Strategická výzkumná agenda Technologické platformy „Energetická bezpečnost ČR“ (TPEB)

Obsah

Strategická výzkumná agenda TPEB – shrnutí

SVA vychází z aktuálních technologických priorit, které byly definovány v rámci analytických dokumentů EK zabývajících se problematikou průmyslu pro ochranu kritické infrastruktury. Současně reflektuje potřeby domácího trhu pro zajištění energetické a kybernetické bezpečnosti.

SVA byla dlouhodobě připravována v souladu s podpůrnými studiemi a analýzami EK v rámci DG Joint Research Centre, které vytvářely podklad pro novou průmyslovou bezpečnostní strategii EK. Bezpečnostní strategie byla zveřejněna v červenci 2012 a je základním strategickým dokumentem pro evropské výzkumné a průmyslové instituce, které se v dané problematice angažují.

Tato strategie odráží i priority konkurenčních světových entit, zejména USA. V mnoha případech zde s USA existují dohody o spolupráci a výměně informací. Tento přístup by měl Evropě, resp. členským státům, které se aktivně účastní od samého počátku zajistit, aby se v příštích letech mohly stát nezastupitelným spolutvůrcem nových technologií a souvisejících legislativně procesních postupů.

Na základě současných poznatků byly identifikovány čtyři základní technologické oblasti, ve kterých bude TPEB iniciovat výzkumné a vývojové projekty zaměřené na návrhy nových produktů a služeb a to jak z hlediska technologického, tak i legislativně procesního. Jedná se o následující technologické oblasti:

- Komunikační technologie
- Kybernetická bezpečnost
- Technologie sledování prvků KI
- Fyzická bezpečnost

Aktivity TPEB do konce roku 2014 budou zaměřeny na využití stávajících národních programů na podporu vědy a výzkumu, zejména programu bezpečnostního výzkumu České republiky v letech 2010 – 2015 (BV II/2-VS) a druhé výzvy TAČR Centra kompetence plánované v roce 2013. Obsah projektů bude zaměřen na jednotlivé technologické oblasti uvedené výše a je uveden v IAP.

Ohrožení aktivit VaVaI může nastat z důvodu:

- Nedostatku v oblasti lidských zdrojů - kvantitativního i kvalitativního
- Redukce aplikovaného výzkumu v oblasti energetické a kybernetické bezpečnosti

Proto musí být vytvořeny podmínky pro:

- Podporu přírodovědných a technických VŠ oborů
- Vytvoření systému osvěty a vzdělávání pro širokou veřejnost v oblasti kybernetické bezpečnosti
- Prosazení problematiky kybernetické bezpečnosti do všech stupňů vzdělávání
- Strategické řízení podpory v oblasti energetické a kybernetické bezpečnosti

Seznam zkratek a pojmů

ČR – Česká republika
EU – Evropská unie
CIP – Critical Infrastructure Protection (ochrana kritické infrastruktury)
CONOPS – Concept and Operations (koncepce a způsoby nasazení)
DG – Directorates General
EHP – Evropský hospodářský prostor
EDA – European Defence Agency
ESA – European Space Agency
HDO – Hromadné dálkové ovládání
ICT – Informační a komunikační technologie
IZS – Integrovaný záchranný systém
KI – Kritická infrastruktura
KKII – Kritická komunikační a informační infrastruktura
MVF – Mezinárodní visegrádské fondy
PSP – Poslanecká sněmovna Parlamentu
SES – Single European Sky
Smart Grids (SG) – Inteligentní sítě
SVA – Strategická výzkumná agenda
TAČR – Technologická agentura České republiky
UAS – Unmanned Aerial Systems (bezpilotní systémy)
UAV – Unmanned Aerial Vehicles (bezpilotní prostředky)
VaVaI – Výzkum, vývoj a inovace
WRC – World Radiocommunication Conference

Představení TPEB

Technologická platforma „Energetická bezpečnost ČR“ byla založena z iniciativy Hospodářského výboru PSP ČR dne na Ustavující členské schůzi dne 24. 11. 2011 v Praze.

TPEB ČR je sdružení právnických osob, veřejného i soukromého sektoru zaměřených na problematiku energetické a kybernetické bezpečnosti a související ochrany kritické infrastruktury.

Záměrem TPEB ČR je prosazování těchto zájmů v uvedených oblastech, tak aby byly zohledňovány a naplňovány požadavky legislativní a rovněž bylo vytvářeno prostředí pro podporu příslušných projektů a programů na úrovni národní i mezinárodní.

TPEB ČR je společenství, které vytváří a stimuluje dialog mezi privátními a veřejnými subjekty s cílem identifikace hlavních hrozeb ve zmíněném prostředí s následným hledáním jejich řešení. Tento dialog začíná již od provozní úrovně firem, tak aby jasně definoval požadavky a podmínky, které průmysl potřebuje pro hledání řešení, budování konkurenceschopnosti, jak ve výrobě a provozu, tak i v oblasti výzkumu. Uvedení těchto postupů v platnost a následná certifikace v souladu s harmonizovanými předpisy EU umožní inovativní řešení využitelná na národní i mezinárodní úrovni.

Posláním TPEB je vytvořit vědecko-výzkumnou a průmyslovou základnu zaměřenou na podporu aktivit souvisejících s výzkumem, vývojem a zaváděním technologií souvisejících se zajištěním ochrany kritické infrastruktury ČR v oblastech energetiky a kybernetiky.

Aktivity TPEB:

- Definuje, reprezentuje, podporuje, hájí a prosazuje oprávněné a společné zájmy svých členů v oblasti výzkumu, vývoje a aplikace moderních technologií zvyšujících úroveň energetické a kybernetické bezpečnosti ČR
- 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 energetické a kybernetické bezpečnosti společného prostoru i jednotlivých členských zemí, zejména pak aktivit souvisejících s mandátem č. 487 EK.
- 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 energetické a kybernetické bezpečnosti.
- Systematicky sleduje možnosti získání prostředků ze zdrojů EU, ČR a jiných, pro podporu výzkumu, vývoje a zavádění moderních technologií v oblasti energetické a kybernetické bezpečnosti.
- Aktivně se podílí na vytváření souvisejících standardů a metodik pro nastavení závazné certifikace pro oblast energetické a kybernetické bezpečnosti.
- Spolu s orgány státní správy spoluvytváří systém a institucionální zajištění energetické a kybernetické bezpečnosti ČR.
- Systematicky optimalizuje bezpečnostní perimetry energetiky pro zajištění bezpečnosti osob a majetku.
- Poskytuje expertízy a konzultace pro orgány státní správy a samosprávy v oblastech souvisejících s energetickou a kybernetickou bezpečností, s důrazem na vyhodnocení

míry ohrozitelnosti a zranitelnosti krizových míst energetické a kybernetické infrastruktury ČR.
- Usiluje o vytvoření a udržování systému efektivního řízení rizik.
- 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.

Řádní členové TPEB:

Čepro a.s.

ČEPS a.s.

Fujitsu Technology Solutions s.r.o.

RWE Transgas, a.s.

SIEZA a.s.

TTS energo s.r.o.

VÍTKOVICE IT SOLUTIONS a.s.

bnt - pravda & partner, s.r.o.

Vodafone Czech Republic a.s.

VŠB -TU Ostrava

Vysoké učení technické v Brně

Přidružení členové TPEB:

Integoo s.r.o

dataPartner, s.r.o.

CNS a.s.

INVEA-TECH a.s.

Icontio CR s.r.o.

1. Úvod

Světový bezpečnostní průmysl je jedním z mála sektorů, který vykazuje velmi výrazný potenciál růstu a zaměstnanosti. Za posledních deset let se z původních 10mld € zdesetinásobil na 100mld € (údaje do roku 2011). Nehledě na velkou segmentaci tohoto trhu tvoří mnohé 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, která mají vést k harmonizaci a rozvoji vnitřního trhu, podobně jak tomu je v USA, které je světovým technologickým vůdcem v uvedené oblasti.

