Univerzita Pardubice
Fakulta elektrotechniky a informatiky

Návrh metodiky zaznamenávání činnosti na prvcích kritické informační infrastruktury v prostředí energetických systémů

Disertační práce

2020 Tomáš Svoboda

Prohlašuji:

Tuto práci jsem vypracoval samostatně. Veškeré literární prameny a informace, které jsem v práci využil, jsou uvedeny v seznamu použité literatury.

Byl jsem seznámen s tím, že se na moji práci vztahují práva a povinnosti vyplývající ze zákona č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon), ve znění pozdějších předpisů, zejména se skutečností, že Univerzita Pardubice má právo na uzavření licenční smlouvy o užití této práce jako školního díla podle § 60 odst. 1 autorského zákona, a s tím, že pokud dojde k užití této práce mnou nebo bude poskytnuta licence o užití jinému subjektu, je Univerzita Pardubice oprávněna ode mne požadovat přiměřený příspěvek na úhradu nákladů, které na vytvoření díla vynaložila, a to podle okolností až do jejich skutečné výše.

Beru na vědomí, že v souladu s § 47b zákona č. 111/1998 Sb., o vysokých školách a o změně a doplnění dalších zákonů (zákon o vysokých školách), ve znění pozdějších předpisů, a směrnicí Univerzity Pardubice č. 7/2019 Pravidla pro odevzdávání, zveřejňování a formální úpravu závěrečných prací, ve znění pozdějších dodatků, bude práce zveřejněna prostřednictvím Digitální knihovny Univerzity Pardubice.

V Pardubicích dne 1.7. 2020

Tomáš Svoboda

PODĚKOVÁNÍ

Na tomto místě bych rád poděkoval svému školiteli prof. Ing. Simeonu Karamazovi, Dr. za odborné metodické vedení v průběhu doktorského studia a Mgr. Josefu Horálkovi, Ph.D. za odborné konzultace a připomínky, které přispěly k tvorbě této práce.

Dále bych rád poděkoval své ženě Karolíně a dceři Nele za podporu při psaní této práce a vytvoření rodinného zázemí.

ANOTACE

Tato práce se zabývá problematikou návrhu nové metodiky pro řešení zaznamenávání činnosti na prvcích kritické informační infrastruktury v prostředí energetických systémů. Za účelem uvedení do problematiky jsou nejprve obecně představeny energetické systémy a jejich dílčí části. V práci je dále představen aktuální legislativní rámec a aktuální stav problematiky bezpečnosti energetických systémů v souvislosti s kybernetickými útoky, které byly v posledních letech cíleny právě na energetický sektor. Pro účel návrhu nové metodiky jsou dále analyzovány různé pohledy na efektivitu zajištění monitoringu činností a událostí s důrazem na zajištění efektivního přístupu k budování architektury bezpečnostních monitorovacích systémů, která je v souladu s potřebami společnosti či organizace. Na základě analýzy možných přístupů k budování architektury jsou dále představeny relevantní mezinárodně uznávané rámce (frameworky), které se zabývají uvedenou problematikou. Na základě stanovených kritérií, které reflektují specifické vlastnosti energetických systémů, je provedena komparativní analýza s cílem výběru relevantního rámce enterprise architektury, který tvoří základ nové metodiky. S využitím výstupů provedené komparativní analýzy je navržena nová metodika podporující návrh komplexní bezpečnostní infrastruktury, resp. bezpečnostního monitoringu, která plně reflektuje požadavky pro zaznamenávání činnosti na prvcích kritické informační infrastruktury v prostředí energetických systémů.

KLÍČOVÁ SLOVA

Energetika, průmyslové řídicí systémy, zaznamenávání činností, kritická informační infrastruktura, kybernetická bezpečnost, kybernetický útok, událost, incident, enterprise architektura, rámec, metodika, TOGAF

TITLE

Design of new methodology for recording activity in critical information infrastructure elements in the environment of energy systems

ANNOTATION

This thesis deals with the design of a new methodology for recording activity on critical information infrastructure elements in the environment of energy systems. In order to introduce the issue, energy systems and their sub-parts are described in general first. Next, the current legislative framework and the current state of the issue of the safety of energy systems in connection with cyberattacks that have lately been targeted specifically at the energy sector

are introduced. For the purpose of designing the new methodology, different perspectives of the efficiency of ensuring monitoring activities and events with emphasis on ensuring an effective approach to building a security monitoring system architecture that is in line with the needs of companies or organizations are then analysed. Based on the analysis of possible approaches to building architecture, relevant internationally recognized frameworks that deal with said issue are also introduced. Based on established criteria reflecting specific properties of energy systems, a comparative analysis is performed with the aim to choose a relevant framework of enterprise architecture, which forms the basis of the new methodology. Using the outputs of the preformed comparative analysis, a new methodology supporting the design of a comprehensive security infrastructure, or rather security monitoring, which fully reflects the requirements for recording activities on critical information infrastructure elements in environment of energy systems, is proposed. The newly proposed methodology is the main goal and output of this work.

KEYWORDS

Energy sector, industrial control systems, logging, critical information infrastructure, cybersecurity, cyberattack, event, incident, enterprise architecture, framework, methodology

OBSAH

SEZNAM OBRÁZKŮ

SEZNAM TABULEK

SEZNAM ZKRATEK

ACL	Access control list
ADU	Application data unit
ARIS	Architecture of Integrated Information Systems
ASDU	Application service data unit
ATM	Asynchronous transfer mode
BPM	Business Process Model
BPMN	Business Process Model Notation
CAPEX	Capital Expenditures
COBIT	Control Objectives for Information and related Technology
CRC	Cyclic Redundancy Check
ČSN	Česká technická norma
ČSRES	České sdružení regulovaných elektroenergetických společností
DCE	Data communications equipment
DDoS	Distributed denial of service
DLP	Data leak prevention
DoDAF	Department of Defense Architecture Framework
DTE	Data terminal equipment
DCS	Distributed control system
FEA	Federal Enterprise Architecture
FEAF	Federal Enterprise Architecture Framework
GDPR	General Data Protection Regulation

GOOSE	Generic object oriented substation event
GPRS	General Packet Radio Service
GSM	Groupe Spécial Mobile
GSSE	Generic Substation State Events
HA	High-availability
HIPPA	Health Insurance Portability and Accountability Act
HMI	Human Machine Interface
HW	Hardware
IEEE	Institute of Electrical and Electronics Engineers
IEC	International Electrotechnical Commission
IED	Intelligent electronic device
ICS	Industrial control systems
IDS	Intrusion detection system
IP	Internet protocol
IPS	Intrusion prevention system
IT	Information technology
IS	Informační systém
ITIL	Information Technology Infrastructure Library
ISDN	Integrated Services Digital Network
kB	Kilobyte
MODAF	Ministry of Defence Architecture Framework
MTU	Master terminal unit
MS	Milisekunda

MW	Megawatt
NIST	National Institute of Standards and Technology
NUKIB	Národní úřad pro kybernetickou a informační bezpečnost
OPEX	Operational Expenditures
PCE	Process control environment
PC	Personal computer
PCI/DSS	Payment Card Industry Data Security Standard
PDU	Protocol data unit
PLC	Programmable logic controller
SCL	Structured Control Language
SIEM	Security information and event management
SW	Software
RTU	Remote terminal unit
SCADA	Supervisory Control And Data Acquisition
TCP/IP	Transport communication protocol/Internet protocol
TOGAF	The Open Group Architecture Framework
UML	Unified Modeling Language
USB	Universal serial bus
USD	United States Dollar
VoKB	Vyhláška o kybernetické bezpečnosti
VN	Vysoké napětí
VPN	Virtual Private Network
VVN	Velmi vysoké napětí

WI-FI	Wireless Fidelity
XML	Extensible Markup Language
ZoKB	Zákon o kybernetické bezpečnosti

ÚVOD

Elektrická energie je v současné době považována za základní složku moderní společnosti, kdy spolehlivost výroby, přenosu a distribuce elektrické energie má v současné době dopady nejen v sociálním, ale také ekonomickém rozvoji jednotlivých národů. Spotřeba elektrické energie a ekonomický růst jsou dva faktory, které se v přímé úměře ovlivňují. Zajištění poskytování elektrické energie v režimu 24 hodin denně, 7 dní v týdnu, 365 dní v roce přispívá k rozvoji ekonomiky státu jako celku. Pro zajištění dodávek elektrické energie od místa její výroby až ke konečnému spotřebiteli je využívána elektrizační soustava. Důležitým faktorem jsou technické možnosti řízení elektrizační soustavy. Prostřednictvím řízení elektrizační soustavy je udržována rovnováha mezi množstvím vyrobené a spotřebované elektrické energie. V rámci elektrizační soustavy jsou využívány různé napěťové hladiny tak, aby byla zajištěna minimalizace ztrát při přenosu elektrické energie na dlouhé vzdálenosti.

Ke změnám napěťové hladiny dochází v elektrických stanicích, které jsou v České republice řízeny z centrálních dispečinků elektrizační soustavy, podle příslušnosti k dané přenosové či distribuční soustavě. Pro účely řízení elektrických stanic a zajištění stabilních dodávek elektrické energie jsou využívány průmyslové řídicí systémy, průmyslové komunikace a průmyslové komunikační protokoly. Součástí průmyslových řídicích systémů jsou rovněž klasické IT systémy, které tvoří podpůrnou součást pro řízení elektrizační sítě. V odborných publikacích a v rámci odborné veřejnosti je pojem elektrická stanice velice často synonymem pro pojmy transformovna, resp. rozvodna elektrické energie. Stejně tak jsou v rámci této práce chápány tyto pojmy jako synonymum.

Energetické systémy, resp. průmyslové řídicí systémy byly historicky koncipovány jako uzavřené systémy využívající proprietární komunikační protokoly a absence komunikačního propojení do vnějšího světa. S postupným vývojem nových komunikačních technologií došlo k nahrazování proprietárních komunikačních protokolů standardizovanými řešeními (IP protokol, Ethernet). Využití standardizovaných komunikačních protokolů zároveň umožnilo integraci průmyslových řídicích systémů s informačními systémy, za účelem např. získávání dat týkající se poruch nebo dat o provozu elektrizační soustavy. Jednalo se o velmi významnou změnu, kdy se průmyslové řídicí systémy začaly podobat podnikovým IT systémům, které využívají standardizované komunikační technologie (Cook et al., 2017, s. 467). Negativním dopadem nasazení standardizovaných řešení je zvyšující se míra zranitelností energetických systémů, které souvisí s jejich větší otevřeností

do vnějšího světa. Bezpečnostní řešení tedy nelze již navrhovat pouze pro část týkající se pouze IT systémů, ale je nutné brát v potaz energetický systém jako celek a pružně reagovat zlepšováním bezpečnosti v rámci dynamického prostředí, ve kterém tyto systémy fungují. (Technology assesments, 2015, s. 3)

V uplynulých několika letech došlo ve světě k významným kybernetickým útokům, které byly cíleny na energetické systémy. Energetické systémy jsou koncipovány jako soubor systémů měřicí, ochranné, řídicí, zabezpečovací, informační a telekomunikační techniky, které jsou tvořeny zařízeními typu PLC, IED, RTU, HMI, SCADA a dohledovými pracovními stanicemi včetně jejich vzájemného komunikačního propojení. (Lim a Sidhu, 2016, s. 157).

Nárůst kybernetických útoků v prostředí energetiky lze sledovat od roku 2010. Propracovanost a efektivita kybernetických útoků se v posledních letech neustále zvyšuje. Veřejnosti nejznámější je především kybernetický útok cílený na Ukrajinskou energetiku, kdy v prosinci roku 2015 došlo vlivem kybernetického útoku k výpadku energetické sítě a přerušení dodávky elektrické energie pro sedm set tisíc lidí. Kybernetické útoky cílené na energetické systémy zahrnují získání přístupu nejen k citlivým informacím, které mohou obsahovat informace o topologii energetické sítě, případně parametrizačních dat pro ovládací prvky infrastruktury, ale především získání samotného přístupu k prvkům infrastruktury a jejich následnou kompromitaci prostřednictvím škodlivých kódů nebo ovládacích příkazů. (Rexhepi, 2017, s. 421) Dopady, které mají kybernetické útoky na energetické systémy lze spatřovat především v ekonomických ztrátách, poškození reputace společnosti zajišťující dodávky elektrické energie a v extrémním případě také ve ztrátách na lidských životech.

Zvyšující se počet kybernetických útoků cílených na subjekty působící v oblasti energetiky vedl ke změně vnímání bezpečnosti energetických systémů. Nezbytným předpokladem pro zavedení komplexních bezpečnostních opatření je existence národní, případně nadnárodní legislativy, která jasným způsobem definuje pravidla pro zabezpečení energetických, resp. průmyslových řídicích systémů. Česká republika byla jednou z prvních zemí v Evropě, která zakotvila ve svém právním řádu Zákon o kybernetické bezpečnosti s účinností od 1. 1. 2015. Předmětem úpravy zákona o kybernetické bezpečnosti je úprava práv a povinností osob a působnost a pravomoci orgánů veřejné moci v oblasti kybernetické bezpečnosti. (Zákon o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti), 2014). Detailní požadavky na implementaci organizačních a technických bezpečnostních opatření stanovuje příslušná prováděcí vyhláška č. 316/2014 Sb.,

resp. její novelizace č. 82/2018 Sb. (Vyhláška o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (vyhláška o kybernetické bezpečnosti), 2018). Dle zákona o kybernetické bezpečnosti a příslušných prováděcích vyhlášek jsou zejména energetické systémy, které slouží pro řízení přenosové soustavy a distribuční soustavy včetně elektrických stanic a vedení o napětí 110 kV prvky kritické, resp. kritické informační infrastruktury státu a požadavky na bezpečnost těchto systémů jsou regulovány zákonem o kybernetické bezpečnosti.

Nutnost regulace subjektů, které provozují systémy pro zajištění klíčových služeb společnosti si plně uvědomila i Evropská unie. 6. července 2016 byla přijata směrnice Evropského parlamentu a Rady (EU) č. 2016/1148 o opatřeních k zajištění vysoké společné úrovně bezpečnosti sítí a informačních systémů v Unii (směrnice NIS). Zákon o kybernetické bezpečnosti a směrnice NIS se v mnoha oblastech překrývají ale zároveň směrnice NIS některé oblasti zákona rozšiřuje. Společnosti působící v oblasti energetiky jsou dle zákona o kybernetické bezpečnosti a směrnice NIS regulovaným subjektem odpovědným za implementaci zákona a směrnice v rámci své působnosti.

Na problematiku bezpečnosti energetických systémů lze rovněž nahlížet z hlediska jejich implementace, provozování, zabezpečení a specifických požadavků souvisejících s jejich implementací v porovnání s implementací a provozem standardních IT systémů. Klíčovými vlastnostmi a požadavky kladenými na energetické systémy jsou požadavky na řízení v reálném čase, geografická rozlehlost systému, hierarchický design systému, komplexita ovládání systému, dostupnost systému, identifikace dopadů selhání systému a zejména bezpečnost systému. (Stouffer, Falco a Scarfone, 2015, s. 2-4–2-5).

Vzhledem k tomu, že energetické systémy reprezentují velké množství technologií a možných přístupů k implementaci bezpečnostních požadavků na ně kladené, je relevantní otázka, jaké přístupy, metody a postupy zvolit pro implementaci bezpečnostních řešení a zajistit tak efektivní monitoring činností a událostí v rozsáhlé architektuře a heterogennosti současných energetických systémů, které jsou určeny jako kritická informační infrastruktura. Systémy kritické informační infrastruktury musí být v souladu s příslušnými legislativními požadavky, které jsou reflektovány prostřednictvím organizačních a technických opatření. Jedná se zejména o legislativní požadavky reflektované zákonem o kybernetické bezpečnosti č. 181/2014 Sb. a příslušných prováděcích vyhlášek. Problematika bezpečnosti energetických

systémů zahrnuje různé technologické, manažerské a ekonomické aspekty. Tato práce se nezaměřuje na všechny uvedené aspekty a oblasti, které souvisí s problematikou bezpečnosti energetických systémů. Pro zájemce uveden seznam odborné literatury, která je relevantní pro jednotlivé oblasti přístupu k této problematice:

- **Architektura energetických systémů:** Stouffer, Falco a Scarfone, 2015; Vlček a Černoch, 2012; Tesařová, 2007; Fanny et al., 2015; Adepu, Mishra a Mathur, 2017; Teti et al., 2010; Yakimov a Iovev, 2017; Son et al., 2018; Moreira et al., 2016; Poudel, Ni a Malla, 2017; Hong a Liu, 2017.

