje a dosažení vysokého stupě konkurenceschopnosti.

Podpora národních a mezinárodních VaVaI projektů

V národním kontextu se TPEB bude soustředit především na výzvy strukturálních fondů, agentury TAČR a programu Bezpečnostního výzkumu Ministerstva vnitra ČR.

V návaznosti na charakter konkrétních výzev bude TPEB uplatňovat následující v praxi odzkoušenou strategii fungování kooperačně inovační sítě:

1. TPEB bude sama iniciovat a organizovat konsorcium, a to zejména v případech, kdy se bude konkrétní agenda zaměřovat na zájmy a potřeby velkých energetických infrastrukturních firem. Do konsorcií budou pozvány utilitní firmy a především členské i nečlenské (potenciálně členské) výzkumné instituce.

2. Projekt bude iniciován výzkumnou institucí, která využije funkční mechanismy a dlouhodobě vybudovanou důvěru mezi TPEB a členskými firmami a prostřednictvím TPEB tak získá relevantní partnery z firemní sféry.

3. Projekt bude založen na konkrétním návrhu utilitní firmy, které TPEB zprostředkuje výzkumné i strategické firemní partnery a poskytne patřičný projektový servis.

V mezinárodním kontextu se TPEB bude dominantně soustředit na budování konsorcií usilujících o projekty v rámci výzev H2020, resp Horizon Europe. Vzhledem k interdisciplinárnímu a mezitematickému charakteru problematiky ochrany kritické infrastruktury budou sledovány v zásadě všechny sekce, přičemž ale hlavní pozornost bude věnována výzvám v sekci Societal Challenges – Secure Societies a Societal Challenges - Secure Clean and Efficient Energy a dále výzvám v oblasti ICT, které mívají značný infrastrukturní přesah. Zvláštní pozornost bude také věnována SME instrumentům. Sekce nové verze programu Horizon Europe ještě nejsou dané.

V návaznosti na výzvy bude TPEB uplatňovat následující odzkoušené strategie:

1. TPEB společně se členy identifikuje konkrétní strategicky zajímavou výzvu a následně prostřednictvím vlastní sítě osloví potenciální zahraniční partnery. Zahraniční síť kontaktů představuje výsledek dosavadní činnosti TPEB v mezinárodních projektových konsorciích a nejrůznějších expertních platformách. Tato síť mimo jiné zahrnuje instituce, jako jsou DG JRC Ispra, European Organisation of Security ERNCIP či KEMEA a dále významné společnosti se značnou VaVaI kapacitou jako jsou například Atos, Indra, Exus. Přirozenou součástí této snahy je i využití kontaktů členských výzkumných institucí.

2. TPEB bude požádána o přistoupení ke konsorciu zahraničním partnerem s tím, že zaštítí a zprostředkuje nabídku členským i nečlenským českým firmám a výzkumným institucím. S rostoucí rozeznatelností TPEB jako spolehlivého partnera lze očekávat, že dojde k potvrzení trendu spočívajícím v rostoucím počtu těchto nabídek. Také prostřednictvím předkládaného projektu má TPEB ambici stát se významným regionálním hubem v oblasti ochrany kritické infrastruktury.

Závěr

Strategická výzkumná agenda TPEB podává stručný přehled o oblasti ochrany kritické infrastruktury v kontextu používaných technologií v oblasti ochrany kritické infrastruktury. Současně představuje možné směry vývoje v těchto oblastech s cílem efektivně anticipovat společenské výzvy a návazně projektové příležitosti v oblastech bezpečnostního výzkumu a vývoje. Tuto skutečnost dokládá výčtem úspešně podaných a podpořených projektů z programu H2020. V neposlední řadě pak představuje již úspěšně odzkoušenou strategii implementace SVA v kontextu evropských výzkumných programů a ETP.

Takto SVA reflektuje klíčové aktivity TPEB, které směřují ke stimulaci, koordinaci a zapojování členské základny a dalších subjektů z vnějšího prostředí do projektů výzkumu a vývoje, přičemž důraz je v této souvislosti kladen na propojování schopností a potřeb firemní a výzkumné sféry reflektující strategické potřeby a zájmy infrastrukturních společností a orgánů státní správy.

Na základě Strategické výzkumné agendy byl zpracován Implementační akční plán obsahující základní kroky TPEB vedoucí k ustavení TPEB jako relevantního aktéra v oblasti VaVaI v odvětví ochrany kritické infrastruktury.