Světový bezpečnostní trh se dle údajů z roku 2011 odhaduje na 100mld E a zaměstnává cca 2 miliony osob; evropský bezpečnostní trh se odhaduje v rozpětí od 26mld € do 36,5mld € a zaměstnává cca 180 000 osob.

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 12,6mld € a v Evropě 3,5mld €. Kybernetická a komunikační bezpečnost ve světě je 19,4mld € a v Evropě 5mld €.

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. Není potřebná koordinace při podpoře výzkumu a aplikace následných výstupů tohoto výzkumu do praxe. Mnohdy je výzkum sám pro sebe a jeho výsledky se nedostanou jako aplikovaný výzkum k využití v průmyslu. Jde tedy o mrhání prostředky na národní i evropské úrovni a o technologickém zaostávání, zejména ve vztahu k USA.

Pro zmapování situace a navržení dalších kroků pověřila EK v září 2011 svým mandátem 487 standardizační úřad CEN/CENELEC analýzou existujících standardů v oblasti ochrany kritické infrastruktury a doporučení postupu jak v oblasti harmonizace standardů, tak i následných legislativních kroků (návrh nové směrnice EK apod.) Do části této aktivity se zapojila TPEB, jak je uvedeno níže, v podobě účasti v poradním orgánu CEN/CENELEC „Koordinační skupina kybernetické bezpečnosti“, která je jednou z evropských platforem pro oblast kybernetiky v kritické infrastruktuře.

EK navrhuje ve svém sdělení z 26.7.2012 „Bezpečnostní průmyslová strategie“ COM (2012) 417 final; kromě jiného vytvoření „EU brand“ (evropské značky) pro bezpečnostní technologie. To bude znamenat řadu normativních a standardizačních iniciativ doprovázených certifikačními a auditorskými procesy.

Dalším významným dokumentem je směrnice EK „Evropský program pro ochranu kritické infrastruktury“ nyní projednávaný v Evropském parlamentu, který bude předložen na podzim 2012. V něm jsou obsaženy priority ochrany kritické infrastruktury a návrhy na jejich zabezpečení.

Nelze nezmínit i souvislost se 7. Rámcovým programem „Bezpečnost“ (2007 – 2013) kde bylo alokováno 1,4mld.€ pro rozvoj vědy a výzkumu v uvedené oblasti. V novém programu EK Horizon 2020 se počítá s navýšením částky o 50% na uvedenou problematiku.

Oba uvedené dokumenty i programy se kromě harmonizace legislativy, standardizace a zkušebnictví zaměřují na podporu rozvoje nových technologií a propojování (technologické, komunikační) jednotlivých zmíněných oblastí. Dávají důraz na aplikovaný výzkum a demonstrační projekty a vymezují průmyslová odvětví z hlediska priorit a času. To vše se odráží v další části předkládané SVA.

TPEB ČR se již nyní přímo účastní činnosti ve dvou základních poradních orgánech EK – jejích Platformách – kterými jsou:

- 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. Zástupce TPEB je ve skupině ERNCIP Industrial Automated Control Systems and Smart Grids Thematic Group, která má do konce roku předložit EK první dílčí doporučení jak postupovat v uvedené problematice, zejména s ohledem na vytváření norem a standardů a nových technologických aplikací.
- V poradním orgánu standardizačního úřadu EK CEN/CENELEC se jedná o (Cyber Security Coordination Group) „Koordinační skupina kybernetická bezpečnost“. Tento nový poradní orgán doporučuje EK úpravy a vytváření norem a standardů a následných certifikací v uvedené oblasti. Vznik platformy byl iniciován mandátem EK 487 v roce 2011. V této problematice zabývající se kybernetickou bezpečností TPEB spolupracuje s Úřadem pro normalizaci, metrologii a zkušebnictví (ÚNMZ) při MPO ČR. Ve zmíněné platformě jsou zástupci obou uvedených organizací.

TPEB dlouhodobě spolupracuje s evropskou institucí European Organisation on Security (EOS). EOS je bruselskou platformou sjednocující 39 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. Jako příklad můžeme uvést aktivitu z března 2012. EOS zorganizoval v Bruselu Konferenci k problematice Průmyslové bezpečnosti pod patronátem a za účasti Antonio Tajani, vicepresidenta EK , komisaře pro průmysl a podnikání Neelie Kroes – vicepresidentky EK a komisařky pro digitální agendu, Siim Kallas – vicepresidenta EK a komisaře pro dopravu a Cecilie Malmstrom - komisařky pro vnitřní záležitosti. Na této konferenci byly na nejvyšší úrovni diskutovány návrhy EK týkající se bezpečnosti v oblasti ochrany kritické infrastruktury, energetiky a kybernetiky. Představitelé EK zde předložili věcný i časový harmonogram jejich implementace. Činnosti a projekty TPEB jsou v souladu s tímto rámcem ve věcné rovině i z pohledu času jeho implementace. (příloha – EOS High Level Security Round Table)

V rámci SVA jsou řešeny následující čtyři tematické oblasti relevantní z hlediska energetické a kybernetické bezpečnosti a to jak z hlediska legislativy, tak technologií:

- Komunikační technologie
- Kybernetická bezpečnost
- Technologie sledování prvků KI
- Fyzická bezpečnost

2. Analýza EB (očekávaný vývoj a změny v ochraně KI v horizontu 20 let)

2.1. Komunikační technologie

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 deset 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 rozhranní a to jak z hlediska HW komponent, tak i vzhledem k jednotnému formátu distribuovaných dat

2.2. Kybernetická bezpečnost

Význam kybernetické bezpečnosti roste v poslední době geometrickou řadou, přestože je z posuzovaných technologických oblastí jednoznačně nejmladší. 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:

- 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

2.3. Technologie sledování prvků KI

V posledních letech jsou vyvíjeny mezinárodní aktivity související se začleněním bezpilotních prostředků do nesegregovaného vzdušného prostoru s cílem umožnit jejich civilní provoz. Probíhající aktivity jsou zaměřeny na testování komunikačních technologií pro satelitní spojení mezi pozemní řídící stanicí a vlastním UAS. Po technické stránce je nutné definovat potřebné parametry pro pozemní řídící stanici a to jak z hlediska funkčních vlastností, tak i komunikačních technologií. Z hlediska legislativy pak nevrhnout potřebné legislativní normy a postupy umožňující toto začlenění.

Současná legislativní úprava civilní využívání bezpilotních prostředků neumožňuje. V rámci mezinárodního projektu ULTRA, kterého se účastní české subjekty, budou vypracovány doporučení pro legislativní podmínky civilního provozu UAS v evropském vzdušném provozu. Zároveň bude otestováno v rámci projektu AO7082 ve spolupráci EDA/ESA satelitní spojení mezi pozemní řídící stanicí a vlastním UAS a ověřena jeho technická použitelnost pro tyto účely. Výsledky jsou očekávány do konce roku 2013 tak, aby byly využitelné pro následující mezinárodní konferenci WRC v roce 2015, která má v agendě plánováno určení kmitočtových přídělů pro komunikaci řídící jednotky s UAS. Následně bude řešeno přidělení kmitočtových pásem pro datové přenosy. Až na základě těchto výsledků bude možné předpovědět další možnosti využívání bezpilotních prostředků na ochranu prvků KI.

Vzhledem k předpokládaným užitným vlastnostem a nízkým provozním nákladům se předpokládá jejich budoucí široké nasazení. Předpokládané využití lze odhadovat v různých oblastech, ale ochrana prvků KI jako součást jejich zabezpečení bude jednou z hlavních aktivit:

Činnost	**Provozovatel**
Nepřetržité sledování prvků KI jak při běžném provozu, tak i v průběhu havárie či katastrofy	Provozovatelé KI (ČEPS, ČEZ, ČEPRO, atd.)
Systematické prohledávání rozlehlých lokalit (vyhledávání osob či předmětů)	Složky IZS
Sledování - Státní hranice - Dopravní situace - Pohyb zboží v silniční a železniční síti	MV ČR MD ČR Celní správa

Tab. 1 Příklady využití UAS

2.4. Fyzická bezpečnost

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.