- **Architektura a využití SCADA systémů:** Knapp a Broad, 2011; Ancillotti, Bruno a Conti, 2013; Osborne, 2013; Radvanovsky a Brodsky, 2016; Ejesh a Zhongling, 2017; Macaulay a Singer, 2012

- **Architektura a možnosti využití průmyslových komunikačních protokolů v energetice:** Stodůlka, 2012; Pal a Dash, 2015; Powell, 2013; Henning, 2016; Fernandes et al., 2016; Bermundes, 2016; Horálek a Soběslav, 2012; Pekárek, 2017; Han et al., 2014; Nazir, Patel a Patel, 2017; Rubio, Alcaraz a Lopez, 2017; Matoušek, 2017

- **Architektura elektrických stanic:** Kabovic, Kabovic a Celebic, 2014; Tesařík, 2014; Ding et al.,2018

- **Kybernetické útoky na energetické systémy**: Paolo Passeri, 2017; Technology assesment, 2015; Rexhepi, 2017; Lee, Assante a Conway, 2016; Holloway, 2015; Broad, Markoff a Sanger, 2011; Goldman, 2015; Ding et al.,2018; Knapp a Broad, 2011; Wu, Du a Wu, 2016; Takala, 2015; Perez a Prokupecz, 2016

- **Legislativa související s energetickými systémy v České republice:** Energetický zákon, 2000; Pravidla provozování distribuční soustavy, 2018; Vyhláška MPO o stavu nouze v elektroenergetice a o obsahových náležitostech havarijního plánu, 2010; Vyhláška o dispečerském řízení elektrizační soustavy a o předávání údajů pro dispečerské řízení, 2010.

- **Bezpečnostní legislativa validní pro energetické systémy:** Zákon o kybernetické bezpečnosti 2014, Vyhláška o kybernetické bezpečnosti, 2018; Škeřík, 2016; Computer Security Incident Handling Guide, 2012; Sennewald a Baillie, 2016; Conrad, Misenar

a Feldman, 2015; Barafort, Mesquida a Mas, 2017; Knapp a Langill, 2015; Roberts, 2016; CIP Standards, 2016; Schlegel, Obermeier a Schneider, 2017; Stouffer, Falco a Scarfone, 2015

- **Bezpečnost průmyslových řídících systémů:** Lee a Huba, 2014; Cook et al., 2017; Canto et al., 2015; Technology assesments, 2015; Stouffer, Falco a Scarfone, 2015; Eder-Neuhauser, 2017

- **Bezpečnost podpůrných IT systémů v energetice:** Moreira et al., 2016; Stouffer, Falco a Scarfone, 2015; Vaidya, Makrakis a Mouftah, 2013; Knapp a Broad, 2011

- **Komunikační sítě a protokoly energetických systémech:** Baldwin et al., 2015; Stouffer, Falco a Scarfone, 2015; Knapp a Broad, 2011; Boyer, 2016; Young, 2015; Maglaras et al., 2018; Vaidya, Makrakis a Mouftah, 2013; Ding et al.,2018

1 CÍLE A METODIKA DISERTAČNÍ PRÁCE

Vzhledem k faktu, že problematika energetických systémů a jejich bezpečnosti představuje velice širokou oblast, jak bylo uvedeno výše, nemůže tato práce pojmout všechny aspekty, související s touto problematikou. Práce je proto zaměřena na vybranou problematiku týkající se zabezpečení energetických systémů kritické informační infrastruktury, neboť tato oblast integruje organizační a zejména technická opatření dané legislativními požadavky, která jsou relevantní pro oblast energetických systémů. Energetické systémy jsou specifické vysokou mírou heterogenností využívaných technologií a současně geografickou rozsáhlostí. Návrh a implementace bezpečnostních systémů pro monitoring činností v takto heterogenním a rozsáhlém prostředí vyžaduje systematický přístup. Otázkou tedy je, jakým způsobem metodicky podpořit oblast návrhu a implementace těchto systémů v rozsáhlé architektuře energetických systémů. Nedílnou součástí návrhu je podpora opětovného využití získaných poznatků a nabytých znalostí v rámci projektu návrhu a implementace. Tyto principy tvoří základní stavební kameny, kterými se zabývá oblast podnikové (enterprise) architektury. Oblast návrhu a implementace podnikové (enterprise architektury) zahrnuje v současné době množství standardů a rámců, které se soustředí na problematiku efektivity implementace informačních technologií v organizaci (společnosti).

Autor práce aktuálně působí ve společnosti, která zajišťuje provozování distribuční soustavy na svěřeném území České republiky a je současně provozovatelem prvků kritické informační infrastruktury státu. Hlavní náplní práce autora je zajištění bezpečnostního dohledu těchto prvků včetně procesu návrhu a implementace bezpečnostních monitorovacích systémů. Z tohoto důvodu je pro něj téma práce velice aktuální, relevantní a využitelné v praxi.

1.1 Cíle disertační práce

Hlavním cílem disertační práce je vytvoření nové metodiky SEC-MON, která vytváří průnik mezi rámci pro návrh a implementaci rozsáhlých architektonických řešení v rámci enterprise architektury a specifickou oblastí problematiky bezpečnostních monitorovacích systémů sloužících pro zaznamenávání činnosti na prvcích kritické informační infrastruktury v prostředí energetických systémů. Přínosem metodiky je zejména vytvoření komplexního pohledu nad problematikou bezpečnostních monitorovacích systémů v kontextu enterprise architektury společnosti s vazbou na legislativní a regulatorní požadavky a současně požadavky byznysu. Sekundárně může navržená metodika sloužit jako vodítko pro zjednodušení implementace

bezpečnostních řešení prostřednictvím jejího využití ve všech projektech, které mají vazbu na kritickou informační infrastrukturu společnosti či organizace.

Za účelem naplnění hlavního cíle práce je nezbytným předpokladem splnění dílčích cílů, které dekomponují hlavní cíl práce, tvoří její obsah a zároveň otevírají otázky, které jsou využitelné v další oblasti výzkumu uvedené problematiky. Dílčí cíle disertační práce jsou následující:

- Vymezit základní terminologii, představit komplexní architekturu energetických systémů s důrazem na její heterogennost, komponent energetických, resp. energetických řídicích systémů a principů komunikace včetně představení komunikačních protokolů.
- Analyzovat aktuální stav problematiky bezpečnosti energetických systémů ve vztahu k plnění legislativních požadavků, které jsou na tyto systémy kladeny s důrazem na zajištění plnění požadavků týkajících se zaznamenávání činností a událostí v energetických systémech.
- Na základě výše uvedené analýzy provést analýzu jednotlivých pohledů s důrazem na efektivní návrh, implementaci, správu a servis bezpečnostní infrastruktury, která ve společnosti či organizaci zajišťuje plnění požadavků týkajících se zaznamenávání činností a událostí v energetických systémech.
- S využitím výsledků předchozí analýzy pohledů provést komparativní analýzu rámců enterprise architektury s cílem výběru konkrétního rámce, který bude tvořit určující rámec pro nově vytvořenou metodiku.
- Na základě určujícího rámce vytvořit metodiku pro návrh komplexní bezpečnostní infrastruktury v prostředí kritické informační infrastruktury energetických systémů. Nezbytnou součástí metodiky je stanovení jejího obsahu a struktury, která reflektuje určující rámec a zejména vstupů a výstupů v jednotlivých fází.
- Ověřit vytvořenou metodiku.

Cílem této práce není detailní představení konkrétních technologií energetických systémů a bezpečnostních řešení, jejich implementace a provozování. Současně není cílem práce detailní pohled na koncepty architektury energetických systémů. Vytvoření takové práce by bylo velice obtížné z hlediska různorodosti technologií, přístupů a standardů které se v této oblasti využívají. Zároveň by taková práce byla velice rozsáhlá.

1.2 Terminologie

Nezbytným předpokladem pro tuto disertační práci je jasné vymezení terminologie. Jak bylo uvedeno, cílem disertační práce je vytvoření nové metodiky. Z tohoto důvodu je vhodné vysvětlit základní pojmy, které souvisí s pojmem metodika.

1.2.1 Metodologie

Ochrana (2019) definuje metodologii jako nauku o metodách, které mohou být využívány ve vědecké práci. Metodologie může být zároveň chápána jako souhrn metod zabývajících se určitým vědním oborem včetně definice základních paradigmat a společného jazyka.

V současné odborné literatuře je pojem metodologie velmi často chápán jako synonymum pojmu metodika nebo metoda. Toto chápání je ve velké míře podpořeno cizojazyčnými, zejména anglickými informačními zdroji, ve kterých se uvádí pojem „methodology“ a tento je chápán jako metodika.

1.2.2 Metodika

Dle Soběslava (2012, s. 110) je metodika obecně chápána jako souhrn doporučených praktik, postupů, pravidel, etap, metod, technik a dokumentů, které definují předmět a způsob provádění určité činnosti. Ochrana (2019) chápe metodiku jako prostředek k dosažení výzkumného cíle. Stejně jako Ochrana (2019) reflektuje pojem metodika i Sebera (2012) a Molnár (2012, s. 38).

1.2.3 Metoda

Jedná se o teoreticko-praktické schéma určující soustavný postup provádění odborné činnosti (Molnár, 2012, s. 38). Odborná činnost není v ideálním případě závislá na schopnostech toho, kdo ji provádí (Sebera, 2012; Ochrana, 2019).

1.2.4 Technika

Detailní postup, který specifikuje konkrétní kroky pro dosažení výsledku. Součástí detailního postupu je i definice potřebných nástrojů pro jednotlivé kroky a určení způsobu jejich použití. Nástroj tvoří prostředek, s jehož pomocí můžeme v rámci techniky dosáhnout určených cílů. (Molnár, 2012, s. 38).

1.3 Metodologie a struktura práce

Disertační práce obsahuje z metodologického pohledu několik analytických metod, zejména srovnávací, resp. komparativní, funkční a multikriteriální analýzu. Uvedené metody slouží k dekompozici a rozboru uvedené problematiky, na kterou se disertační práce zaměřuje.

Citační norma je založena na české citační normě ČSN ISO 690:2011 s využitím tzv. harvardského citačního stylu, který je založen na uvedení autora a roku publikace, případně i rozsahu stran, které jsou citovány (pokud je údaj k dispozici).

Vzhledem k dekompozici hlavního cíle disertační práce do několika dílčích cílů je disertační práce rozdělena do 8 hlavních kapitol a dále úvodu, závěru a seznamu využité literatury. V úvodu práce jsou vymezeny možné přístupy k řešené problematice a zaměření samotné disertační práce.

1. kapitola představuje cíle práce, motivaci autora ve vztahu k řešené problematice, využité metody a strukturu práce.

2. Součástí druhé kapitoly je představení principů, architektury a analýzy energetických systémů a jejich komponent, včetně komunikace a komunikačních protokolů, které jsou specifické pro energetické systémy.

3. Třetí kapitola se zaměřuje na analýzu bezpečnosti energetických systémů s důrazem na nutnost řešení bezpečnosti energetických systémů v kontextu celosvětově narůstajícího počtu kybernetických útoků v oblasti energetiky. Současně je ve třetí kapitole analyzována národní a nadnárodní legislativa, která se zaměřuje na problematiku bezpečnosti energetických systémů.

Součástí 4. kapitoly je analýza problematiky návrhu systémů pro monitoring činností a událostí v energetických systémech na základě technického, ekonomického a manažerského pohledu.

V 5. kapitole jsou představeny pojmy enterprise architektura a příslušné frameworky (rámců), které jsou pro tento účel využitelné. Kapitola jako celek vychází z analýzy možných přístupů a pohledů k dané problematice, která byla provedena ve 4. kapitole.

V 6. kapitole je provedena analýza představených rámců prostřednictvím srovnávací, resp. komparativní analýzy s důrazem na jejich využití pro návrh architektury systémů bezpečnostního monitoringu v kontextu enterprise architektury s důrazem na specifika jejich využití v energetickém sektoru. Na základě výstupů z provedené analýzy je v rámci 6. kapitoly vybrán určující rámec enterprise architektury, který dále slouží jako referenční rámec pro vytvoření nové metodiky.

7. kapitola představuje návrh zcela nové metodiky, která poskytuje systematický pohled pro návrh systémů bezpečnostního monitoringu v oblasti kritické informační infrastruktury

v prostředí energetických systémů. Metodika vychází z určujícího rámce, který byl vybrán v kapitole 6.

8. kapitola obsahuje zhodnocení navržené metodiky s přihlédnutím k jejím klíčovým vlastnostem a oblastem využití.

2 ENERGETICKÉ ŘÍDICÍ SYSTÉMY

Obecné definování energetických systémů je úzce spojeno s geografickým nasazením a zvyklostmi z oblasti energetiky. Z toho plyne, že jednoznačná definice či určení není jednoduše přenositelné a oblast působení je vždy nutné jasně definovat pro daný účel a oblast. V prostředí České republiky je tedy nutné se orientovat na základě platné legislativy a veřejně dostupných předpisů a norem subjektů působících v oblasti energetiky. Pro téma této práce jsou pak zejména relevantní tyto právní předpisy:

- Zákon č. 458/2000 Sb. zákon o podmínkách podnikání a o výkonu státní správy v energetických odvětvích a o změně některých zákonů (energetický zákon).
- Zákon č. 181/2014 Sb. zákon o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti), ve znění pozdějších předpisů.
- Zákon č. 240/2000 Sb. zákon o krizovém řízení a o změně některých zákonů (krizový zákon), ve znění pozdějších předpisů
- Vyhláška č. 82/2018 Sb. vyhláška o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (vyhláška o kybernetické bezpečnosti).
- Pravidla provozování distribuční soustavy (PPDS) 2018.
- Vyhláška MPO č. 80/2010 Sb. ze dne 18. 3. 2010 Sb. o stavu nouze v elektroenergetice a o obsahových náležitostech havarijního plánu.
- Vyhláška MPO č. 79/2010 Sb. ze dne 18. 3. 2010 Sb. o dispečerském řízení elektrizační soustavy a o předávání údajů pro dispečerské řízení.

Na základě výše uvedeného, lze energetické systémy definovat jako komplex systémů, které zajišťují přenos a distribuci elektrické energie, a to včetně informací pro řízení, parametrizaci a kontrolu stavu energetické soustavy. Dle §2 odstavce a) energetického zákona jsou nedílnou součástí energetických systémů tzv. technologické systémy, které je možné definovat jako zařízení systémů měřící, ochranné, řídicí, zabezpečovací, informační a telekomunikační techniky (dále jen systémy) sloužící výhradně k zajištění distribuce elektřiny a chodu distribuční soustavy v reálném čase. (Zákon č. 458/2000 Sb.: zákon o podmínkách podnikání

a o výkonu státní správy v energetických odvětvích a o změně některých zákonů (energetický zákon), 2000).

Součástí technologických systémů jsou i softwarové a hardwarové prostředky (včetně standardních IT prostředků) pro přímou nebo vzdálenou správu a zajištění provozu těchto systémů, prostředky pro přímý nebo vzdálený uživatelský přístup a prostředky pro zajištění bezpečnosti (fyzické, informační) technologických systémů. Součástí energetických systémů jako celku jsou mimo jiné:

- prvky energetické soustavy a dispečerských pracovišť přenosové a distribuční soustavy dle §26 energetického zákona,
- průmyslové řídicí systémy,
- komunikace a komunikační protokoly,
- podpůrné IT systémy.

Provoz, správa a rozvoj energetických, resp. technologických systémů je pak z důvodů jejich kritického nasazení regulován v souladu s §25a zákona 458/2000 Sb. ve znění zákona 211/2011 Sb., PPDS, zákona o kybernetické bezpečnosti 181/2014 Sb. a vyhlášky o kybernetické bezpečnosti 82/2018 Sb. (Zákon č. 458/2000 Sb. zákon o podmínkách podnikání a o výkonu státní správy v energetických odvětvích a o změně některých zákonů (energetický zákon), 2010; Zákon č. 181/2014 Sb. zákon o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti), 2014; Vyhláška č. 82/2018 Sb. vyhláška o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (vyhláška o kybernetické bezpečnosti), 2018)

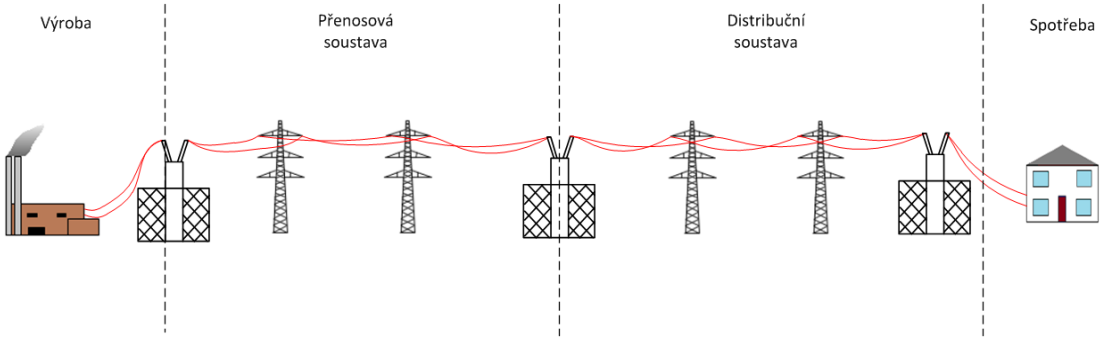
2.1 Prvky energetické soustavy

Prvky energetické soustavy tvoří podstatnou část energetických systémů. Pro vytvoření komplexního pohledu na problematiku energetických systémů jako celku budou proto prvky energetické soustavy krátce představeny.