3. Oblasti VaVaI

3.1. Komunikační technologie

3.1.1. Legislativa

Legislativa v oblasti komunikačních technologií je koordinována v rámci Evropské unie a v ČR řešena především Českým telekomunikačním úřadem. Ten vydává individuální oprávnění k užívání rádiových kmitočtů, stejně jako všeobecná oprávnění, kterými uvolňuje vybraná kmitočtová pásma pro bezlicenční využití při dodržení stanovených podmínek. Požadavky na elektromagnetickou kompatibilitu, tj. především omezení nežádoucího vyzařování, jsou do českých norem ČSN přejímány z harmonizovaných standardů EU, na jejichž tvorbě se příslušné české úřady podílejí.

Standardizace komunikačních systémů pro vzájemnou interoperabilitu je obvykle řešena konsorciem výrobců, které standard specifikuje. Prosazení takových standardů, jsou-li navrženy v souladu se závaznými normami, je pak především marketingovou záležitostí výrobců.

3.1.2. Technologie – popis současného stavu

Rozvoj komunikačních technologií a nárůst přenášených informací se projevuje ve všech směrech. Zasáhl jak oblast komunikace (převážně hlasové) využívanou 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 energetické bezpečnosti a 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 bylo mnoho kritiky na včasnou informovanost 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 vyšší přenosových rychlostí. Typickým představitelem metalické sítě je 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 bezlicenční 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 bezlicenčních pásem, uvolněných na základě generálního povolení. Kromě již popsané technologie WiFi a spíše výjimečného nasazení BlueTooth jsou využívány zejména systémy ZigBee a proprietární úzkopásmová 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.

3.1.3. Technologie - směry vývoje

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.

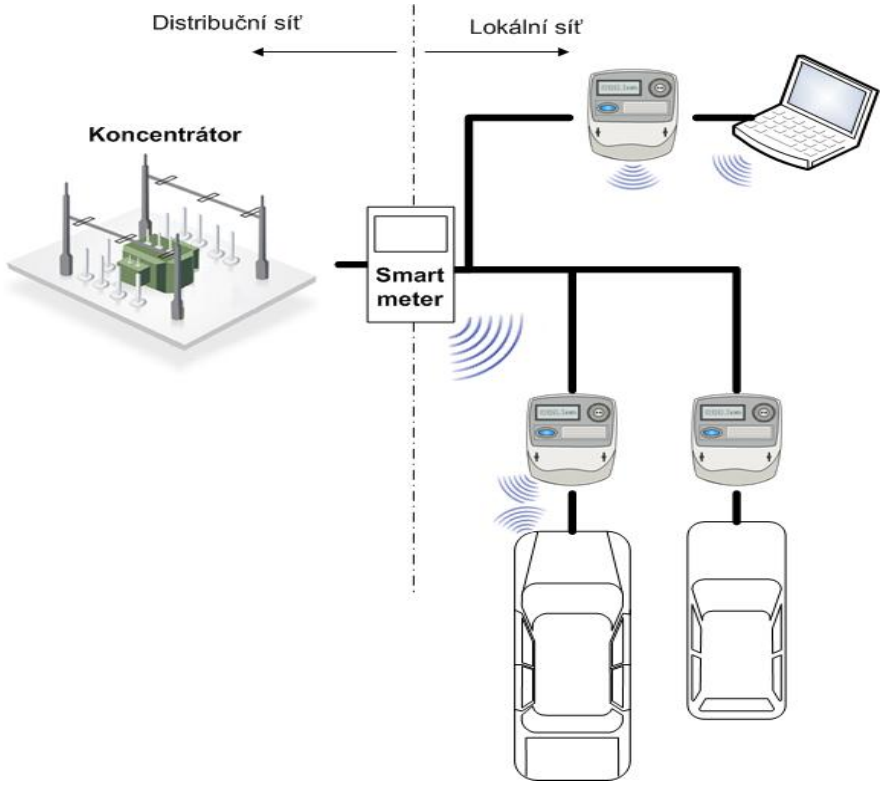
S očekávaným nárůstem spotřeby zejména elektrické energie u mobilních odběratelů (např. elektromobily) je potřeba řešit i otázku identifikace těchto odběratelů za účelem řízení distribuce energie tak, aby byla nejen optimalizována vytíženost sítě, předešlo se kolapsům (částí) energetické sítě kvůli dynamicky 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.

Příklady aplikace:

- Dobíjení elektromobilu při parkovaní na veřejných prostranstvích a ve společných garážích
- Řízení a kontrola odběru elektrické energie ve veřejných prostorách (např. společné prostory úřadů, letišť, konferenční centra)

V takových aplikacích je potřeba řešit spolehlivost a bezpečnost identifikace koncových uživatelů. Jako perspektivní se v tomto směru jeví zejména bezdrátová komunikace na principu radiofrekvenční identifikace (RFID), a to z důvodu rozšířeného využití této technologie v oblasti mobilních komunikací, identifikace osob a objektu (mobilních i stacionárních) a platebního styku. Obrázek 1. představuje schematický nákres napojení lokální sítě odběrných míst pro mobilní odběratele na distribuční síť. V tomto ohledu je potřeba zajistit návaznost smart meteru na technologie pro provoz sítě lokálních odběrných míst, řízení spotřeby energie, její měření, identifikaci a sběr dat pro vyúčtování.



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:

- Optimalizace 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

3.2. Kybernetická bezpečnost

3.2.1. Legislativa

V posledních letech, zejména v souvislosti s rozšířením internetových služeb, došlo k masivnímu průniku informačních technologií do řídících i ochranných prvků v rámci provozu kritické infrastruktury. Významný nárůst objemu zpracovávaných a uchovávaných dat zvýšil nároky na kapacitu a bezpečnost datových center, jednotlivé subjekty KI se staly závislé na řídicích systémech založených na ICT (informační a komunikační technologie).

Největší rizika z hlediska kybernetických hrozeb se jeví při zavádění nových technologií spojených s inteligentními sítěmi (SG – Smart Grids).

V současné době je problematika SG velmi diskutovanou otázkou. Na základě směrnice 2009/72/ES byly spuštěny pilotní projekty SG v členských státech (ČR-Vrchlabí) a nyní probíhá ekonomické posouzení všech dlouhodobých nákladů a přínosů pro trh i spotřebitele, které bude ukončeno 3. 9. 2012. V případě kladného výsledku posouzení dojde do roku 2020 k instalaci inteligentních technologií (smart meterů) na 80% odběrných míst. V opačném případě bude implementace odložena a v horizontu cca tří let bude provedeno opětovné posouzení z ekonomického hlediska. Otázka tedy nezní „zda“, ale „kdy“ bude schválena

implementace SG. Následně vzniknou podmínky pro masivní rozvoj smart technologií, a to především ve městech, kde budou součástí vyšších smart celků (inteligentní budovy, atd.).

Kybernetická bezpečnost a bezpečnostní standardy se však neřeší souběžně s vývojem nových technologií. Přitom překonání nedůvěry uživatelů je v současné době hlavní překážkou zavádění SG technologií. Je to podmíněno zprávami o manipulaci dat v SG systémech v technologicky vyspělých státech, kde je již používají. Škody způsobené neoprávněnou manipulací a daty jsou značné jak na straně provozovatelů, tak i uživatelů SG. Většina současných studií se věnuje bezpečnosti SG na technologické, ne však bezpečnostní úrovni.

Snahou TPEB bude vytvořit podmínky a podporovat tvorbu legislativních a standardizačních aktivit zaměřenou na kybernetickou bezpečnost KI.

- Legislativa
    - Definice kritické komunikační a informační infrastruktury (KKII) jako prvku KI a zároveň spojovacího prvku mez i prvky KI
    - Definování bezpečnostních standardů a jejich prosazení do informačních, komunikačních a řídicích systémů subjektů VS a subjektů provozujících prvky KI
    - Definice práv a povinností uživatelů kyberprostoru

- Standardy kybernetické bezpečnosti – informační a komunikační technologie
    - Vývoj bezpečnostních technologií v souvislosti s rozvojem a aplikací nových technologií v odvětvích zahrnutých do KI – SMART GRID atd.
    - Vývoj doporučení pro budování bezpečných IS (informační systémy)
    - Vývoj a vybudování systému pro průběžný vývoj, testování, ověřování a certifikaci technologií pro aplikaci bezpečnostních standardů do IS – Centre of excelence. Nepřetržité sledování vývoje bezpečnostních hrozeb a zranitelností v segmentu KI
    - Prosazování aplikace bezpečnostních standardů u subjektů provozujících prvky KKII (operátoři)
    - Stanovení požadavků na nepřetržitý bezpečnostní monitoring infrastruktury

3.2.2. Technologie

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.
- Vytvoření metodiky pro budování a udržování zabezpečených sítí
- Vytvoření metodiky a nástrojů pro testování zranitelnosti zabezpečených sítí.
- Vytvoření metodiky a nástrojů pro bezpečnostní monitoring
- Stanovení požadavků, které bude muset splňovat software (jeho dodavatel), který bude moci být použit u provozovatelů kritické infrastruktury. Zvážit vytvoření určité certifikace pro dodavatele těchto softwarů. Tento bod lze realizovat až po shodě na jednotných bezpečnostních standardech.

3.3. Technologie sledování energetických prvků kritické infrastruktury (KI)

3.3.1. Dálkový dohled (struktura, cíle, technologie)

Současné dohledové systémy všech typů distribučních sítí využívají systémy založené na sběru dat z různých senzorů a čidel pro získávání informací o aktuálním stavu vybraných klíčových parametrů nebo služeb. Následné využití získaných informací umožňuje:

- Efektivně řídit distribuci
- Lokalizovat poruchy a jejich rozsah
- Provádět pravidelné kontroly a optimalizaci
- Atd.

Naopak má nedostatky:

- Predikce ohrožení
    - Lidskou činností (úmyslné poškození, jiná činnost vedoucí k neúmyslnému poškození)
    - Působení přírodních živlů (blížící se požár, potopa, atd.)
- Dlouhodobé vizuální sledování v případě poškození (úniky ropných látek, hoření plynu, atd.)
- Nutná vysoká míra zabezpečení dat – jejich zničení nebo úmyslné pozměnění může způsobit kalamitní stavy

V těchto případech může vhodně doplnit nebo nahradit stávající technologie zavedení bezpilotních prostředků pro civilní použití.

3.3.2. Možnosti využití UAS

3.3.2.1. Legislativa

Mezinárodní provoz UAS, bez ohledu na hmotnost, spadá do kompetencí ICAO. V USA mají FAA ve své pravomoci civilní UAS o jakékoliv hmotnosti, které jsou provozovány vnitrostátně i mezinárodně. V Evropě je situace odlišná, touto problematikou se zabývá více subjektů na národní i regionální úrovni, ačkoliv k odpovědnosti vůči Úmluvě o civilním letectví jsou zavázány jednotlivé Členské státy EU.

Zejména současný rozsah tzv. základního nařízení ((ES) Č. 216/2008 o společných pravidlech v oblasti civilního letectví) se vztahuje na všechny letecké oblasti (letovou způsobilost a provoz, vydávání licencí leteckému personálu, řízení letového provoz). Některé UAS jsou však z kompetenci EASA vyjmuty (státní. pro výzkumné, experimentální nebo vědecké účely. individuálně postavené a všechny UAS s MTON menší než 150 kg).

V rámci své působnosti EASA v roce 2009 vydala zásady pro žadatele o osvědčení letové způsobilosti civilních UAS nad 150 kg a umožňuje tak již nyní certifikaci dle jiných dostupných dokumentů. Tvorba speciálních prováděcích pravidel je však předmětem dlouhodobého plánu 2013-2017. Dohled nad UAS mimo oblast působnosti základního nařízení je plně v kompetenci členských států EU. Další subjekty působící v oblasti regulace bezpečnosti a vypracování dobrovolných standardů pro UAS zahrnují EUROCONTROL, JARUS a EUROCAE. Aby UAS byly bezpečné a létaly bezpečně, je třeba právní otázky řešit mj, v souladu s právními předpisy EU týkající se SES (Single European Sky) a základního nařízení.

V současné době neexistují jednotná pravidla pro provoz UAS na úrovni EU. Některé členské státy Evropské unie mají vypracované vnitrostátní pravidla provozu ve vzdušném prostoru. Přeshraniční postupy však zatím nebyly vyvinuty na státní ani regionální úrovni. Letištní provoz je zatím řešen odděleně od ostatního provozu. Současný přístup k integraci UAS je řešen krok za krokem tam, kde je možnost využit prvotní zkušenosti průmyslu a provozovatelů v rámci vnitrostátního vzdušného prostoru.

Požadované mezinárodní či evropské standardizační a certifikační materiály nebudou dokončeny před rokem 2014. Zajištění jejich včasného dodání je závislé na podpoře pro ICAO Eurocae a v neposlední řadě národní úřady. Podpora mezinárodní spolupráce ze strany úřadů probíhá úspěšně (vč. ČR), ze strany průmyslu se omezuje na větší společnosti, které svým zaměstnancům umožňují účastnit se jednání. Situace malých a středních firem je zcela odlišná, nemají srovnatelné možnosti poskytnutí podpory.

V poslední době vzniklo několik národních projektů a činností na podporu integrace UAS do společného vzdušného prostoru. Nicméně výsledky těchto projektu nejsou vždy UAS komunitě k dispozici, Zvyšuje se tak riziko zdvojováni úsilí a neefektivního využívání zdrojů.

Dnešní systém regulace bezpečnosti v Evropě spočívá na roli EASA. připravuje pravidla na národních úřadech, které je implementují a opětovně na EASA, která tuto implementaci kontroluje. Z tohoto pohledu by navržené rozšíření kompetenci EASA nebylo v rozporu s tím, aby osvědčení typu byla vydávána na národní úrovni, což by zjednodušilo a zlevnilo postup pro žadatele a udrželo rovnoměrné rozložení kvalifikovaných pracovníků v EU. Zahájení provozu UAS může být podpořeno možnosti vydáván omezených osvědčení typu pro UAS provozovaná s určitými omezeními např. v nevyhrazeném vzdušném prostoru nad neobydlenými oblastmi v malých výškách.

Proto vzniká „Masterplan for civil UAS insertion into the Single European Sky“, který se aktuálně připravuje v rámci projektu FP7 ULTRA, kterého se aktivně účastní subjekty z ČR. Výstupy budou ovlivňovat další rozvoj UAS v rámci Horizont 2020.

Agenda je zaměřena především na vytvoření minimálních regulačních a certifikačních požadavků na začlenění UAS:

- Minimální úpravy a vybavení infrastruktury, která umožní začlenění UAS do civilního provozu
- Bezpečnostní a sociální kritéria pro začlenění UAS
- Ekonomické dopady, vliv začlenění UAS do civilního provozu na evropský průmysl
- Závěry a doporučení

Výše uvedené požadavky budou následně aplikovány v Evropě.