Přenos elektrické energie od výrobce ke konečnému spotřebiteli je zajištěn prostřednictvím souboru zařízení elektrizační soustavy. Pojem elektrizační soustava je definován v §2, odstavec 2, písmeno a, bod č. 4, zákona č. 458/2000 Sb. energetického zákona jako: „*vzájemně propojený soubor zařízení pro výrobu, přenos, transformaci a distribuci elektřiny, včetně elektrických*

přípojek, přímých vedení, a systémy měřicí, ochranné, řídicí, zabezpečovací, informační a telekomunikační techniky, a to na území České republiky“.

Obrázek 1 schematicky znázorňuje prvky elektrizační soustavy, včetně jejich vzájemných vazeb.



Obrázek 1 - Obecné schéma elektrizační soustavy. Zdroj: upraveno dle Mission Support Center (2016, s. 8)

Proces výroby elektrické energie začíná v elektrárnách, které produkují elektrickou energii a za využití transformátorů ji transformují do přenosové soustavy. V průběhu transformace elektrické energie z výroby do přenosové soustavy dochází ke zvyšování napěťové hladiny na 400 kV z důvodu snižování ztrát elektrické energie v průběhu přenosu na velké vzdálenosti v rámci přenosové soustavy. Elektrárny v České republice se podle způsobu výroby elektrické energie rozlišují na elektrárny vodní, parní, jaderné, uhelné, solární, paroplynové, plynové, větrné a geotermální. (Vlček a Černoch, 2012, s. 318–319)

Přenosová soustava je v Českém právním řádu definována v §2, odstavec 2, písmeno a, bod č. 10 Energetického zákona jako: „*vzájemně propojený soubor vedení a zařízení 400 kV, 220 kV a vybraných vedení a zařízení 110 kV, uvedených v příloze Pravidel provozování přenosové soustavy, sloužící pro zajištění přenosu elektřiny pro celé území České republiky a propojení s elektrizačními soustavami sousedních států, včetně systémů měřicí, ochranné, řídicí, zabezpečovací, informační a telekomunikační techniky; přenosová soustava je zřizována a provozována ve veřejném zájmu*“. Provozovatel přenosové soustavy na území České republiky musí být dle energetického zákona držitelem licence na provozování přenosové soustavy. Provozovatelem přenosové soustavy na území České republiky, který zajišťuje propojení na přenosové soustavy sousedních zemí je v současné době společnost ČEPS, a. s. (ČEPS a. s. – O Společnosti) Společnost ČEPS provozuje v současné době 41 rozvoden, včetně 71 transformátorů, které v rozvodnách elektrické energie transformují napěťovou hladinu přenosové soustavy 400 kV a 220 kV na napěťovou hladinu 110 kV do distribuční soustavy.

Tesařová (2007, s. 11) definuje přenosovou soustavu jako síť, do které je elektrická energie přiváděna z elektráren a je dále s využitím transformoven (rozvoden) transformována do distribuční soustavy. Zároveň se sledují parametry optimálního rozložení výkonu v určité geografické oblasti, ve vztahu k vynaloženým nákladům na výrobu elektrické energie a její přenos do distribuční soustavy.

Distribuční soustava je dalším prvkem, který zajišťuje přenos elektřiny od výrobce, resp. z přenosové soustavy až ke konečnému spotřebiteli. Mezi konečné spotřebitele patří průmyslové podniky, nákupní centra, výrobní závody, domácnosti, atp. Distribuční soustava je v Českém právním řádu definována v §2, odstavec 2, písmeno a, bod č. 1 Energetického zákona jako: „*vzájemně propojený soubor vedení a zařízení o napětí 110 kV, s výjimkou vybraných vedení a zařízení o napětí 110 kV, která jsou součástí přenosové soustavy, a vedení a zařízení o napětí 0,4/0,23 kV, 1,5 kV, 3 kV, 6 kV, 10 kV, 22 kV, 25 kV nebo 35 kV sloužící k zajištění distribuce elektřiny na vymezeném území České republiky, včetně systémů měřicí, ochranné, řídicí, zabezpečovací, informační a telekomunikační techniky včetně elektrických přípojek ve vlastnictví provozovatele distribuční soustavy; distribuční soustava je zřizována a provozována ve veřejném zájmu*“ (Energetický zákon, 2009, s. 4471). Stejně jako v případě přenosové soustavy musí být i každý subjekt provozující distribuční soustavu na území České republiky, dle energetického zákona, držitelem licence na provozování distribuční soustavy.

Tesařová (2007, s. 11) definuje distribuční soustavu jako rozvodnou síť, která je schopna přivést elektrickou energii ke konečným spotřebitelům. Součástí distribuční soustavy mohou být připojované zdroje o malých výkonech. Jedná se především o malé vodní elektrárny a v dnešní době především solární elektrárny. Primárním zdrojem elektrické energie pro distribuční soustavu je přenosová soustava (E.ON Česká republika, s.r.o., 2017).

Držiteli licence na provozování distribuční soustavy na území České republiky jsou v současné době společnosti ČEZ Distribuce, a. s., E.ON Distribuce, a. s. a PREdistribuce, a. s.

2.2 Průmyslové řídicí systémy

V současné době obsahují elektrické stanice systémy měřicí, ochranné, řídicí, zabezpečovací, informační a telekomunikační techniky za účelem parametrizace ochran a automatizace. Moderní systémy automatizace elektrické stanice, vycházejí z požadavku získat a využívat komplexních dat z používaných a nasazených Intelligent Electronic Device (dále jen IED) zařízení (Přenosová a distribuční soustava 1. Část – vedení velmi vysokého napětí (vvn), 2017).

Významným požadavkem na systémy automatizace rozvoden je zajištění autonomního fungování nejdůležitějších prvků a ochran silových prvků elektrické stanice, zabránění chybným manipulacím, které by mohly vést k poškození zdraví osob či majetku a zabránění chybnému působení ochran vedoucím ke zbytečnému přerušení dodávky elektrické energie do rozvodné sítě a narušení funkcionality celého systému. (Lim a Sidhu, 2016, s. 157) V současné době se prosazuje koncept systémů automatizace rozvoden postavený na základě mezinárodního standardu IEC 61850. (Fanny et al., 2015, s. 42)

Hlavní částí systému elektrické stanice jsou průmyslové řídicí systémy zahrnující sběrnice IEC 61850 a IED, komunikační brány RTU zajišťující spojení mezi nadřazenými řídicími centry a rozvodnou a datové přenosové cesty na nadřazená řídicí centra. (Giannakis et al., 2013, s. 110).

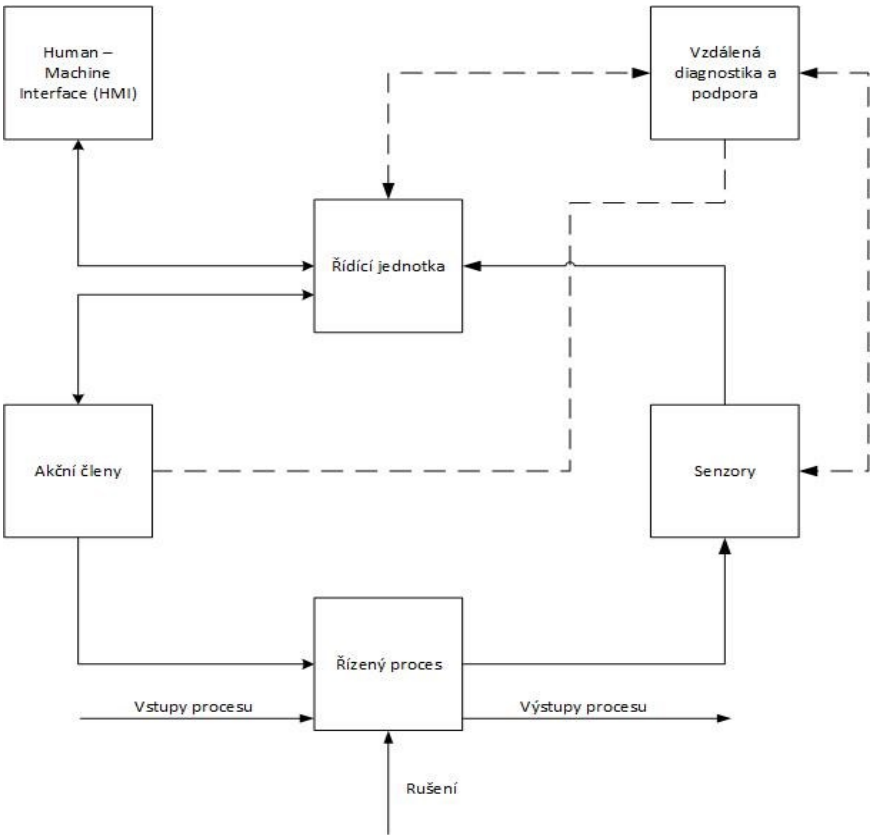
Dle Stouffera, Falca a Scarfoneho (2015, str. 2-1) jsou průmyslové řídicí systémy obecně zastřešujícím pojmem, který v sobě zahrnuje technologie sloužící k řízení průmyslových procesů v oblasti energetiky, ropného průmyslu, automobilového průmyslu, letectví apod. (Zhu, Joseph a Sastry, 2011, s. 1) Principem funkce průmyslových řídicích systémů je ovládání velkého množství fyzických zařízení rozmístěných v geograficky odlišných lokalitách za účelem řízení a parametrizace řízeného procesu. (Adepu, Mishra a Mathur, 2017, s. 1)

Z hlediska potřeby lidského faktoru v řídicím systému lze procesy rozlišit na systémy s obsluhou a bez obsluhy (Crater a Holdman, 1998, s. 1). Systémy s obsluhou mohou navíc fungovat v režimu s otevřenou, případně uzavřenou smyčkou. Režim otevřeného cyklu dovoluje obsluze konfigurovat parametry systému, zatímco v režimu uzavřeného cyklu je výstup jednoho procesu vstupem do dalšího procesu.

2.3 Komponenty průmyslových řídicích systémů

Základní komponenty, které tvoří průmyslový řídicí systém a slouží k ovládání řízeného procesu, jsou řídicí smyčky, HMI, nástroje pro vzdálenou údržbu a diagnostiku (Stouffer, Falco a Scarfone, 2015, s. 2–3).

Obrázek 2 zobrazuje obecné schéma fungování průmyslových řídicích systémů.



Obrázek 2 - Obecný princip fungování ICS. Zdroj: upraveno dle Stouffera, Falca a Scarfoneho (2015, s. 2-4)

V následujících kapitolách budou základní komponenty a jednotlivé technologie sloužící k řízení průmyslových procesů podrobně představeny, včetně možností jejich vzájemné interakce.

2.3.1 Řídicí smyčka

Řídicí smyčka slouží k manipulaci řízeného procesu s využitím senzorů, které měří vybrané fyzikální veličiny a jejich hodnoty odesílají ve formě informací do řídicí jednotky. Řídicí jednotka tyto informace interpretuje a na základě předem naprogramovaného algoritmu manipuluje s příslušnými akčními členy. Akční členy jsou prvky, které přímo slouží k ovládání řízeného procesu (Teti et al., 2010, s. 1). V prostředí energetických systémů se jedná především o jističe, spínače, ochranné prvky trafostanic, distribučních stanic, elektrických stanic a rozvoden elektrické energie. Primárním účelem akčních členů v rámci energetické soustavy je ochrana části energetické soustavy, která je v daném okamžiku ve stavu poruchy. Tento stav je třeba zaregistrovat v co možná nejkratším čase a současně za využití ochran vypnout postiženou část energetické soustavy. (Systémy chránění, 2017)

2.3.2 PLC

Yakimov a Iovev (2017, s. 911) definují PLC jako robustní a flexibilní zařízení, které má široké možnosti uplatnění při řízení procesů, včetně uplatnění v energetických systémech.

Pomocí analogových vstupů jsou PLC schopny monitorovat analogové a digitální signály, které reprezentují elektrické i neelektrické fyzikální veličiny, z připojených senzorů zajišťujících správnou funkčnost elektrické stanice. Na základě naprogramované logiky je možné tyto senzory ovládat. Součástí PLC je uživatelsky programovatelná paměť, která slouží pro ukládání instrukcí za účelem implementace specifických funkcí, především ovládání připojených senzorů. (Son et al., 2018, s. 73)

2.3.3 RTU

RTU je typem komunikačního zařízení, které je řízeno prostřednictvím mikroprocesoru a je odpovědné za zasílání, přijímání a provádění příkazů z řídicího centra (Siemens, 2016, s. 1; Razi Kazemi a Dehghanian, 2012, s. 31). Poskytuje komunikační rozhraní mezi systémem SCADA, který slouží pro centrální řízení elektrizační soustavy v řídicím centru a fyzicky připojených prvků, typicky IED (Alcaraz et al, 2013, s. 1091).

Pro zajištění komunikace z řídicího centra je možné využít spojení prostřednictvím modemu, rádiového spojení, mobilního datového spojení, případně širokopásmové komunikační technologie. Pro komunikaci s podřízenými IED jsou využívány specifické komunikační protokoly pro průmyslové sítě, které jsou podrobně představeny v další části této práce. V energetických systémech je RTU nedílnou součástí elektrické stanice. (Moreira et al. 2016, s. 1553)

2.3.4 IED

IED je komunikační zařízení obsahující mikroprocesorovou řídicí jednotku, která umožňuje přijímat nebo odesílat signály z/na přímo připojené externí zdroje, resp. senzory. Mezi běžné typy IED se řadí regulátory jističů, regulátory přepínačů zátěže, přepínače kondenzátorů a ochranná reléová zařízení (Poudel, Ni a Malla, 2017, s. 124). Poskytované funkce IED lze členit do pěti oblastí: ochrana, řízení, monitoring, měření a komunikace. IED je schopno provádět tyto vlastnosti zcela autonomně a nezávisle na použití jiných komunikačních zařízení jako RTU. (Hong a Liu, 2017, s. 1)

Z hlediska měření umožňují IED měřit širokou škálu fyzikálních veličin – napětí, proud, frekvenci, atd. Tyto informace přenáší IED do systému SCADA, kde jsou vizualizovány

operátorům. V rámci energetických průmyslových systémů nachází IED využití především v oblasti měření kvality parametrů v rozvodnových systémech a zvýšení ochrany v případě nestandardních napěťových, proudových, případně kmitočtových parametrů. Na základě zjištění nestandardního stavu je IED naprogramováno pro vykonání odpovídajícího řídicího příkazu na připojeném externím zdroji, který vypne postiženou část elektrizační soustavy. (Kezunovic, 2011, s. 12861)

Z pohledu řízení lze využít lokální, případně vzdálený přístup. IED disponuje pro lokální řízení a programovatelnosti integrovaným HMI panelem, který obsahuje tlačítkové vstupy. Tato zařízení se nasazují do provozu jako podřízená zařízení, která jsou řízena prostřednictvím předřazeného RTU (Kang et al., 2011, s. 1521). Pro účely stahování dat a nahrávání konfigurace disponuje IED rovněž sériovým, případně optickým portem pro připojení servisního PC.

Součástí IED jsou rovněž funkce pro monitoring stavu IED, obsahující možnosti měření teploty skříně, kvality napájení, monitoringu logování činností apod.

2.3.5 HMI

Za účelem nastavování parametrů řízeného procesu využívají operátoři rozhraní HMI (Pai et al., 2017, s. 1). Prostřednictvím HMI mají operátoři zprostředkovaný ovládací panel k připojeným PLC, RTU. V případě potřeby mohou být prostřednictvím HMI zprostředkovány ovládací panely IED prvků. (Knapp a Broad, 2011, s. 93–94)

HMI nahrazuje a centralizuje ruční ovládací HW prvky na separátních PLC, RTU a IED prostřednictvím jejich interpretace v SW aplikaci. Přizpůsobení a úprava SW je snadná.