3.3.2.2. Technologie

Nové technologie budou směřovat k zabezpečení následujících hlavních cílů:

- Integrace UAV do nesegregovaného vzdušného prostoru umožňující civilní využití
    - Antikolizní systémy (Sense and Avoid)
    - Řízení a komunikace (SATCOM – připravuje se společný demonstrační projekt EDA/ESA)
    - Komunikační standardy
- Integrace UAV do celkového systému ochrany kritické infrastruktury
- Definice požadavků CIP operátorů
    - Struktura
    - Cíle
    - Vhodné technologie
- Funkční a fyzická architektura UAS pro CIP
    - Platforma
    - Pozemní řídící stanice
        - Řízení UAV
        - Integrace mission aids
        - Plánování misí
        - Spolupráce více prostředků na stejném komunikačním protokolu
        - Zpracování a vyhodnocení informací
    - Rozhraní do stávajících řešení CIP a spolupráce s nimi
    - Čidla a senzory
        - Výběr, přizpůsobení, optimalizace napájení, atd.
        - Přenos a zpracování dat (datová komunikace, zpracování informací)
        - Data fusion a vyhodnocovací algoritmy

3.4. Fyzická bezpečnost KI

Ještě v nedávné době byly bezpečnostní technologie jen zařízení, která pracovala izolovaně od okolního světa a poskytovala funkce pro sledování stavu detektorů, čteček nebo přenášela obraz z kamer. Během krátké doby se ukázalo, že provozování instalací s více ústřednami EZS nebo EPS nelze snadno obsluhovat a především bylo jasné, že obsluha musí být

technicky vnímavá. Díky dostupnosti počítačů řady PC začaly v 90. letech vznikat první softwary pro sledování stavu technologií, včetně bezpečnostních.

První softwarové nadstavby byly pouhým tablem, tedy jednoduchou vizualizací, která však dokázala do obrazovky PC vtěsnat stavy připojených technologií a sjednotit tak pohled na sledovanou oblast. Díky úspěchu nového přístupu, zažila oblast software pro vizualizaci obrovský boom. Během několika dalších let vzniknuly funkce pro vzdálené ovládání, spouštění úloh v plánovaném čase nebo vnitřní programovací jazyky, které umožnily skutečnou integraci technologií.

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.

3.4.1. Legislativa

V současné době jsou v rámci harmonizace legislativy v oblasti fyzické bezpečnosti platné zejména dále citované evropské normy, které jsou průběžně doplňovány a aktualizovány.

ČSN EN řady 50 130	Poplachové systémy – Všeobecně
ČSN EN řady 50 131	Poplachové systémy - Poplachové zabezpečovací a tísňové systémy
ČSN EN řady 50 132	Poplachové systémy – CCTV sledovací systémy pro použití v bezpečnostních aplikacích
ČSN EN řady 50 136	Poplachové systémy – Poplachové přenosové systémy a zařízení

Tab. 2 Evropské normy v oblasti FB

Příkladem mohou být např. normy z oblasti CCTV řady 50 132, kdy došlo díky stále vyššímu uplatňování IP CCTV technologií k vytvoření zcela nových standardů a v podstatě zde dochází k postupnému prolnutí bezpečnostních a IP technologií.

Jako příklad lze uvést např. nové požadavky kladené na kamerové systémy určené do objektů s vysokými riziky st. 4, kde je mimo jiné požadováno identifikovat substituci obrazových dat. Toto je velmi inovativní myšlenka, avšak není jednoznačně definováno, jakými prostředky se má tohoto stupně ochrany dosáhnout a je tedy velmi diskutabilní, jak by případný zadavatel výběrového řízení prováděl hodnocení v tomto kritériu.

V dlouhodobém horizontu se dá s největší pravděpodobností předpokládat, že společně se zvýšenou poptávkou v oblastech kamerových, požárních a ostatních např. perimetrických systémů bude docházet k doplňování standardů. Konkrétně pak v oblasti CCTV musí dojít ke zpřesnění nových požadavků norem z oblasti EN 50 132 a to formou i národních „technických normalizačních informací“.

V oblasti požárních systémů dojde vlivem dalšího tlaku na výrobce a jimi dodávané technologie ve smyslu včasnější a přesnější identifikace potencionálně nebezpečných situací a obdobně jako tomu je v oblastech CCTV, PZTS apod. k postupnému přechodu komunikačních infrastruktur směrem k IP standardům. S tím souvisí i postupný přechod navazujících systémů varování a vyrozumění do této oblasti.

V oblasti perimetrických poplachových systémů by mělo dojít k postupnému vyplnění normativní mezery v této specifické odnoži PZTS a CCTV systémů. Nyní např. v rámci ČR pracují dvě komise (PPS AGA a CEN/TC388) s touto specializací napojené na procesy v rámci CENELECu.

3.4.2. Technologie

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.

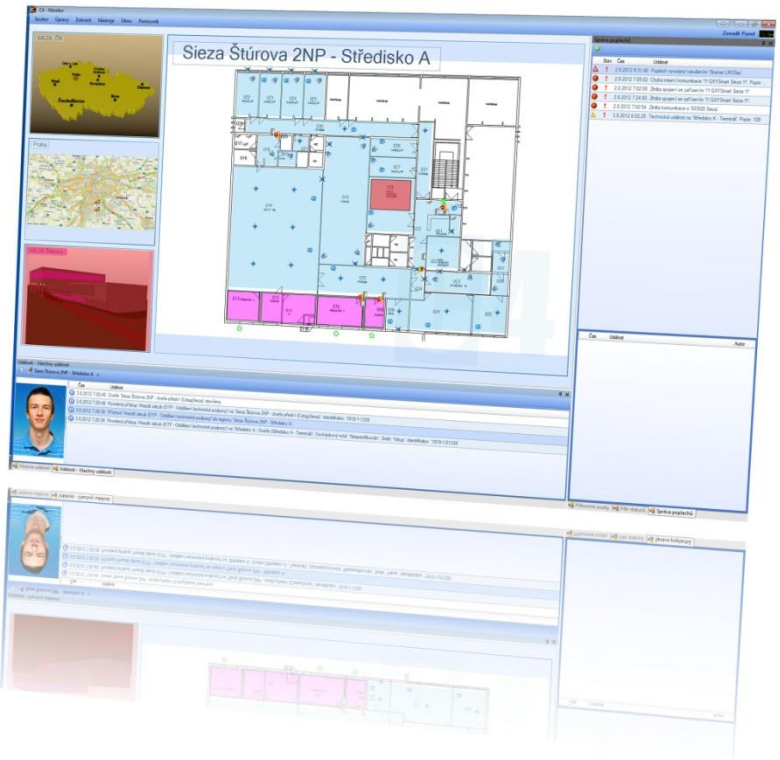
Markantním příkladem je např. výrazně zvýšená poptávka a s ní související rozvoj perimetrických poplachových systémů, jejichž nezbytnou součást v podobě verifikačního systému právě kamerové systémy tvoří. Tyto systémy získávají na oblibě zejména z důvodu, že vyjma své preventivní funkce dokáží identifikovat 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.



Obr. 2 Integrace systémů

3.5. Vliv zvýšení energetické bezpečnosti na ceny energií

Všeobecně jakékoliv další zabezpečení si vyžádá zvýšení nákladů na provoz energetických zdrojů a distribučních soustav. Ne v každém případě se však musí zákonitě promítnout do zákaznických cen. V jednotlivých oblastech se bude vliv zavedení bezpečnostních opatření výrazně lišit. Předpokládané dopady vlivu zavedení nových opatření ke zvýšení energetické bezpečnosti ve vztahu ke koncové ceně elektrické energie jsou stručně rozebrány v následujících kapitolách po jednotlivých oblastech.

3.5.1. Komunikační technologie

Komunikační technologie jsou typickou oblastí s dynamickým rozvojem, kde se ve velmi krátkých časových intervalech objevují nová řešení a služby. Jejich zavádění je nutné z hlediska kompatibility a interoperability jednotlivých systémů. Vzhledem k tomu, že tato výměna probíhá kontinuálně již několik desítek let, není důvod, aby se projevila nyní v koncových cenách.

Vážným rizikem, které by tuto domněnku mohlo zvrátit, je zavedení nových nadnárodních standardů. Vznikla by tak potřeba okamžité výměny technologií před ukončením jejich plánované životnosti a tím i mimořádné finanční náklady, které by se do koncových cen pravděpodobně promítly.

Snahou TPEB je těmto situacím předcházet právě aktivní účastí při tvorbě nových standardů a tím umožnit členům TPEB přístup k požadovaným informacím v dostatečném předstihu.

Samostatnou kapitolou je zavádění inteligentních sítí (SMART GRIDS), kde komunikační technologie tvoří značnou část. Předpokladem jejich zavedení je ekonomická výhodnost, kde se předpokládají úspory na straně spotřebitelů vzhledem k zavedení plovoucích cenových tarifů v závislosti na aktuálním stavu přenosové soustavy. Zároveň by mělo dojít i ke snížení celkové spotřeby. V podmínkách ČR se nyní tyto technologie testují, ale je reálné, že výsledky nepotvrdí jejich ekonomickou přínosnost a implementace SMARD GRIDS v ČR bude o několik let odložena právě z důvodu ekonomické náročnosti.

3.5.2. Kybernetická bezpečnost

Oblast kybernetické bezpečnosti se od předchozí odlišuje především tím, že v současné době není dostatečně řešena a v budoucnu dojde k jejímu masivnímu rozšíření. Náklady spojené se zavedením bezpečnostní opatření a nákupem potřebného SW vybavení se zcela jistě promítne do celkových nákladů na výrobu a distribuci energií.

Kompenzace zvýšených nákladů by mělo být dosaženo snížením energetických ztrát v důsledku:

- Včasného zjištění a zastavení úniku energií z důvodu poruchy
- Omezení neoprávněných odběrů zvýšeným zabezpečením či rychlou identifikací
- Atd.

3.5.3. Technologie sledování energetických prvků kritické infrastruktury (KI)

Doplnění současných sledovacích technologií o platformy bezpilotních systémů se do zvýšení cenových nákladů neprojeví.

Předpokládá se jejich využití tam, kde se nyní používá pilotovaný prostředek a v takovém případě dojde naopak k výrazným cenovým úsporám. Vzhledem k poměru cen letové hodiny pilotovaného letounu a bezpilotního prostředku je zřejmé, že návratnost prvotní investice do nákupu UAS je rychlá.

Musíme také vzít v úvahu i druhotné úspory, které nelze reálně vyčíslit. V průběhu havárií nebo katastrof umožní získané informace z paluby UAS včasný a přesně lokalizovaný zásah za účelem snížení rozsahu ztrát a to jak na lidských životech, tak i na materiálu a dalších škod, zejména ekologických.

3.5.4. Fyzická bezpečnost KI

Náklady na systémy fyzické bezpečnosti celosvětově stoupají a tento trend se nevyhne ani energetice. Nové systémy jsou složitější, integrují v sobě několik dříve samostatných systémů, používají nejnovější a tedy i nejdražší technologie. Neustále se vyvíjejí a zdokonalují, aby pružně reagovaly na zjištěné nedostatky. Z toho vyplývá, že náklady na jejich provoz, modernizaci, s tím související kontinuálně probíhající školení obsluhujícího personálu, neustále rostou.

Můžeme konstatovat, že zavádění nových technologií v oblasti fyzické bezpečnosti se projeví v koncových cenách energií.

4. Mezinárodní spolupráce pro VaVaI

4.1. Analýza současného stavu a návrh opatření

Z hlediska mezinárodní spolupráce v oblasti VaVaI jsou aktivity v ČR řízeny cestou MŠMT, Možnosti spolupráce jsou rozděleny do následujících mezinárodních programů:

- S povinnou národní účastí
    - Cestou MŠMT
        - Rámcový program ES (FP 7, HORIZON 2020)
        - COST
        - Společné technologické iniciativy (programy ENIAC a ARTEMIS)
        - EDA (nyní pozastaveno financování nových projektů)

- S možností přímých dotací z různých institucí EU
    - TEN-E Trans-European Energy Network (DG Energy)
        - elektrické a plynové sítě
        - definované priority
    - Prevention, Preparedness and Consequence Management of Terrorism and other Security-related risks (DG Home Affairs)
        - non-profit projekty
        - 140 mil EUR, 2007-2013, max. dva roky
        - až 90% kofinancování (odpadá problém s MŠMT)
        - priority 2012:
            - Implementace směrnice 2008/114/EC (!)
            - CIIP Action Plan
            - technologický rozvoj v oblasti bezpečnosti sítí kritické energetické infrastruktury
    - SET plan (plán na podporu rozvoje strategických energetických technologií) cestou jeho iniciativ s alternativními způsoby financování:
        - Evropská průmyslová iniciativa (EII) – pro větrnou a solární energii, biomasu, jadernou energii, technologii CCS (zachycování a ukládání emisí CO2) a přenosové sítě
        - Evropská aliance pro výzkum v energetice (EERA) – sdružení významných výzkumných institucí, které mají koordinovat svůj

výzkum v oblasti energetiky a realizovat společné výzkumné programy – vyhlášené ve 2011:

- Chytrá města (Smart Cities), v rámci kterého se angažuje 60 institucí ze 14 evropských zemí
- Palivové články a vodík (17 institucí z 11 zemí)
- Ukládání energie (26 institucí z 12 zemí)
- AMPEA – pokročilé materiály a procesy pro aplikace v energetice (24 institucí z 10 zemí)

Návrh opatření:

- Sledovat a aktivně se účastnit jednání o změnách v systému podpory mezinárodní spolupráce ve VaVaI.
- Vyčlenit financování projektů EDA z kapitoly MŠMT (financovat samostatně nebo vrátit zpět do podřízenosti MO).
- Využívat v maximální možné míře výzkumných kapacit nově vzniklých výzkumných center v akademické sféře, která nabízejí špičkové technologické vybavení (zpravidla budou dokončena a dovybavena do konce roku 2012). Jedná se zejména o možnost využití jejich personálních kapacit a osobních vazeb na zahraniční akademická pracoviště.

4.2. Napojení na struktury EU

V návaznosti na kapitolu 1. Úvod a základní dokumenty EK, jež byly publikovány, nebo jsou ve fázi předložení a následné realizace provádí EK konkrétní činnosti pro jejich naplňování. 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 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. Ve skupině ERNCIP Industrial Automated Control Systems and Smart Grids Thematic Group, která má do konce roku předložit EK první dílčí doporučení jak postupovat v uvedené problematice, zejména s ohledem na vytváření norem a standardů a nových technologických aplikací je zástupce TPEB. ERNCIP je poskytnout rámec, v němž experimentální zařízení a laboratoře budou sdílet znalosti a zkušenosti s cílem harmonizovat zkušební protokoly v celé Evropě, což povede k lepší ochraně kritických infrastruktur před všemi typy hrozeb a nebezpečí.

Posláním ERNCIP je podporovat vznik inovačních, kvalifikovaných, efektivních a konkurenceschopných bezpečnostních řešení, a to prostřednictvím sítě evropských experimentálních laboratoří a testovacích zařízení.

ERNCIP je řešením pro chybějící sít´ 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.

První setkání skupiny se konalo v únoru 2012. Zde byla vymezena činnost, která se zaměřila na vytváření komunikace mezi všemi hlavními výzkumnými laboratořemi a testovacími zařízeními v EU a definování priorit. Jedná se o:

- Vytvoření distribuované databáze výsledků testů;
- Normy, protokoly a kritéria pro kvalifikaci infrastruktury výzkumu a technologického rozvoje;
- Posílení lidských zdrojů vzdělávání;
- Koordinace a spolupráce národních, evropských a mezinárodní souvisejících iniciativ.

Jednotlivé pracovní skupiny se schází pravidelně jednou za pět měsíců, mezitím spolu komunikují a předávají si výstupy své činnosti, tak jak si ji naplánovali během setkání.