Operátoři mají prostřednictvím HMI k dispozici aktuální informace o stavu procesu v grafické podobě, včetně vizualizace možnosti ovládání, resp. spouštění či zastavování cyklů a úprav nastavených hodnot, které slouží jako vstup do příslušného procesu. Součástí HMI je i sada diagnostických nástrojů a nástrojů pro údržbu. Pro interakci mezi operátorem a HMI je využívána počítačová konzole (Stouffer, Falco a Scarfone, 2015, s. 2–6). Pro zajištění řízení přístupu se operátor autentizuje do systému HMI s využitím kombinace uživatelského jména a hesla. Na základě úspěšné autentizace operátora jsou mu k dispozici předem definované funkce HMI, které může využívat. Pro komunikaci s RTU, PLC a IED jsou využity specifické proprietární i standardizované komunikační protokoly pro průmyslové sítě, které jsou podrobně představeny v další části této práce.

2.3.6 Dohledové pracovní stanice

Za účelem dohledu stavu průmyslového řídicího procesu mohou být pro tento účel využívány dohledové pracovní stanice. Stejně jako HMI shromažďují i dohledové pracovní stanice data z připojených RTU, PLC a IED zařízení. Data jsou k dispozici pouze v režimu čtení a nelze tedy žádným způsobem modifikovat nastavení připojených zařízení a tím ovlivnit řídicí proces. (Stouffer, Falco a Scarfone, 2015, s. 2-6, Knapp, 2011, s. 94)

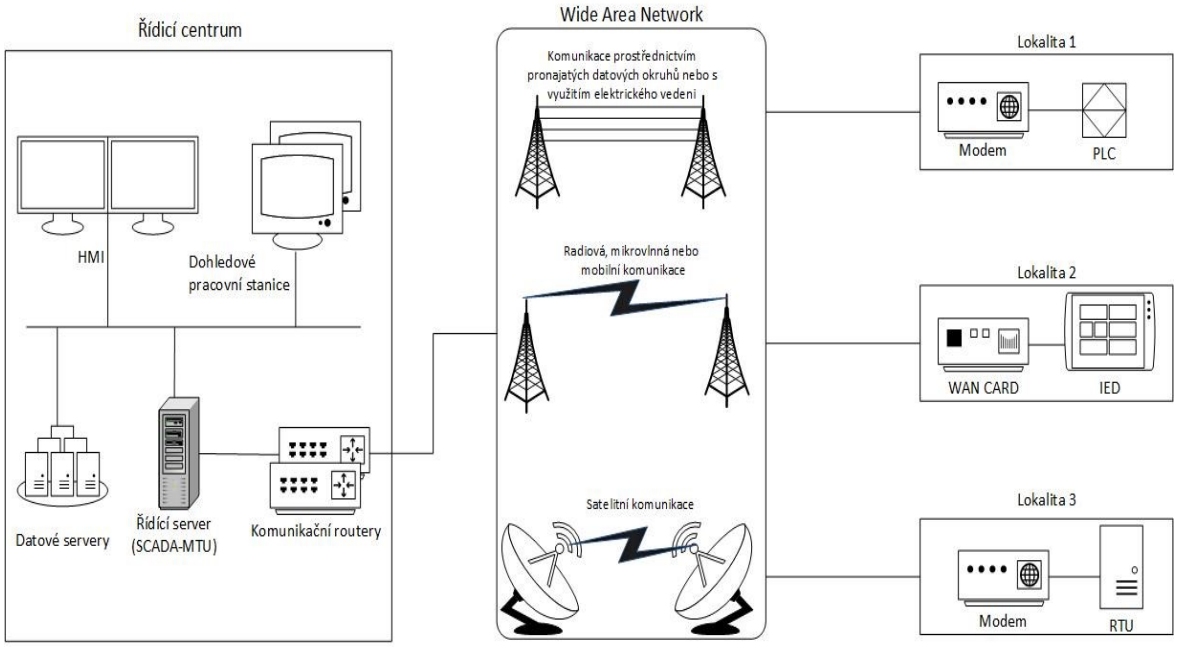
2.3.7 SCADA

SCADA systémy poskytují operátorům energetických systémů kombinaci monitorovacího a řídicího systému, který je navržen pro velké množství vstupně/výstupních operací (Kang et al., 2011, s. 1521). Jako základ monitorovacího systému slouží software běžící v rámci HMI, který získává informace prostřednictvím datových přenosů. Informace jsou ukládány na datové servery (Holmes, Russell a Allen, 2013, s. 130).

Bailey a Wright (2003, s. 6) považují za výhody softwaru systému SCADA podporu uživatelského rozhraní, grafické reprezentace dat, možnost signalizování chybových stavů prostřednictvím alarmů, podporu predikovatelnosti budoucího vývoje na základě historických dat, podpora rozhraní pro připojení RTU a PLC, škálovatelnost, podporu přístupu k datům s využitím databáze, odolnost proti chybám, redundanci a distribuované zpracování s využitím modelu klient-server.

Součástí systémů SCADA je také řídicí server umístěný v operačním centru, komunikační zařízení (např. rádio, telefonní linku, kabelové, případně satelitní spojení) a jedno nebo více geograficky rozložených polí sestávajících z RTU, případně PLC, které řídí proces pouze místně v rámci lokality (Ancillotti, Bruno a Conti, 2013, s. 3). Prostřednictvím HMI jsou informace zobrazovány operátorům graficky nebo textově a ti tak mohou centrálně ovládat systém jako celek v reálném čase z řídicího centra. (Macaulay a Singer, 2012, s. 46) Pro zajištění redundance v případě poruchy primárního řídicího centra lze typicky využít záložní řídicí centrum, umístěné v geograficky odlišné lokalitě.

Obrázek 3 zobrazuje architekturu SCADA systému a použité komponenty dle Stouffera, Falca a Scarfoneho (2015, s. 2–6).



Obrázek 3 - Obecná architektura SCADA. Zdroj: upraveno dle Stouffera, Falca a Scarfoneo (2015, s. 2-6)

Součástí řídicího centra jsou komunikační zařízení, oddělující vnější a vnitřní komunikační síť. Informace z geograficky rozmístěných lokalit jsou shromažďovány na datové servery, ke kterým jsou připojeny pracovní stanice operátorů, HMI a řídicí server SCADA. Příjem všech dat je realizován prostřednictvím řídicího serveru SCADA, který se v literatuře označuje také jako systémový sever, master terminal unit, případně hlava systému a který realizuje ukládání dat na datové servery ve formě datových bodů. Každý bod může obsahovat hodnotu (naměřená hodnota napětí, proudu apod.) včetně informace o čase vzniku a zdroji informace. Současně jsou na datových serverech uloženy všechny zadané řídicí povely. (Osborne, 2013, s. 251–253)

Řídicí server SCADA všechna přijatá data dále zpracovává za využití výpočetních a logických operací. Na základě výsledků může provádět další definované akce. Součástí logiky řídicího severu je také zpracování dat, která jsou následně interpretována grafickým rozhraním pro operátory. Z grafického rozhraní jsou prostřednictvím řídicího severu zpracovány všechny povely operátorů, které jsou zároveň ukládány na datové servery. (Radvanovsky a Brodsky, 2016, s. 3–5)

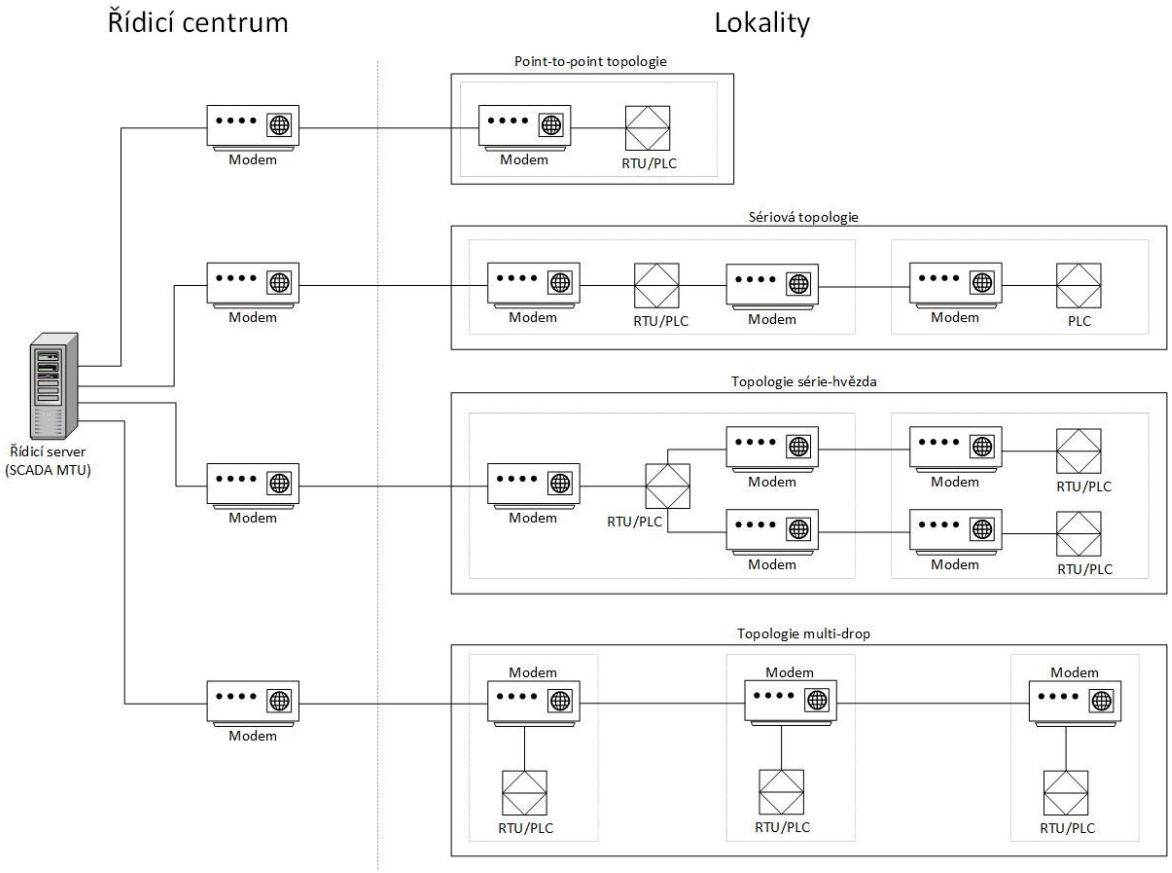
Datové servery obsahují speciální SW systém sloužící ke sběru dat a s nimi souvisejících informací, které jsou ukládány do databáze, která je pro tyto účely speciálně navržena. Vzhledem k faktu, že data uložená na datovém serveru slouží jako zdroj informací o aktuálním stavu řídicího procesu pro systémy SCADA a HMI, jejich dostupnost v požadovaném čase

je pro efektivní řízení klíčovým parametrem. V případě jejich úplné či částečné nedostupnosti by mohlo dojít k chybnému rozhodování operátora a špatnému nastavení parametrů řízeného procesu. V případě energetických systémů by dopady vzniklé situace mohly představovat chybné řízení toků elektrické energie v přenosové nebo distribuční soustavě, případně úplné vypnutí části přenosové či distribuční soustavy. (Radvanovsky a Brodsky, 2016, s. 3–4).

V oblasti průmyslových systémů sloužících pro výrobu elektrické energie v uhelných a jaderných elektrárnách by mohlo dojít, v případě nedostupnosti informací nebo chybné interpretace dat z datových serverů operátorem, k přerušení výroby elektrické energie a následné náročné opravě části technologie, která k výrobě slouží (Ejesh a Zhongling, 2017, s. 1705). Pokud by k výše uvedenému scénáři došlo v rámci výroby elektrické energie v jaderných elektrárnách, mohlo by to mít dalekosáhlé následky obsahující ekonomické a reputační ztráty, včetně možnosti ztrát na lidských životech. Z výše uvedených důvodů jsou datové servery využívané v průmyslových řídicích systémech navrhovány jako redundantní. V případě výpadku jednoho datového serveru jsou aktuální data stále k dispozici ze záložního datového serveru. (Stouffer, Falco a Scarfone, 2015, s. 2–5 – 2–6)

Na základě interpretovaných dat z datových serverů je operátorovi umožněno vykonávat příslušné akce. V rámci lokality je poskytováno místní řízení přes lokální HMI daného systému, včetně podpory vzdáleného přístupu s využitím drátové, případně bezdrátové technologie. (Radvanovsky a Brodsky, 2016, s. 3–4).

Stouffer, Falco a Scarfone, 2015, s. 2-7 dále představují základní a rozšířenou topologii komunikace v rámci SCADA systému společně s popisem jednotlivých topologií. Jedná se o topologie bod-bod, série, série-hvězda a multi-drop. Obrázek 4 zobrazuje grafickou reprezentaci základní topologie.



Obrázek 4 - Komunikační topologie SCADA. Zdroj: upraveno dle Stouffera, Falca a Scarfoneho (2015, s. 2-7)

Point-to-point je funkčně nejjednodušší typ. Nevýhodou jeho využití jsou vysoké ekonomické náklady na zřízení jednotlivých komunikačních kanálů potřebných pro každé komunikační spojení mezi lokalitou (rozvodnou elektrické energie) a řídicím centrem. Sériová topologie přináší úsporu finančních nákladů, kdy jsou jednotlivé komunikační kanály sdíleny mezi více lokalitami. Sdílení komunikačních kanálů však souvisí negativně s dopadem na efektivitu a složitost operací SCADA nejen v rámci sériové topologie, ale také u topologie série-hvězda a multi-drop. V rámci energetických systémů, které využívají pro řízení SCADA systémy, je geograficky rozmístěno velké množství RTU, které komunikují s řídicím SCADA serverem.

2.4 Komunikace a komunikační protokoly využívané v průmyslových řídicích systémech

Komunikaci komponent průmyslových řídicích systémů, tedy PLC, RTU a IED s lokálním řídicím systémem elektrické stanice a současně komunikaci lokálního řídicího systému elektrické stanice s nadřazeným systémem SCADA v řídicím centru lze realizovat s využitím široké škály komunikačních protokolů. V historickém kontextu byly různými výrobci těchto zařízení nejprve používány proprietární protokoly, založené na sériové komunikaci.

Tyto protokoly jsou z důvodu diverzifikace systémů využívaných ve velkém počtu rozvoden elektrické energie v dnešní době stále využívány. Významným faktorem, který přispívá k jejich využití v dnešní době, je pomalá doba obnovy rozvoden elektrické energie a s tím souvisejících lokálních řídicích systémů. Mezi proprietární protokoly patří SPA a RP570 od firmy ABB, Profibus od firmy Siemens a dále např. DF1 firmy Allan & Bradley nebo F4F firmy Westinghouse.

S postupným vývojem a obnovou prvků včetně lokálního řídicího systému v rozvodnách elektrické energie jsou proprietární protokoly nahrazovány standardizovanými řešeními. V dnešní době patří mezi nejvyužívanější řešení komunikační protokoly založené na mezinárodních standardech IEC 60870 a 61850. Komunikaci založenou na těchto protokolech je třeba důsledně monitorovat a analyzovat. Případné narušení komunikace by mohlo znemožnit centrální řízení energetické soustavy a ohrozit tak poskytování základní služby, tj. dodávání stabilních dodávek elektrické energie ke konečnému spotřebiteli. Detailní specifikace jednotlivých komunikačních protokolů není předmětem této práce. Za účelem úvodu do kontextu využití komunikačních protokolů v energetických systémech budou tyto protokoly pouze stručně představeny. Komunikace a komunikační protokoly využívané v rámci energetické soustavy je podle jejich účelu rozdělena na vertikální a horizontální komunikaci.

Vertikální komunikace v elektrické stanici slouží k předávání časově nekritických dat z IED zařízení a dalších prvků do nadřazeného řídicího systému SCADA spuštěného v rámci lokálního řídicího systému a přístupného operátorovi prostřednictvím lokálního HMI.

Stodůlka (2012, s. 22) uvádí, že horizontální komunikace slouží, na rozdíl od vertikální komunikace, k předávání informací pouze na stejné úrovni lokálního řídicího systému elektrické stanice. Jedná se o úroveň IED zařízení. Tradiční způsob realizace této komunikace spočíval v propojení binárních vstupů a výstupů IED zařízení. Tento způsob byl neefektivní především v nutnosti používání velkého množství metalických vodičů nebo svorek. Horizontální komunikace definovaná standardem IEC 61850 umožnila realizaci tohoto typu propojení za použití pouze jednoho ethernetového metalického kabelu (Pal a Dash, 2015, s. 8-9).

V době vzniku této práce je celosvětově aktuálním tématem otázka, který ze standardů IEC (60870 nebo 61850) bude využíván v rámci vertikální komunikace a plně v budoucnu nahradí využívané proprietární protokoly. S nasazováním těchto komunikačních protokolů

je třeba aktuálně řešit zabezpečení přenosu dat z rozvoden do řídicího centra a možné způsoby jejich monitorování.

2.4.1 RP570

RP570 je proprietárním komunikačním protokolem firmy ABB, který se používá pro spojení mezi rozvodnou a „front-end“ počítačem umístěným v řídicím centru energetické soustavy. Označení RP570 je zkratkou pro „RTU Protocol based on IEC 57 část 5-1“ Protokol nabízí rozšíření v podobě protokolu RP 571, který je určen pro komunikaci zařízení typu komunikační brána. Hlavní nevýhodou RP570 je, stejně jako v případě dalších proprietárních protokolů, využití pouze u firmy ABB. (RP 570 Protocol description, 1997, s. 3–5)

2.4.2 MODBUS

Modbus je průmyslový komunikační protokol, vyvinutý v 70. letech 20 století firmou Modicon jehož účelem je propojení IED s PLC zařízeními v rozvodnách. Protokol je založen na komunikaci typu master-slave. Původně publikovaný protokol byl proprietární pouze pro firmu Modicon. V následujících letech se protokol stal otevřeným. V důsledku otevřenosti protokolu bylo vytvořeno několik různých interpretací a modifikací původního protokolu v závislosti na využívání protokolu řadou společností. (Powell, 2013, s. 1–5)

Modbus podporuje sériové komunikační linky typu RS-232, RS-485 a RS-422, dále komunikační linky založené na optických sítích, rádiových sítích a síti typu Ethernet založené na protokolu TCP/IP. Komunikace master-slave je založena na principu požadavek-odpověď. Součástí požadavku je kód, reprezentující požadovanou akci, která má být provedena. (Ronešová, 2005, s. 1–3; Powell, 2013, s. 1–2)

Implementace Modbus TCP/IP je specifikace protokolu Modbus, ve které je zpráva Modbus RTU zapouzdřena do paketu Modbus TCP/IP a doplněna o MBAP hlavičku (Ronešová, 2005, s. 17; Modbus TCP/IP, 2017).

2.4.3 PROFIBUS

PROFIBUS je komunikační sběrnicí, která je využívána v průmyslových řídicích systémech. První návrh PROFIBUS pochází z 90. let 20. století a je zaměřen na požadavky průmyslové komunikace určené pro automatizaci výroby a výrobních procesů (Powell, 2013, s. 3–5).

Architektura PROFIBUS vychází z referenčního modelu ISO/OSI. Výhodou daného modelu je možnost abstraktního popisu komunikačních pravidel bez nutnosti vazby na konkrétní aplikaci.

PROFIBUS definuje z modelu ISO/OSI pouze 1., 2. a 7. vrstvu z důvodu časové optimalizace (Kryštůfek, 2001).

2.4.4 PROFINET

PROFINET je standardem, který vznikl jako reakce na vývoj průmyslových komunikačních sběrnic směrem k využívání komunikačních sběrnic na bázi Ethernetu (Henning, 2016). Narozdíl od technologie PROFIBUS využívá PROFINET fyzickou vrstvu Ethernetu, a tedy lze využít i zapojení do síťové topologie stromu případně hvězdy. (Fernandes et al., 2016, s. 278-279)

2.4.5 DNP3

DNP3 je komunikační protokol sloužící pro komunikaci mezi RTU, IED, HMI a nadřazeným systémem SCADA (Bermundes, 2016, s. 48). Vývoj protokolu započal v roce 1993 společností Harris, Distributed automation products a byl přijat jako standard EEE 1815-2010 až v roce 2010. Základem pro jeho standardizaci byly normy technické komise 57, pracovní skupiny 03 spadající pod organizaci IEC. Kromě energetických systémů našel DNP3 využití i dalších průmyslových odvětvích jako je vodohospodářství, doprava nebo ropný a plynárenský průmysl (Overview of the DNP3 protocol, 2011). V současné době je DNP3 v největší míře využíván v rámci energetických systémů ve Spojených státech amerických, a to ve více, než 75 % případů (Senthivel, Ahmed a Roussef, 2017, s. 65).

Komunikace DNP3 je založena na principu klient-server. V roli klienta zde vystupují RTU a IED. Roli serveru plní nadřazený SCADA server nebo lokální řídicí systém v rámci elektrické stanice, který je přístupný přes HMI. (Transmission and distribution committee substations technical committee of the ieee power & energy society, 2010, s. 14–16).

2.4.6 Standardy IEC

Již v roce 1906 byla založena organizace IEC v reakci na absenci interoperability a unifikace elektrických zařízení. Jak uvádí Horálek a Soběslav (2012, s. 65–1) jedná se o neziskovou a nevládní organizaci, která definuje mezinárodní normy pro elektrická a elektrotechnická zařízení. Členy IEC jsou mezinárodní výbory, které jmenují členy z průmyslových odvětví, vládních orgánů a akademické obce, aby se podílely na revizi vydávaných IEC norem. V současné době sdružuje organizace 84 členských států včetně 22 spolupracujících členských států. Normy IEC jsou přejímány v platnost v rámci České republiky jako ekvivalentní

standardy s označením ČSN. Relevantními standardy v oblasti komunikačních protokolů a komunikací v rámci energetických systémů jsou především IEC 61870 a IEC 61850.

IEC 60870

Standard IEC 61870 (v České republice reprezentován jako ČSN EN 61870) je standard pro sadu norem s názvem *Systémy a zařízení pro dálkové ovládání*. Standard je rozdělen do šesti základních částí.

První a druhá část (60870-1 a 60870-2) standardu definuje všeobecná ustanovení a provozní podmínky, tj. napájení, elektromagnetickou kompatibilitu, mechanické vlivy apod.

Obsahem třetí části (60870-3) je popis elektrických charakteristik rozhraní. Jedná se o popis podmínek, které musí splňovat rozhraní jednotlivých prvků, které společně tvoří funkční systém.

Čtvrtá část (60870-4) definuje „požadavky na vlastnosti“, tj. charakteristiky, které mají vliv na provoz systémů dálkového ovládání a mají vazby na vlastnosti aplikace a aplikační funkce zpracování dat. Obsahem čtvrté části je dále stanovení souboru pravidel pro hodnocení a specifikaci požadavků na výkon, a je-li to účelné, také klasifikace do tzv. výkonnostních tříd pro každou vyjmenovanou vlastnost. (Pekárek, 2017, s. 15–16)

Konkrétní určení průmyslových komunikačních protokolů využívaných pro dálkové ovládání a řízení energetické soustavy je obsahem páté části tohoto standardu, tedy 60870-5. Jedná se o protokoly využívající přenos kódovaných binárních dat prostřednictvím sériové komunikace (Han et al., 2014, s. 321).

Standard IEC 60870-5 vychází z komunikačního modelu master-slave. Komunikace probíhá mezi master jednotkou (řídicí jednotka), která odesílá požadavky, resp. dotazy nebo příkazy postupně všem podřízeným slave (řízeným) jednotkám. Slave jednotky reagují individuálně na požadavky, které jsou jim určeny. Jde o klasické komunikační schéma na principu požadavek-odpověď (request-response), které má pevná pravidla. Na uvedeném modelu je založeno mnoho v dnešní době široce rozšířených komunikačních protokolů. V tomto typu protokolů je každý přenos dat nebo zpráv po síti řízen jednotkou master. V případě rozsáhlých energetických systémů je řídicí server SCADA jednotkou typu master. RTU, IED a PLC jednotkami typu slave. (Rudzinski a Vladyka, 2010, s. 21–22)

Z pohledu komunikačních protokolů využívaných v rámci elektrizační soustavy a energetických systémů je nejvýznamnější částí norma IEC 60870-5-1, resp. její dvě části, tj. 60870-5-101 a 60870-5-104 (Nazir, Patel a Patel, 2017, s. 439).

Část 60870-5-101 s názvem *Společná norma pro základní úkoly dálkového ovládání* určuje mechanismus přenosu dat. Jejím cílem je definovat a umožnit interoperabilitu mezi jednotlivými prvky pro dálkové řízení elektrizační soustavy. Původní norma byla publikována již v roce 1995. V roce 1998 byla výrazně revidována. Obsahem revize byla definice přenosu úplné časové značky dané události. Standard využívá přenos prostřednictvím asynchronního sériového kanálu mezi DCE a DTE zařízením. Komunikace prostřednictvím IEC 60870-5-101 probíhá mezi řídicím centrem (DCE, master, řídicí server) – SCADA a dálkově ovládanými stanicemi (DTE, slave) – RTU nebo IED, prostřednictvím komunikačního spojení. (Hégr, 2012, s. 20).

Část 60870-5-104 má název *Síťový přístup pro IEC 60870-5-101 používající normalizované transportní profily*. Jejím účelem je doplnění aplikační vrstvy 60870-5-101 o použití transportních technologií klasických komunikačních sítí typu Ethernet, X25, Frame Relay, ATM, ISDN nebo GSM, s využitím architektury TCP/IP (RFC 2200). Na aplikační vrstvě je definován formát zpráv a objekty pro klasifikaci dat podle různých příkazů dle IEC 60870-5-5. Daný protokol podporuje cyklické získávání dat s možností dotazování a funkcí pro synchronizaci času. Dále na stejné aplikační úrovni poskytuje ochranu proti ztrátám a duplicitám přenášených dat mimo standardní mechanismy definované pomocí protokolu TCP na transportní vrstvě. (Rubio, Alcaraz a Lopez, 2017, s. 212)

V současné době je v rámci energetických systémů v České republice protokolem IEC 60870-5-104 přenášena většina informací ze zařízení rozvoden elektrické energie do řídicího centra. Je třeba důsledně monitorovat a analyzovat případné narušení bezpečností těchto komunikací tak, aby nedošlo k narušení dostupnosti, důvěrnosti a integrity přenášených dat. Zabezpečení komunikace s využitím komunikačního protokolu IEC 60870-5-104 úzce souvisí s využíváním standardních technologií klasických počítačových sítí – Ethernet a principy TCP/IP. Matoušek (2017) uvádí jako možné typy útoků na komunikaci protokolem IEC 60870-5-104 následující útoky, jejichž úspěšnost ve velké míře závisí na chybějící implementaci zabezpečení síťové vrstvy:

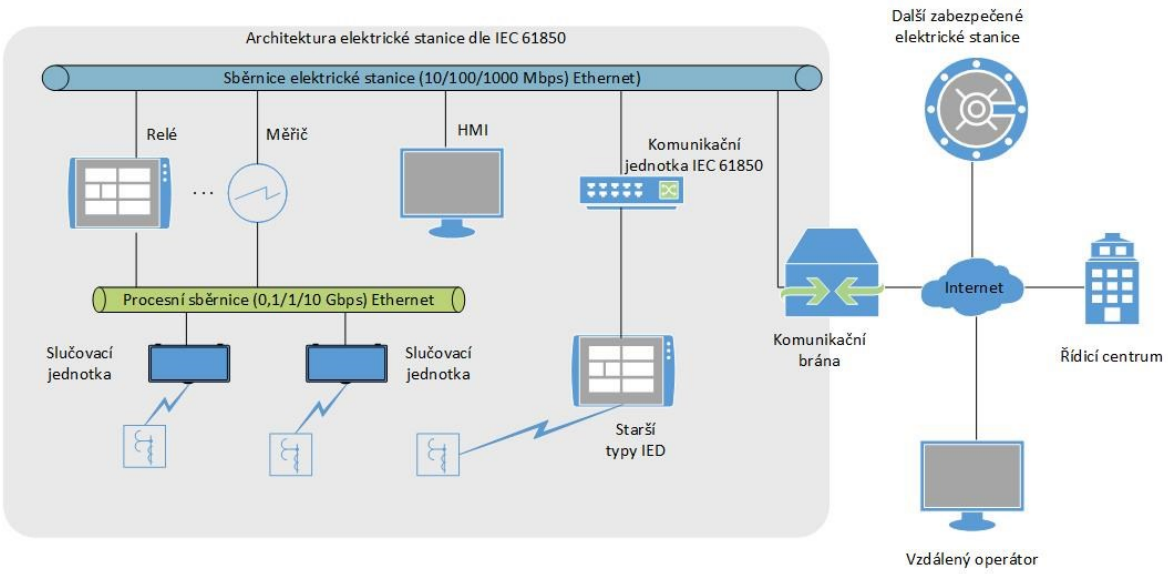
- změna dat ASDU,

- podvržení ASDU zpráv,
- provedení DDoS útoku na master nebo slave jednotku a tím způsobenou nedostupnost dat,
- podvržení falešné master jednotky do komunikační sítě,
- narušení přenosu dat mezi master a slave jednotkami.

IEC 61850

Standard IEC 61850 vznikl v roce 2003 jako reakce na požadavky automatizovaného řízení rozvoden, optimalizaci řízení rozvoden s minimalizací interakce s operátorem řídicího centra (Alvarez de Sotomayor, 2017, s. 2). Na vzniku standardu se podílely velké firmy jako ABB, Alstom, Schneider, SEL, Siemens apod. a organizace IEC. Standard definuje metody komunikace, dále pravidla pro vzájemnou komunikaci mezi IED zařízeními v elektrických stanicích, mezi elektrickými stanicemi navzájem a současně mezi elektrickými stanicemi a řídicím centrem. (Stodůlka, 2012, s. 18).

Obrázek 5 znázorňuje architekturu elektrické stanice, která je založena na standardu IEC 61850. Podle architektury elektrických stanic dle standardu IEC 61850 je vzájemné propojení IED zařízení realizováno jako komunikační síť využívající komunikační protokol TCP/IP a technologii Ethernet (Hégr, 2012, s. 3). Architektura komunikačního protokolu je typu klient-server. V případě, že je zároveň využita i horizontální komunikace, jsou zařízení IED schopna si navzájem předávat data. Komunikační protokol TCP/IP a technologie Ethernet je stejně tak využita i pro připojení komunikační sítě elektrické stanice do venkovní sítě, resp. propojení na řídicí centrum energetické soustavy, která je realizována přes zabezpečenou komunikační bránu. Protože je komunikační protokol IEC 61850 založen na využití principu technologie Ethernet a komunikačního protokolu TCP/IP, zabezpečení komunikace a další bezpečnostní mechanismy lze realizovat typicky s využitím standardně využívaných zařízení v této oblasti, které podporují nastavení bezpečnostních funkcí na síťové vrstvě TCP/IP. Mezi tato zařízení patří routery, případně firewally. (Mackiewicz, 2006, s. 623–630)



Obrázek 5 - Architektura elektrické stanice. Zdroj: upraveno dle Kabovice, Kabovice a Celebice (2014, s. 20) a Tesaříka (2014, s. 17)

Standard IEC 61850 rozděluje prováděné operace v rámci elektrické stanice do tří úrovní (IEC 61850 Substation Overview, 2018):

- Procesní úroveň – v rámci procesní úrovně dochází k získávání informací pro řízený proces. Jedná se především o měření veličin elektrického napětí, elektrického proudu apod. v různých částech elektrické stanice.
- Úroveň jednotek – je složena ze zařízení IED, která shromažďují informace z procesní úrovně. Na základě poskytnutých informací mohou IED ovládat příslušnou část elektrické stanice, předávat data ostatním IED, případně nadřazenému systému SCADA, a především plnit ochranné funkce elektrické stanice.
- Úroveň elektrické stanice – součástí této úrovně jsou HMI, lokální SCADA servery a v případě potřeby i operátoři, kteří mohou prostřednictvím lokálního řídicího systému dostupného přes HMI ovládat elektrickou stanici.

Horizontální komunikace mezi IED zařízeními přináší z pohledu zajištění ochranných funkcí elektrické stanice velké nároky na spolehlivost a čas přenosu dat. Pro zajištění těchto požadavků je tato komunikace založena na upravené architektuře klient-server. Komunikace využívá přístupu typu peer-to-peer, která umožnuje i IED zařízením řízení přenosu dat.