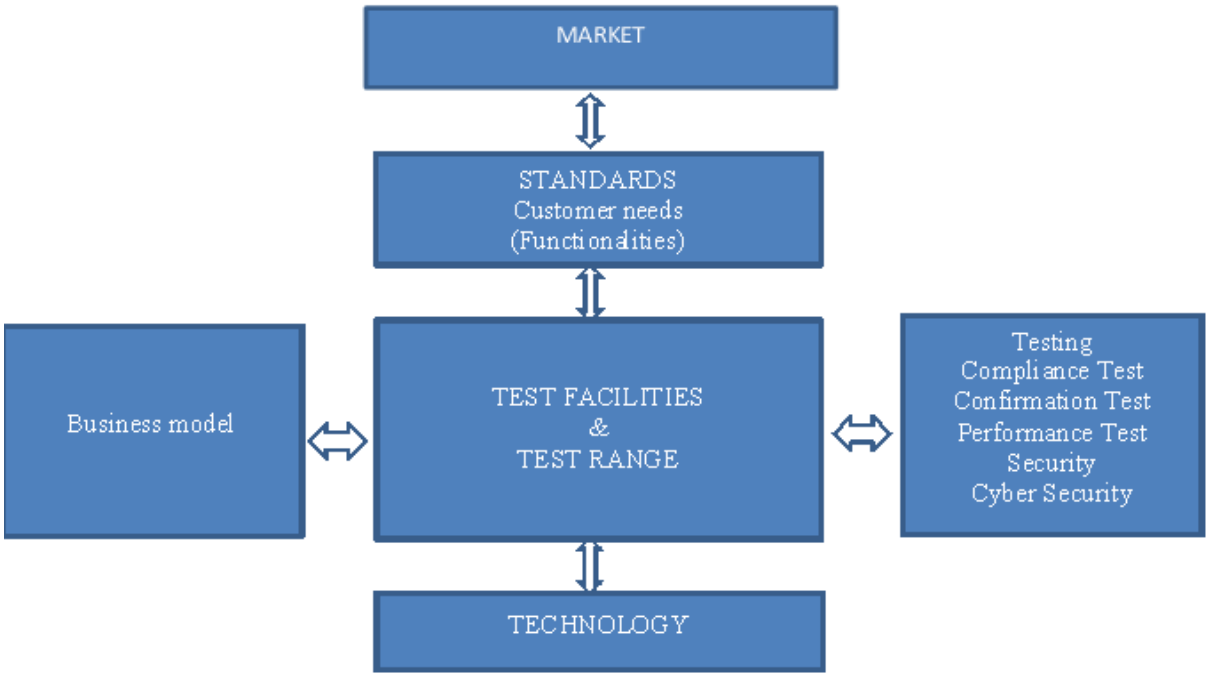
Poslední jednání **3rd ERNCIP CIIP SCADA – Integrated Control Systems a SmartGrids** se uskutečnilo dne 6.7.2012 a projednalo následující body. Současně uložilo členům rozpracovat tuto problematiku do příštího setkání plánovaného na podzim 2012.

Byla presentována spolupráce s NICE (National Initiative on Cyber Education – USA) s výhledem společných aktivit (souvisí s níže uvedenými činnostmi), které se budou presentovat na první konferenci ERNCIP 13 – 13 12. 2012 v JRC Ispra.

Byly vyhodnoceny informace, které se vyměnily s ostatními pracovními skupinami a organizacemi v rámci EK s ohledem na připravovanou legislativu a projekty pro Ochranu Kritické Infrastruktury EU. (ENISA, EOS, etc.).

Skupina pracuje na následujících okruzích problematiky:

- Analýza existujících standardů Ochrany kritické infrastruktury (OKI)
- Laboratoře
    - Co by měly splňovat – akreditace, technologie, postupy
    - Co se má testovat (compliance test; confirmation test, performance test; security test; cyber test, atd.)
    - Jak by měly být využívány/resp. vzájemně spolupracovat
    - Kdo je konečný uživatel (vendor, integrator, system provider, atd.)
- Vytvoření obchodního modelu



Obr. 3 Business model

Další jednání této skupiny za účasti zástupce TPEB se uskuteční na podzim 2012. Termín se upřesňuje.

15.10.2012 se bude v Amsterdamu konat v konference „ Building a Resilient Digital Society“ za účasti zástupců EK, ENISA, GŘ Vnitro a zástupců amerických institucí.

12. – 13.12.2012 se bude konat 1. Konference ERNCIP v Ispra, která by měla zhodnotit dosavadní práci jednotlivých skupin a potvrdit plán činnosti na příští období.

Účast v platformě úřadu EK CEN/CENELEC „Koordinační skupina kybernetická bezpečnost“ (Cyber Security Coordination Group CSCG)

EK pověřila svým mandátem M/487 standardizační úřad CEN/CENELEC analýzou 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 zabývají standardizací. Problematika norem není postižena vůbec.

Zmíněná analýza uvádí mezi doporučenými prioritami, které by měly být standardizovány mimo jiné:

• Obnovení bezpečnosti a ochrany v případě krize - připravenost, plánování a reakce

• Obecná koordinace bezpečnostních norem

• Ochrana osob a zařízení

• Podpora bezpečnosti průmyslu v EU

• Zjednodušení harmonizace bezpečnostních politik EU

Tyto priority mají být rozpracovány a předloženy EK do konce 2012.Následně bude vypracován plán priorit EK pro druhou fázi 2012 - 2014.

V rámci uvedeného procesu TPEB spolupracuje 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.

CEN Technický výbor schválil vytvoření skupiny Cyber Security Coordination Group - CSCG za účasti CEN, CENELEC a ETSI v únoru 2012 a přizval k této spolupráci národní standardizační autority a zástupce odborné veřejnosti států.

Rozsah činnosti a cíle CSCS pro období do roku 2014:

- poskytnout strategické poradenství pro technické výbory CEN, CENELEC a ETSI
- rozvíjet gap analýzu evropských a mezinárodních standardů pro kybernetickou bezpečnost
- definovat společné evropské požadavky pro evropské a mezinárodní standardy pro kybernetickou bezpečnost
- vytvoření evropského plánu na sjednocení kybernetické bezpečnosti
- působit jako kontaktní místo pro všechny otázky, institucí EU, týkající se normalizace kybernetické bezpečnosti
- navrhnou společné americké a evropské strategii pro vytvoření rámce mezinárodních standardů v oblasti kybernetické bezpečnosti
- posílit koordinaci evropských aktivit v ISO a IEC norem výbory s cílem provádění této společné transatlantické strategii

Další schůzka této pracovní skupiny by se měla konat na podzim 2012.

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

TPEB dlouhodobě spolupracuje s evropskou institucí European Organisation on Security (EOS), která je bruselskou platformou sjednocující 38 špičkových výzkumných ústavů, firem a institucí zabývajících se otázkami bezpečnosti. Problematika, ve které spolupracuje, je zaměřena na otázky energetické a kybernetické bezpečnosti v souvislosti s přípravou pokračování Bílé knihy „Bezpečnost energetické infrastruktury" a „Postupy pro implementaci strategie evropské kybernetické bezpečnosti". Tyto dokumenty by měly být novelizovány a rozpracovány v průběhu 2013 a 2014. Zde vidíme velkou příležitost pro prosazování národních zájmů ve spojitosti s připravovanými technologiemi v oblasti energetiky a kybernetiky.

Spolupráce s DG Joint Research Centre

TPEB spolupracuje s Directorat General Joint Research Centre (DGJRC) – Institutem pro ochranu obyvatelstva v Ispra (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 o získávání informací, které souvisí s aktivitami ve výše uvedených poradních orgánech, o možnosti je připomínkovat, komentovat a spolupodílet se na jejich dalším řešení.

Spolupráce v 7. RP a programu Horizon 2020

TPEB se v součinnosti s rakouským bmvit (Bundesministerium für Verkehr, Innovation und Technologie - Spolkové ministerstvo dopravy, inovací a technologií) bude účastnit výzvy 7. Rámcového programu Evropské komise v rámci mezinárodního projektu řešícího problematiku bezpečnosti inteligentních sítí (Smart Grids).

Spolupráce s ETP ARTEMIS a ENIAC

Společné technologické iniciativy (JTIs) podporují partnerství soukromého a veřejného sektoru v oblasti zabudovaných počítačových systémů (ARTEMIS) a nanoelektroniky (ENIAC) a umožňují kombinovat soukromé a veřejné zdroje financování (národní i evropské).