Pro rychlý a spolehlivý přenos informací o časově kritických událostech v rámci celého systému elektrické stanice a pro přenos vzorkovaných hodnot jsou v rámci standardu IEC 61850-7-2 definovány GSE zprávy – generické události elektrické stanice. Data GSE události jsou

přijímána pouze skupinou zařízení prostřednictvím multicastového vysílání. GSE se dělí na 2 typy: GOOSE a GSSE. (Vavreczky, 2012, s. 21; Ali a Hussain, 2016, s. 989)

GOOSE zprávy jsou objektově orientované události elektrické stanice. Prostřednictvím lokální sítě jsou přenášeny tzv. data-sety. Obsahem data-setu jsou stavová data a zároveň hodnoty jednotlivých proměnných v IED. GOOSE zprávy představují časově kritické zprávy, protože na rychlosti přenosu dat mezi IED tak, aby v IED zařízení byly k dispozici požadované informace o aktuálním stavu ostatních IED zařízení, je závislá správná funkčnost ochranných prvků elektrické stanice (Ali a Hussain, 2016, s. 989). Mezi vytvořením a odeslání GOOSE zprávy nesmí uplynout více než 4 milisekundy. (Da Silva a Coury, s. 825–826)

GSSE se používá pouze pro přenášení stavových dat, tedy pouze dat ze stavového seznamu, nikoli datového objektu. Z hlediska požadavků na časovou kritičnost těchto zpráv nejsou kladeny na GSSE zprávy stejně přísné požadavky, jako na GOOSE zprávy. Ve srovnání s GOOSE zprávami trvá vytvoření a přenos GSSE zpráv déle. (Vavreczky, 2012, s. 21)

Jak již bylo uvedeno v předchozí kapitole, standard a protokol IEC 61850 je v dnešní době stále více využíván pro komunikaci v rámci elektrické stanice a probíhá i jeho postupná implementace v rámci vertikální komunikace z rozvoden do řídicího centra energetické soustavy. Je třeba důsledně monitorovat a analyzovat případné narušení bezpečností těchto komunikací tak, aby nedošlo k narušení dostupnosti, důvěrnosti a integrity přenášených dat, stejně jako v případě protokolů rodiny IEC 60870.

2.5 Vlastnosti a požadavky při implementaci průmyslových řídicích systémů

Klíčovými vlastnostmi a požadavky kladenými při návrhu průmyslových řídicích systémů, fungujících jako jeden celek, jsou dle Stouffera, Falca a Scarfoneho (2015, s. 2–4 – 2–5):

- Požadavek na řízení v reálném čase – požadavky na procesy a operace vykonávané v rámci průmyslových řídicích systémů kladou velké nároky na jejich vykonání v omezeném časovém intervalu. Jedná se především o požadavky na rychlost zpracování dat, konzistenci dat a synchronizaci. Zajištění těchto požadavků bez použití automatizace částí průmyslových řídicích systémů, pouze prostřednictvím ručního ovládání a zásahu do systému, nemusí být spolehlivé, a tedy požadavek na řízení v reálném čase nemusí být splněn. Průmyslové řídicí systémy využívané v rámci řízení elektrizační soustavy navíc vyžadují, aby byly výpočty částečně realizované co nejblíže

jednotlivým akčním členům, čímž dochází ke snížení latence komunikace, protože pro zajištění potřebných výpočtů nemusí být tato data přenášena do řídicího centra.

- Geografická rozlehlost – průmyslové řídicí systémy disponují různými stupni geografické rozlehlosti, vzhledem k účelu jejich využití. Malé systémy využívají např. pouze lokálně řízený proces, zatímco geograficky rozlehlé systémy jsou typické při využití řízení elektrizačních soustav, ropovodních soustav apod. S požadavkem na geografickou rozlehlost vzrůstá i požadavek na zajištění zabezpečené komunikace dané lokality s řídicím centrem prostřednictvím pronajatých komunikačních linek, případně mobilní komunikace.

- Hierarchický design – řídicí centrum shromažďuje data ze vzdálených, geograficky odlišně umístěných lokalit a na základě interpretace a vizualizace dat operátorům je umožněno centrální řízení systému jako celku z jednoho místa.

- Komplexita ovládání systému – jednoduché řídicí funkce jsou naprogramovány ve formě algoritmů v PLC a IED. Se vzrůstající složitostí daného systému je nezbytná kontrola nastavených parametrů a případná úprava algoritmů operátory daného systému.

- Dostupnost – dostupnost systému je klíčovým parametrem při návrhu systému jako celku. Vysoká dostupnost systému může být dosažena s využitím redundance klíčových prvků systému, včetně redundance komunikačních linek pro komunikaci z lokalit do řídicího centra.

- Dopady selhání systému – dopady, při selhání řízení systému, představují v oblasti řízení energetické soustavy především ekonomické ztráty. Tyto systémy vyžadují schopnost standardně fungovat pomocí redundantních ovládacích prvků a manuálního řízení. Při návrhu systému musí být tyto požadavky zohledněny.

- Bezpečnost – Při návrhu systému je třeba brát zřetel rovněž na bezpečnostní požadavky. Systém musí být schopen rozpoznat nestandardní či nebezpečné stavy a vykonat příslušné akce, které tyto stavy omezují. Dohled operátorů, včetně kontroly potencionálně nebezpečných stavů, je nezbytnou součástí v oblasti řízení energetické soustavy.

3 BEZPEČNOST ENERGETICKÝCH SYSTÉMŮ

Z hlediska bezpečnosti energetických systémů, resp. průmyslových řídicích systémů versus standardních podnikových IT systémů je třeba brát na zřetel jejich rozdílné využití a tomu přizpůsobit i bezpečnostní požadavky na ně kladené (Contributors, 2016). Na rozdíl od standardních podnikových IT systémů může narušení bezpečnosti průmyslových řídicích systémů způsobit výrobní ztráty, poškození dobrého jména firmy, dopad na ekonomiku národa jako celku a v neposlední řadě rovněž ohrožení bezpečnosti lidských životů (The state of Industrial Cybersecurity, 2017). Dalším významným rozdílem souvisejícím s bezpečností průmyslových řídicích systémů je požadavek na jejich řízení v reálném čase.

Dle Govindarasu a Sauera (2012, s. 2–3) byly energetické systémy zranitelné po celá desetiletí. Až v dnešní době začíná být plně chápána závažnost potencionálních hrozeb a návazných kybernetických útoků, které mohou energetické sítě a systémy ovlivnit. Jak již bylo uvedeno v předchozích kapitolách, komponenty využívané v současné době v rámci energetických systémů a primárně podpůrných IT systémů jsou ve velké míře závislé na využití standardních PC a IT technologií. Datové servery SCADA, řídicí servery SCADA, HMI a stanice operátorů využívají standardizované operační systémy, což zvyšuje riziko jejich potencionálního zneužití útočníky a proniknutí do systému řízení energetické soustavy prostřednictvím zneužití známých zranitelností.

Motivaci ke zvyšování bezpečnosti v energetických systémech lze rozdělit do několika hledisek, které pohlíží na problematiku bezpečnosti jako celku, včetně problematiky implementace bezpečnostních opatření ve specifickém prostředí energetických systémů. Na problematiku nutnosti zvyšování bezpečnosti v energetických systémech lze nahlížet především z pohledu zvyšujícího se počtu úspěšně provedených kybernetických útoků na energetické systémy, které byly provedeny v posledních letech.

Nezbytným předpokladem pro zvyšování bezpečnosti energetických systémů je existence národní, případně nadnárodní legislativy, ve které jsou jasně definována pravidla pro bezpečnost energetických systémů. Dále je možné na tuto problematiku nahlížet z hlediska implementace a bezpečnosti průmyslových řídicích, resp. energetických systémů a specifických požadavků souvisejících s jejich implementací v porovnání s implementací a provozem standardních IT systémů. V následujících kapitolách budou tyto tři oblasti podrobně představeny s důrazem na přínos v oblasti zvyšování bezpečnosti energetických systémů.

3.1 Kybernetické útoky cílené na energetické systémy

Motivace útočníků k provedení kybernetického útoku je často motivována účelem osobního zisku, zničení systému, případně vyvoláním paniky. Významným faktorem motivace také vědomí, že útočníci dokáží napadnout i tento typ systému. Útočníky jsou v současné době nejen jednotlivci, ale i teroristé, skupiny útočníků, vládní organizace nebo armádní jednotky. (Česko v datech, 2016)

Celkový počet kybernetických útoků se v posledních letech neustále zvyšuje. Paolo Passeri (2018), který provozuje web hackmageddon.com, eviduje za rok 2018 celkem 1337 kybernetických útoků. Proti roku 2016, respektive 2015, kdy bylo evidováno celkem 1017 kybernetických útoků, je vidět jasný nárůst počtu kybernetických útoků. Obrázek 6 reprezentuje přehled motivací k provedení kybernetického útoku v roce 2018. Následující statistiky vychází od Paolo Passeri (2017), pokud není uvedeno jinak.

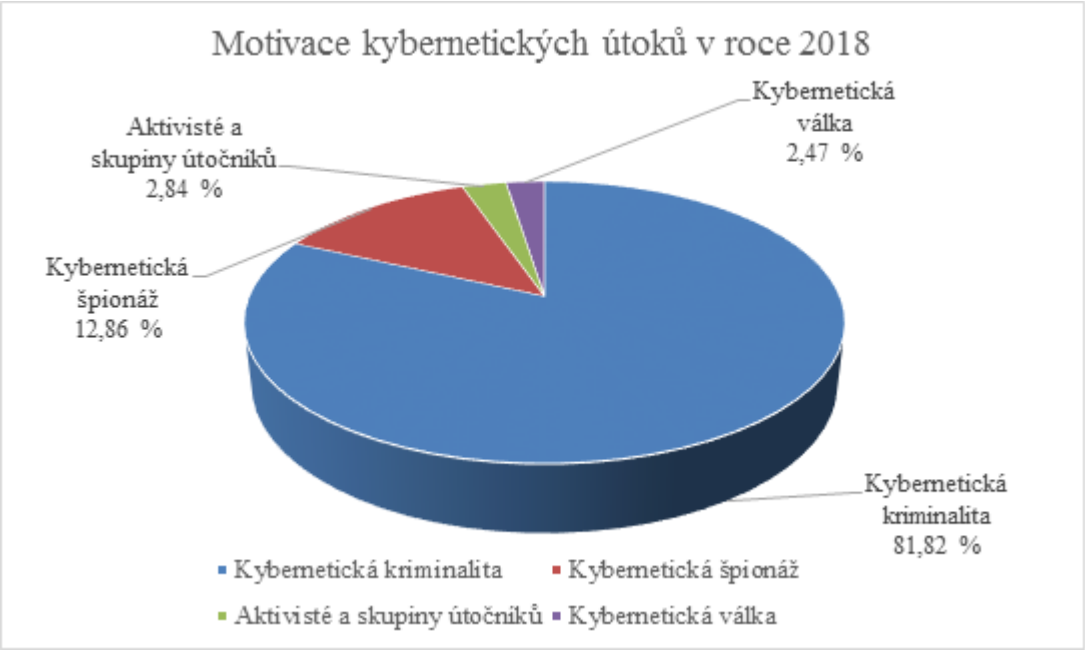
Kybernetická špionáž[1] (Cyber Espionage) byla hlavní motivací útočníků ve 12,86 % případů. Aktivisté a skupiny útočníků[2] (Hactivism) měli na svědomí celkem 2,84 % útoků a pouze 2,47 % útoků představovalo tzv. kybernetickou válku[3] (Cyber Warfare). V největší míře 81,82 % byly zastoupeny útoky motivované kybernetickou kriminalitou[4] (Cyber Crime).

[1] Kybernetická špionáž je dle výkladového slovníku kybernetické bezpečnosti definována jako *„Získávání strategicky citlivých či strategicky důležitých informací od jednotlivců nebo organizací za použití či cílení prostředků IT. Používá se nejčastěji v kontextu získávání politické, ekonomické nebo vojenské převahy.“* Citace výkladového slovníku kybernetické bezpečnosti, vyskytujících v celém textu práce, čerpá výhradně ze zdroje Jiráska, Nováka a Požára (2013)

[2] Dle výkladového slovníku kybernetické bezpečnosti se jedná o praktiku „*Použití hackerských dovedností a technik k dosažení politických cílů a podpoře politické ideologie.“*

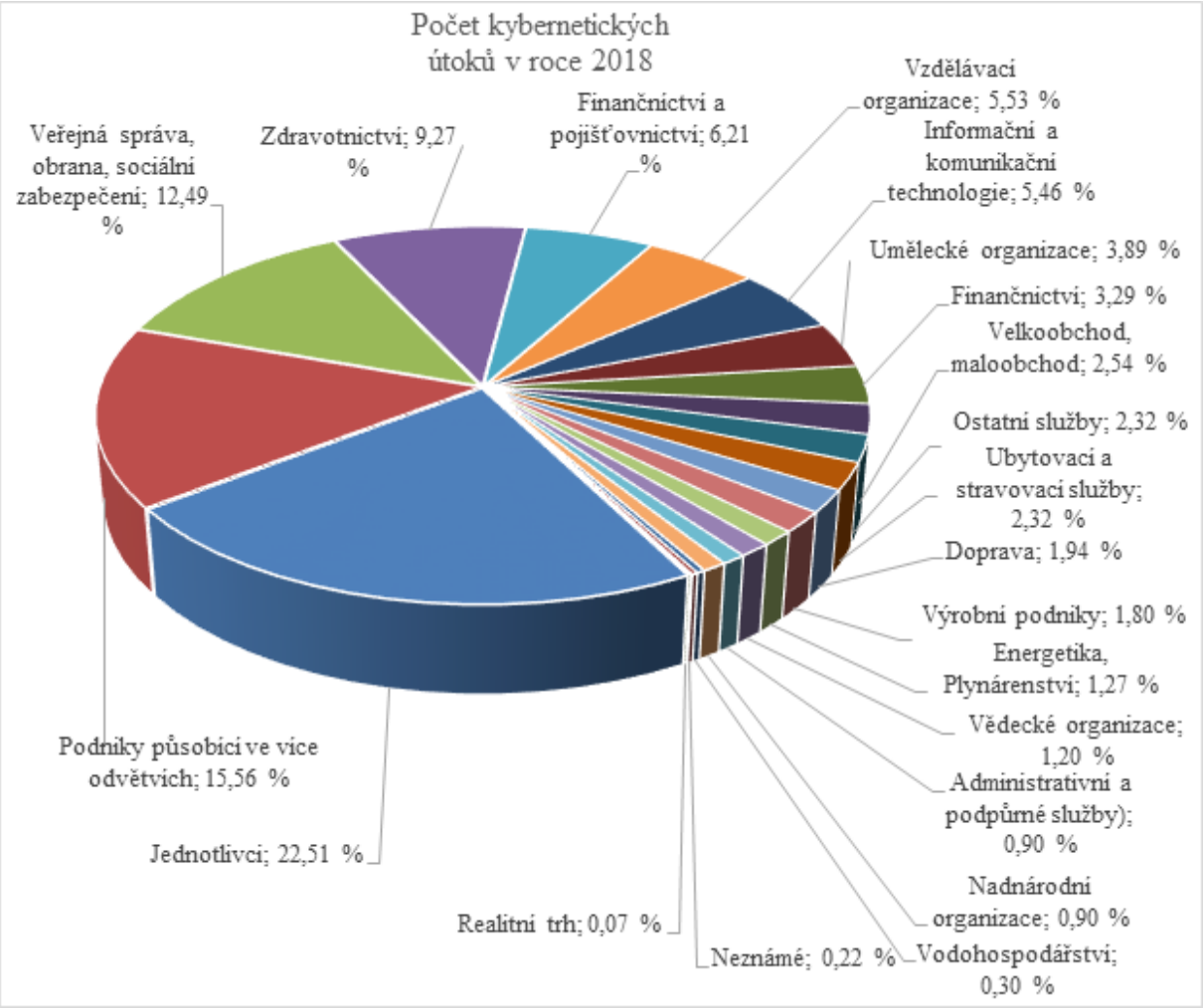
[3] Kybernetická válka je dle výkladového slovníku kybernetické bezpečnosti definována jako *„Použití počítačů a Internetu k vedení války v kybernetickém prostoru. Soubor rozsáhlých, často politicky či strategicky motivovaných, souvisejících a vzájemně vyvolaných organizovaných kybernetických útoků a protiútoků.“*

[4] Kybernetická kriminalita je dle výkladového slovníku kybernetické bezpečnosti definována jako *„Trestná činnost, v níž figuruje určitým způsobem počítač jako souhrn technického a programového vybavení (včetně dat), nebo pouze některá z jeho komponent, případně větší množství počítačů samostatných nebo propojených do počítačové sítě, a to buď jako předmět zájmu této trestné činnosti (s výjimkou té trestné činnosti, jejímž předmětem jsou popsaná zařízení jako věci movité) nebo jako prostředí (objekt) nebo jako nástroj trestné činnosti.“*



Obrázek 6 - Motivace k provedení kybernetického útoku. Zdroj: upraveno dle Passeriho (2018)

Obrázek 7 nabízí detailnější porovnání. Reprezentuje 25 oblastí lidské činnosti, které byly zasaženy kybernetickými útoky v roce 2018. Je evidentní, že v roce 2018 bylo nejvíce útoků zaměřeno na jednotlivce a podniky působící ve více odvětvích. Podniky, jejichž oblast činnosti spočívá v energetickém a plynárenském odvětví, byly v roce 2018 vystaveny celkem 17-ti kybernetickým útokům. Vzhledem k tomu, že se tato hodnota jeví jako minimální ve srovnání s ostatními odvětvími, je nutné brát na zřetel, že tato statistika vychází pouze z odhalených kybernetických útoků. Zároveň je nutné přihlédnout k tomu, že kybernetické útoky vedené proti energetickým, plynárenským, vodohospodářským, respektive průmyslovým systémům mají větší míru dopadu na fungování společnosti a zajištění základní služby, než v případě napadení systémů např. v uměleckých organizacích a administrativních službách.



Obrázek 7 - Kybernetické útoky v roce 2018. Zdroj: upraveno dle Passeriho (2018)

Nárůst kybernetických útoků v prostředí energetiky lze sledovat od roku 2010 (Technology assesment, 2015, s. 1). Propracovanost a efektivita kybernetických útoků představují výraznou změnu v ohrožení energetických systémů. Technology assesment (2015, s. 1) dále uvádí, že existují důkazy o zvyšování kybernetické špionáže, která je vedena státy a cílena na poskytovatele služeb, včetně oblasti energetiky.

Kybernetické útoky cílené na energetické systémy zahrnují získání přístupu nejen k citlivým informacím, které mohou obsahovat informace o topologii energetické sítě, případně parametrizačních dat pro ovládací prvky infrastruktury, ale především získání samotného přístupu k prvkům infrastruktury a jejich následnou kompromitaci prostřednictvím škodlivých kódů nebo ovládacích příkazů. (Rexhepi, 2017, s. 421)

Ke změně vnímání hrozeb, které mohou ovlivnit energetické sítě, resp. jsou relevantní pro oblast energetiky, došlo výrazně v letech 2015 a 2016 událostmi na Ukrajině. Dne 23. 12. 2015 Ukrajinská společnost Kyivoblenergo, zajišťující distribuci elektrické

energie, informovala své zákazníky o výpadcích elektrické energie. S využitím kybernetického útoku byl penetrován SCADA systém a několik počítačů společnosti. Probíhající kybernetický útok způsobil odpojení a zamezení dálkového řízení 7 rozvoden 35 kV a současně 23 rozvoden 35 kV. Obnova dodávek elektrické energie byla zajištěna přepnutím ovládání rozvoden do manuálního režimu a manuálním řízením ovládacích prvků v jednotlivých rozvodnách (Lee, Assante a Conway, 2016). Původní předpoklad počítal s výpadkem, který ovlivnil přibližně 80 000 zákazníků společnosti. Pozdější vyšetřování ukázalo, že stejným způsobem byly napadeny i další dvě distribuční společnosti a výpadek postihl v součtu až 225 000 zákazníků, přičemž jednotlivé kybernetické útoky na distribuční společnosti byly provedeny v rozmezí 30 minut. Ukrajinská vláda krátce na to potvrdila, že se skutečně jednalo o kybernetický útok. Vyšetřováním útoku se zabývali Ukrajinští vyšetřovatelé, soukromé společnosti i vyšetřovatelé z USA.

Kybernetický útok na společnost Kyivoblenergo nebyl zdaleka prvním typem tohoto útoku souvisejícím s odvětvím energetiky. V roce 2010 byl využit červ Stuxnet k napadení závodu na obohacování uranu v Iránu s cílem oddálit, případně úplně zastavit spuštění tamní jaderné elektrárny. Stuxnet byl malý (500 kB) soubor schopný infikovat několik operačních systémů. Principem jeho funkce bylo mapování lokální sítě a operačních systémů počítačů, které byly v síti připojeny. Následně se Stuxnet začal samovolně na těchto počítačích replikovat (Holloway, 2015). V dalším kroku došlo k infikování softwaru pro řízení PLC a získání neoprávněného přístupu. V Iránu červ Stuxnet vyřadil a následně zničil přes 900 centrifug sloužících pro obohacování uranu. Zničením centrifug došlo ke zpoždění spuštění jaderné elektrárny a snížení efektivity prací zhruba o 30 %. (Broad, Markoff a Sanger, 2011).

Na konci roku 2014 byl proveden kybernetický útok cílený na zaměstnance jihokorejské společnosti Korea Hydro and Nuclear Power's, který využíval phishingový útok prostřednictvím e-mailových adres zaměstnanců dané společnosti. Principem phishingového útoku je krádež citlivých informací za využití vydávání se za legitimní subjekt (Wu, Du a Wu, 2016, s. 6678). Celkem 3 571 zaměstnancům bylo v průběhu jednoho měsíce rozesláno 5 986 phishingových e-mailů obsahujících škodlivý software. Podle informací z Jižní Koreji byla za útok odpovědná Severní Korea, protože IP adresy, ze kterých byly vedeny útoky pochází ze Severní Koreji, a navíc programový kód využití v e-mailu byl svou konstrukcí podobný kódu, který Severokorejští hackeři obvykle využívají (Goldman, 2015). Podle vyjádření společnosti nedošlo k úniku klíčových dat.

Kybernetické útoky cílené na průmyslové řídicí systémy se nevyhnuly ani Spojeným státům americkým. V roce 2015 provedla íránská skupina SOBH Cyber Jihad úspěšný kybernetický útok na přehradu nacházející se poblíž New Yorku, která slouží pro ochranu před povodněmi. Skupina dokázala převzít kontrolu nad ovládacím systémem přehrady (Bennet, 2015). Útok byl v krátké době elimininován. Dle Takaly (2015), který cituje dokumenty ministerstva vnitra Spojených států amerických, došlo k tomu, že skupina získala přístup k přihlašovacím údajům do systému, ale nedocházelo k manipulaci s ovládacími prvky přehrady. Takala (2015) dále cituje slova Lea Taddeho, bývalého zvláštního agenta FBI v New Yorku, který byl odpovědný za kybernetické oddělení (Perez a Prokupecz, 2016). Taddeo vidí hlavní problém v nepřipravenosti organizací a podniků, kteří neberou v úvahu preventivní opatření, neprovádí aktualizace řídicích a operačních systémů včetně ochrany vnitřního perimetru, vnějšího perimetru a provádění hardeningu jednotlivých systémů.

Kybernetické útoky se v současné době nevyhnuly ani České republice. Dne 11. 12. 2019 byl kybernetickým útokem zcela ochromen provoz Nemocnice Benešov, a. s. Podle prvotního vyšetřování, kterého se účastnili zástupci NUKIB, došlo k napadení nemocnice za využití ransomware. Kybernetický útok měl za následek úplné vyřazení nemocničního IT vybavení, zašifrování uložišť s daty a dále způsobil nefunkčnost specializovaného vyšetřovacího přístrojového vybavení. Dne 30. 12. 2019 byl obnoven provoz laboratoří za využití obnovy IT systémů ze záloh (Kovaničová, 2019). Byly nakoupeny nové bezpečnostní prvky, omezen přístup na internet z vnitřní počítačové sítě a omezeno vzdálené připojení k síti. Vyšetřování útoku předpokládá za hlavní příčinu počítačový virus Ryuk původem z Ruska. (Magdoňová, 2020)

K podobnému útoku došlo dne 23. 12. 2019 v těžební společnosti OKD. Sedlák (2019) uvádí, že počítačová síť společnosti OKD se stala terčem kybernetického útoku, který způsobil nefunkčnost serverů a celé počítačové sítě. Společnost OKD okamžitě zastavila těžbu ve všech svých dolech za účelem ochrany zdraví všech zaměstnanců. Na vyšetřování kybernetického útoku se podílel, stejně jako v případě Benešovské nemocnice, tým z NUKIB. Obnova hlavních IT systémů byla dokončena až ve druhé polovině února roku 2020 (ČTK, 2020).

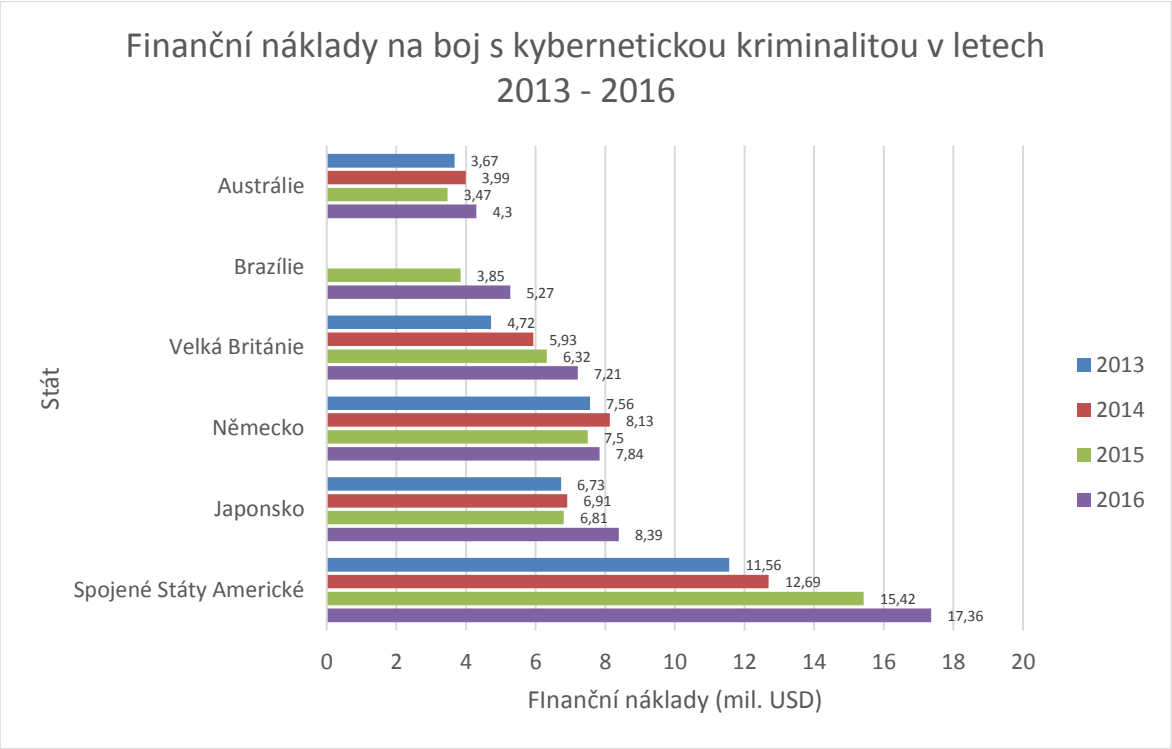
V reakci na provedené kybernetické útoky vydal vládní CERT tým varování o hrozbě, která cílí na organizace v České republice. Podle vyjádření vládního CERTu hrozba využívá botnetu Emotet v kombinaci s ransomwarem Ryuk a malwarem TrickBot. (Sedlák, 2019).

Dalšímu veřejně známému kybernetickému útoku byla v březnu 2020 vystavena FN Brno. Jak uvádí Osouch a Škarda (2020), kybernetický útok znemožnil přenos dat z jednotlivých ordinací do jednotného databázového systému. Fungování laboratoří a radiologických systémů nebylo ovlivněno. Na vyšetřování útoku se podíleli specialisté z NUKIB, kteří jsou členy týmu vládního CERTu a současně specialisté z Národní centrály proti organizovanému zločinu.

K jednomu z posledních veřejně známých kybernetických útoků, který byl cílený přímo na energetický sektor v České republice došlo ve dnech 3. 4. 2020 a 8. 4. 2020. Cílem útoku byla společnost ČEZ Distribuce, a. s. Cílem kybernetického útoku bylo narušení dostupnosti perimetrových komunikačních prvků. Díky nasazeným bezpečnostním opatřením byla tato aktivita bezprostředně odhalena. Dostupnost perimetrových komunikačních prvků a jejich služeb byla zachována v maximálním možném rozsahu. (Shabu, M., 2020)

3.1.1 Finanční dopady kybernetických útoků na energetické systémy

Každý kybernetický útok má širokou škálu dopadů zahrnující úplnou, případně částečnou nedostupnost systému nebo poskytované služby, ztrátu reputace a dobrého jména organizace, až po velké finanční ztráty. Detailnější pohled na statistiku kybernetických útoků než Passeri (2016) uvádí společnost Ponemon Institute, která sídlí ve Spojených státech amerických a provádí nezávislé výzkumy zabývající se bezpečnosti informací, ochrany soukromí a ochrany dat. Ponemon Institute rovněž každoročně vydává studii týkající se finančních nákladů na boj s kybernetickou kriminalitou. První studie o kybernetické bezpečnosti byla vydána Ponemon Institute v roce 2009 a zahrnovala statistiku týkající se společností působících ve Spojených státech amerických. Od roku 2012 jsou ve studii zahrnuty i další státy. Obrázek 8 reprezentuje výsledky studie v letech 2013 až 2016. Studie vydaná v roce 2016 využívala jako vzorek dat celkem 237 společností v 6 státech – Spojené státy americké, Velkou Británii, Německo, Austrálie, Japonsko a Brazílii. V rámci studie bylo provedeno celkem 1 278 interview se zaměstnanci daných společností. Výsledky studie ukázaly, že participující společnosti čelily celkem 465 kybernetickým útokům každý týden. Od roku 2012, kdy společnosti čelily celkem 262 útokům za týden, lze pozorovat výrazný nárůst potřených finančních nákladů. (Ponemon Institute, 2016)

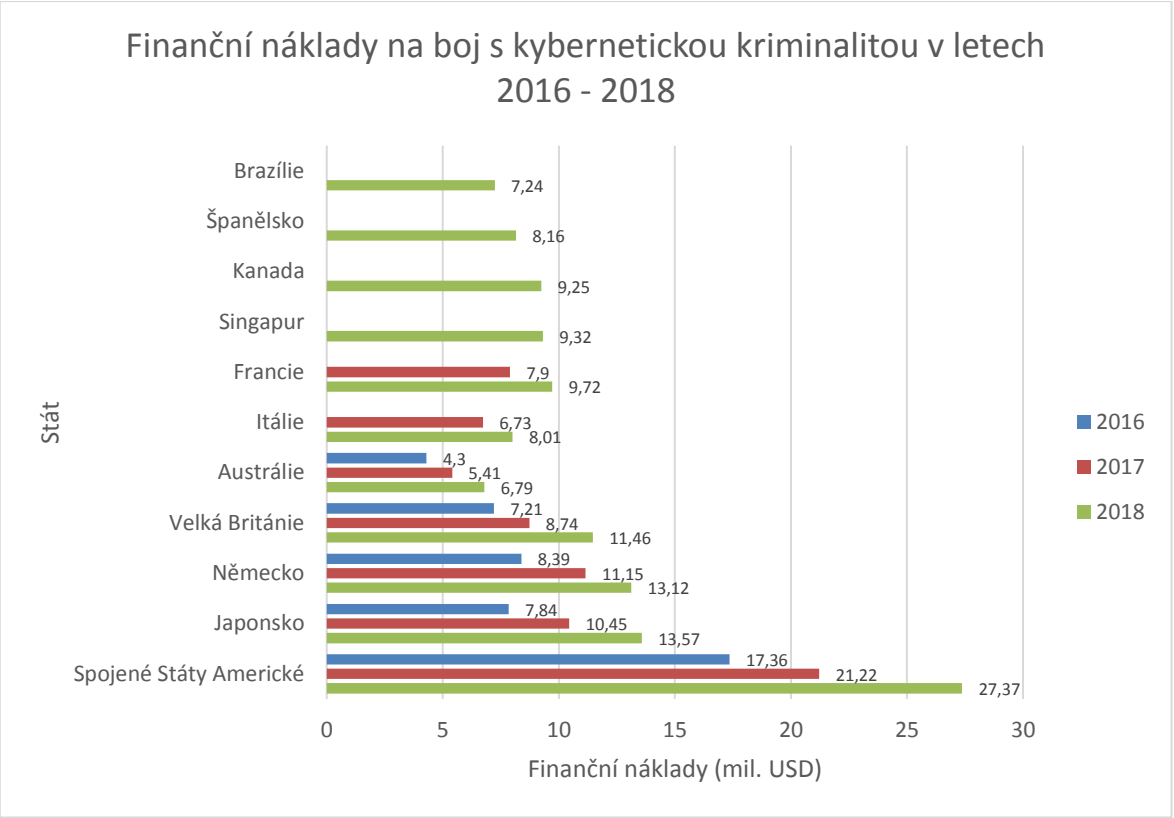


Obrázek 8 – Průměrné finanční náklady související s kybernetickými útoky v letech 2013, 2014, 2015 a 2016. Zdroj: upraveno dle: (Ponemon, 2016)

S narůstajícím množství kybernetických útoků je zároveň pozorovatelný výrazný nárůst objemu finančních prostředků souvisejících s kybernetickými útoky napříč jednotlivými státy, které se zapojili do uvedené studie. Nejvýrazněji je tento nárůst viditelný v případě Spojených států amerických. Mezi lety 2013 a 2016 vzrostly finanční náklady o 5,8 mil. USD.