V současné době se VUT v Brně, zakládající člen TPEB, podílí na řešení mezinárodních projektů jako součást konsorcia řešitelů. Cílem je využít technologických příležitostí pro ostatní členy TPEB a jejich zapojení do společné technologické iniciativy podporované MŠMT ČR.

5. Lidské zdroje

5.1. Analýza současného stavu

V posledních dvaceti letech došlo k masovému rozšíření a používání nových digitálních technologií. Vyrostla generace počítačově zdatných uživatelů, kteří nové technologie navrhují, ovládají i využívají, ale zdaleka ne všichni si dostatečně uvědomují problematiku bezpečnosti. Zavádění nových technologií a služeb zpravidla předbíhá jejich zabezpečení, které se řeší až v průběhu plného provozu, často až ve chvíli poškození systému a následných finančních ztrát.

5.2. Návrh opatření

- Vytvoření systému osvěty a vzdělávání pro širokou veřejnost v oblasti kybernetické bezpečnost
- Prosazení problematiky kybernetické bezpečnosti do všech stupňů vzdělávání
- Vývoj systémů vzdělávání odborníků na kybernetickou bezpečnost
- Vývoj systému vzdělávání v oblasti kybernetické bezpečnosti pro orgány činné v trestním řízení
- Vývoj metodik a nástrojů pro forenzní analýzu kybernetických útoků

- Rozvoj vzdělávacích programů zaměřených na pracovníky, kteří jsou odpovědní za bezpečnost ICT infrastruktury. Programy zohlední nejenom technickou stránku věci, ale i obecné zásady bezpečnosti, protože řada útoků na ICT infrastrukturu je vedena s využitím metod sociálního inženýrství.

6. Možnosti VaVaI pro EB v ČR – podpora průmyslu

6.1. Analýza současného stavu

V současné době dochází k restrukturalizaci národních dotačních programů s cílem omezení jejich celkového počtu. Pro podporu průmyslu jsou nyní nejvhodnější programy:

- Resortní program výzkumu a vývoje TIP realizuje účelovou podporu průmyslového výzkumu a vývoje z prostředků státního rozpočtu České republiky určených na tento účel v rozpočtové kapitole Ministerstva průmyslu a obchodu. Doba trvání 2009 – 2017.
- Programu bezpečnostního výzkumu České republiky v letech 2010-2015 (BV II/2-VS) zaměřený na projekty aplikovaného výzkumu a experimentálního vývoje podporované z veřejných prostředků Ministerstva vnitra.

Oba programy v blízké době skončí a zatím není rozhodnuto, zda a za jakých podmínek budou pokračovat. Ostatní programy v rámci TAČR, GAČR a MPO-CzechInvest nejsou na podporu VaVaI v průmyslových podnicích jednoznačně nastaveny a jsou vesměs složitější jak po stránce administrativní, tak i finanční. Nejsou pro průmyslové subjekty příliš výhodné, proto je reálný předpoklad snížení celkové podpory plynoucí do průmyslu a v případě nízké procentuální úspěšnosti následné utlumení žádostí o podporu ze strany podniků. Dochází tak systematicky k redukci aplikovaného výzkumu.

6.2. Návrh opatření

Jsou zřetelné dvě oblasti, které pomáhají průmyslovým podnikům:

- Přímá finanční podpora
  - Podpora mezd zaměstnanců
  - Podpora investičních akcí
- Nepřímá podpora v zavedení nových standardů a postupů
  - Výrobcům eliminuje ztráty způsobené nesprávně orientovaným směrem vývoje nových produktů.
  - Umožní výrobcům připravit se na zavedení nových výrobků a tím získají nezanedbatelnou konkurenční výhodu.

Z tohoto hlediska by bylo vhodné:

- U realizovaných projektů zpracovat doporučení týkající se potřebných legislativních úprav nebo standardů.
- Zahájit specializované programy na podporu VaVaI v podnikatelské sféře zaměřené na udržitelnost výzkumných týmů formou podpory určené na krytí části jejich mzdových nákladů.
- Využívat v maximální míře nabídky strukturálních fondů na obnovu vnitropodnikové infrastruktury.

7. Možnosti financování pro VaVaI

7.1. Analýza současného stavu

Je zřejmé, že v současné době stagnace hospodářství nebudou investice do VaVaI ze strany podnikatelských subjektů narůstat, spíše naopak. Představa, že si privátní společnosti budou nechávat dělat vývoj na zakázku u specializovaných výzkumných a vývojových center z akademické sféry, není reálná bez finanční podpory z veřejných zdrojů.

7.2. Návrh opatření

- Národní programy
  - Zahájit nový víceletý národní program na podporu průmyslových subjektů, umožňující podporu projektů z oblasti energetické a kybernetické bezpečnosti
  - Vytvořit podmínky pro udržení nově vzniklých výzkumných center v rámci akademické sféry a vytvořit motivační program pro spolupráci průmyslových podniků s těmito výzkumnými centry.
- Mezinárodní programy
  - Strukturální fondy EU budou pokračovat v dalším cyklu po roce 2014 a nabízí finanční podporu investičním projektů v průmyslové sféře
  - HORIZON 2020 (FP 8) bude poskytovat finanční podporu průmyslovým subjektů i akademickým institucím na VaVaI v oblasti nových technologií. Vhodné by bylo vyčlenění určitých finančních prostředků jen pro projekty zaměřené na energetiku a její bezpečnost.
- Ostatní
  - Mezinárodní visegrádský fond – využít pro propagaci TPEB
    - byl založen 9. 6. 2000 za účelem podpory rozvoje a bližší spolupráce členských zemí. Členskými státy jsou: Česká republika, Maďarsko, Polsko a Slovensko (země V4). Fond je určen na podporu aktivit v těchto oblastech: kultura, věda a výzkum, vzdělávání, výměna mládeže, turismus a přeshraniční spolupráce. Nabízí se zejména využití příhraniční spolupráce, kde v oblasti energetických rozvodných sítí a produktovodů jsou mezinárodní vazby zcela zřejmé.
  - Ve specializovaných technologických oblastech je vhodné spolupracovat s EDA a ESA. Podmínkou účasti je však spoluúčast státu, která byla zmražena pro projekty EDA v roce 2011, a od tohoto roku nebylo možné účastnit se nových mezinárodních projektů. Pro účast českých firem v těchto projektech je nutné co nejdříve obnovit finanční podporu mezinárodních projektů organizovaných EDA.
  - Norské fondy a fondy EHP – zvýšit informovanost členů
    - Fondy jsou financovány ze strany Norska, Lichtenštejnska a Islandu a doplňují strukturální fondy EU. Povinnost přispívat na snižování regionálních a sociálních nerovností v EU vyplývá těmto zemím z účasti ve vnitřním trhu EU.
    - Instrumenty jsou určené pro patnáct kohezních zemí Unie včetně České republiky. Tyto velmi oblíbené nástroje jsou obnovovány v pravidelných pětiletých intervalech (nyní běží 2009 – 2014). Celkový objem financí určených pro ČR bude zhruba 3,3 miliardy Kč (131,8 milionu eur). Ačkoli i v budoucím období bude v některých případech potřeba pro předložení projektu najít partnera z dárcovské země, celková zodpovědnost za implementaci bude náležet české státní správě.

8. Závěr

Strategická výzkumná agenda TPEB podává stručný přehled o používaných technologiích v oblasti energetické a kybernetické bezpečnosti a jejich odhadovaný směr vývoje v následujících letech. Současně identifikuje oblasti, které se podílí na řešení této problematiky v současnosti a popisuje jejich možný podíl v budoucnosti.

SVA stručně mapuje aktuální situaci v ČR a navrhuje vhodná opatření z hlediska:

- Zvýšení všeobecného povědomí o nutnosti kybernetické bezpečnosti
- Kvalifikovaných lidských zdrojů
- Možností VaVaI v oblasti EB a jejich financování

Na základě Strategické výzkumné agendy byl zpracován Implementační akční plán obsahující základní kroky TPEB vedoucí ke zvýšení energetické a kybernetické bezpečnosti ČR.