V roce 2017 publikovala společnost Ponemon společně se společností Accenture další verzi studie s názvem Cost of CyberCrime Study, která využívala jako reprezentativní vzorek celkem 254 společností v 7 státech. Oproti studii z roku 2016 na výsledcích neparticipovala Brazílie. Do výzkumu byla zahrnuta i data ze společností z Itálie a Francie. Společnosti působící v Brazílii participovaly na výzkumu opět v roce 2018. Kromě Brazílie se výzkumu nově účastnily i společnosti ze Singapuru, Kanady a Španělska.

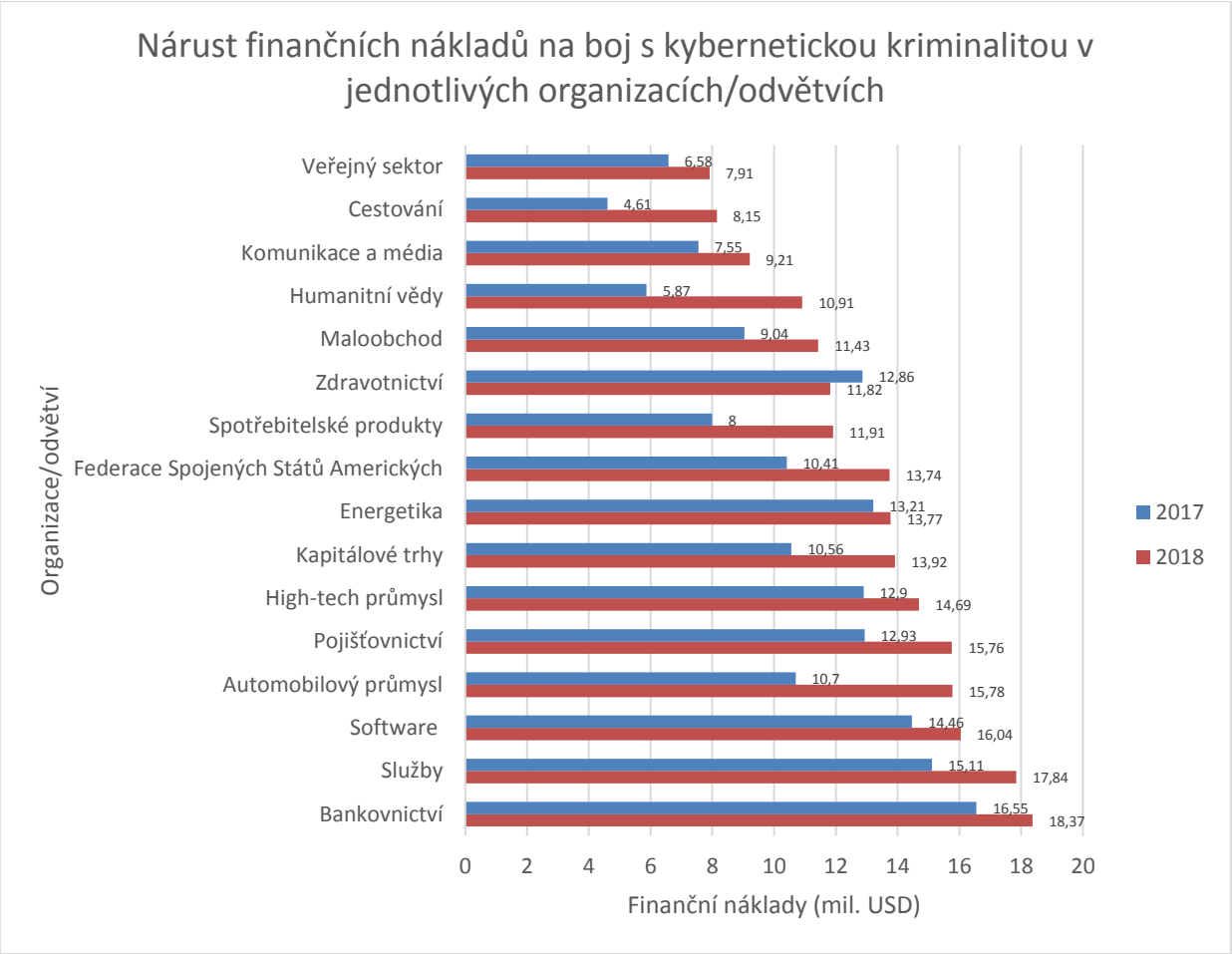
Ve srovnání s finančními náklady související s kybernetickými útoky mezi lety 2013 a 2016 lze v nejnovější studii, která prezentuje data rovněž pro roky 2017 a 2018 lze opět pozorovat výrazný nárůst vynakládaných finančních prostředků. Obrázek 9 reprezentuje výsledky studie v letech 2016 až 2018. Primární důvod lze spatřovat ve vzrůstajícím množství kybernetických útoků a jejich sofistikovanosti, kdy kybernetické útoky využívají stále sofistikovanější techniky napadení cílových systémů a s tím souvisí zvýšené množství finančních nákladů potřebných na eliminaci následků kybernetických útoků, které představují pro napadené společnosti významné finanční ztráty.



Obrázek 9 – Náklady související s kybernetickými útoky v letech 2016, 2017 a 2018. Zdroj: upraveno dle Accenture (2018)

Nejvýraznější nárůst objemu finančních prostředků na boj s kybernetickou kriminalitou je opět pozorovatelný v případě Spojených Států Amerických. Mezi lety 2016 a 2018 došlo ke zvýšení finančních prostředků o 10,01 mil. USD. Vzhledem k postavení Spojených států amerických v rámci světové ekonomiky jako světové velmoci je zřejmé, že zvýšené finanční náklady jsou příčinou vzrůstajícího množství útoků, zejména s využitím technik kybernetické špionáže, především za účelem získání politické, ekonomické nebo vojenské převahy.

Pokud se podíváme na podrobnější interpretaci výsledků dle jednotlivých odvětví lidské činnosti, resp. oblastí podnikání, je patrný významný nárůst finančních nákladů ve všech sledovaných odvětvích zahrnujících i oblast energetiky. Pouze v odvětví zdravotnictví došlo k mírnému poklesu finančních prostředků. Obrázek 10 interpretuje tyto výsledky.



Obrázek 10 – Nárůst finančních nákladů na boj s kybernetickou kriminalitou v jednotlivých odvětvích. Zdroj: upraveno dle Accenture (2018)

Výsledky této studie názorně ukazují, že kybernetickým útokům jsou vystavena v dnešní době všechna průmyslová odvětví a současně náklady na odstranění těchto útoků jsou jedny z nejvyšších u energetických společností, kde dosahují částky 13,77 mil. USD. Důvody lze spatřit především v souvislosti s výpadky elektrické energie, které mohou být přímým následkem kybernetického útoku. Při probíhajícím kybernetickém útoku může být výpadky postiženo velké množství obyvatel a současně náklady na obnovení provozu se pohybují ve vysokých finančních částkách.

3.2 Legislativní rámec

Problematika bezpečnosti energetických systémů je v dnešní době velice aktuální téma, vzhledem k důležitosti zajištění základní služby, tj. dodávek elektrické energie. Vzhledem k množství kybernetických útoků, které jsou cíleny na energetické systémy a jejich zvyšující se míru sofistikovanosti, jak bylo uvedeno v předchozí kapitole, je nezbytné aktivně monitorovat a zaznamenávat činnosti, které souvisí s provozem, správou a údržbou energetických systémů. Nutnost zajištění monitoringu činností rovněž vychází z legislativních

požadavků kladených na energetické systémy, resp. podpůrné IT systémy, neboť tyto jsou v rámci České republiky součástí kritické infrastruktury státu, resp. kritickou informační infrastrukturou a spadají do legislativní působnosti zákona o kybernetické bezpečnosti. (Zákon o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti), 2014)

3.2.1 Kritická infrastruktura

Kritická infrastruktura státu je definována v zákoně č. 240/2000 Sb., o krizovém řízení jako *„prvek kritické infrastruktury nebo systém prvků kritické infrastruktury, narušení jehož funkce by mělo závažný dopad na bezpečnost státu, zabezpečení základních životních potřeb obyvatelstva, zdraví osob nebo ekonomiku státu“*.

Prvkem kritické infrastruktury je zejména stavba, zařízení, prostředek nebo veřejná infrastruktura, určené podle průřezových a odvětvových kritérií. Tato kritéria jsou obsažena v nařízení vlády č. 432/2010 Sb., ve znění novely č. 315/2014 Sb. o kritériích pro určení prvku kritické infrastruktury. Pro určení prvku jako prvku kritické infrastruktury platí následující hlediska pro průřezová kritéria:

a) obětí s mezní hodnotou více než 250 mrtvých nebo více než 2500 osob s následnou hospitalizací po dobu delší než 24 hodin,

b) ekonomického dopadu s mezní hodnotou hospodářské ztráty státu vyšší než 0,5 % hrubého domácího produktu, nebo

c) dopadu na veřejnost s mezní hodnotou rozsáhlého omezení poskytování nezbytných služeb nebo jiného závažného zásahu do každodenního života postihujícího více než 125 000 osob.

Tabulka 1 reflektuje odvětvová kritéria pro oblast energetiky (výroba, přenosová soustava, distribuční soustava), které jsou posuzována ve druhém kroku:

Tabulka 1 - Odvětvová kritéria. Zdroj: upraveno dle novely nařízení vlády č. 315/2014 Sb.

Oblast	Výrobna elektřiny	Přenosová soustava	Distribuční soustava
Odvětvová kritéria	Výrobna s celkovým instalovaným elektrickým výkonem nejméně 500 MW.	Vedení přenosové soustavy o napětí nejméně 110 kV.	Elektrická stanice distribuční soustavy a vedení o napětí 110 kV (stanice typu 110/10 kV, 110/22 kV a 10/35 kV a k nim patřící vedení se posuzují podle jejich strategického významu v distribuční soustavě).
	Výrobna poskytující podpůrné služby ve smyslu § 2 odst. 2 písm. a) zákona č. 458/2000 Sb., o podmínkách podnikání a o výkonu státní správy v energetických odvětvích a o změně některých zákonů (Energetický zákon), ve znění pozdějších předpisů, s celkovým instalovaným elektrickým výkonem nejméně 100 MW.	Elektrická stanice přenosové soustavy o napětí nejméně 110 kV.	Technický dispečink provozovatele distribuční soustavy.
	Vedení pro vyvedení výkonu a zabezpečení vlastní spotřeby výrobny elektřiny.	Technický dispečink provozovatele přenosové soustavy.	

3.2.2 Kritická informační infrastruktura

Kritická informační infrastruktura je vymezena v zákoně o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti) č. 181/2014 Sb. jako: *„prvek nebo systém prvků kritické infrastruktury v odvětví komunikační a informační systémy v oblasti kybernetické bezpečnosti“*.

Určování kritické informační infrastruktury se řídí stejně jako v případě kritické infrastruktury nařízením vlády č. 432/2010 Sb., ve znění novely č. 315/2014 Sb. o kritériích pro určení prvku kritické infrastruktury s důrazem na bezpečnost dat a informací, tj. důvěrnost, dostupnost a integritu.

Pojem důvěrnost vyjadřuje skutečnost, že k informacím, datům, resp. IT systémům mají přístup pouze oprávněné autority. Výkladový slovník kybernetické bezpečnosti definuje dostupnost jako: „*Vlastnost, že informace není dostupná nebo není odhalena neautorizovaným jednotlivcům, entitám nebo procesům.“*

Pojem dostupnost vyjadřuje skutečnost, že informace, data, resp. IT systémy jsou přístupné oprávněným autoritám kdykoli je potřebují. Výkladový slovník kybernetické bezpečnosti definuje dostupnost jako: „*Vlastnost přístupnosti a použitelnosti na žádost autorizované entity*.“

Pojem integrita vyjadřuje skutečnost, že nebyla provedena neautorizovaná změna dat. Výkladový slovník kybernetické bezpečnosti definuje integritu dat jako: „*Jistota, že data nebyla změněna. Přeneseně označuje i platnost, konzistenci a přesnost dat, např. databází nebo systémů souborů. Bývá zajišťována kontrolními součty, hašovacími funkcemi, samoopravnými kódy, redundancí, žurnálováním atd. V kryptografii a v zabezpečení informací všeobecně integrita znamená platnost dat.*“

Dostupnost, důvěrnost a integrita dat a informací tvoří jeden z principů pro zajištění kybernetické bezpečnosti. V dnešní době je problematika dostupnosti, důvěrnosti a integrity dat vztahována primárně k oblasti informační bezpečnosti, která se zaměřuje na ochranu informací. Jak uvádí Kolouch et al., ve vztahu k aktivitám spojeným s využíváním ICT prostředků, které v oblasti energetických systémů reprezentují zejména podpůrné IT systémy jsou principy dostupnosti, důvěrnosti a integrity aplikovány i na oblast kybernetické bezpečnosti. V oblasti energetických systémů se jedná zejména o data a informace, které jsou uchovávány, přenášeny a zpracovávány v rámci řídicích systémů, resp. podpůrných IT systémů.

V rámci procesu určování prvků kritické informační infrastruktury jsou v první kroku posuzována průřezová kritéria, stejně jako v případě určování kritické infrastruktury. V případě, že narušení bezpečnosti informací (důvěrnosti, dostupnosti, integrity) informačního nebo komunikačního systému za následek alespoň jedno z výše uvedených průřezových kritérií jsou posuzována odvětvová kritéria. Schéma procesu určování prvků kritické informační infrastruktury je graficky znázorněno v příloze A (Národní úřad pro kybernetickou a informační bezpečnost, 2018).

V případě, že informační nebo komunikační systém splňuje alespoň jedno z uvedených odvětvových kritérií, jedná se o systém, který je kritickou informační infrastrukturou. V rámci energetických systémů se jedná zejména o systémy řízení výroby elektrické energie a systémy řízení přenosové a distribuční soustavy, tedy podpůrné IT systémy.

Vzhledem k tomu, že narušení dostupnosti, důvěrnosti a integrity energetických systémů, resp. podpůrných IT systémů může způsobit omezení poskytování nezbytných služeb nebo jiný závažný zásah do každodenního života postihující více než 125 000 osob a zároveň tyto systémy ovlivňují významně nebo zcela činnost prvku kritické infrastruktury a zároveň je nahraditelný jen při vynaložení nepřiměřených nákladů nebo v časovém období delším jak 8 hodin, spadají tyto systémy do kritické informační infrastruktury státu a vztahují se na ně požadavky zákona o kybernetické bezpečnosti č. 181/2014 Sb. a příslušných prováděcích vyhlášek, zejména vyhlášky o kybernetické bezpečnosti č. 82/2018 Sb.

3.2.3 Legislativa v České republice

Česká republika patří k jedné z prvních zemí v rámci Evropského kontinentu, která zakotvila ve svém právním řádu právě zákon o kybernetické bezpečnosti. Schválení zákona proběhlo dne 23. 7. 2014 s účinností od 1. 1. 2015. Předmětem úpravy zákona o kybernetické bezpečnosti je úprava práv a povinností osob a působnost a pravomoci orgánů veřejné moci v oblasti kybernetické bezpečnosti. V zákoně jsou zapracovány příslušné předpisy Evropské unie a upravuje zajišťování bezpečnosti sítí elektronických komunikací a informačních systémů s výjimkou informačních a komunikačních systémů, které nakládají s utajovanými informacemi.

Detailní požadavky na implementaci bezpečnostních opatření stanovuje příslušná prováděcí vyhláška č. 316/2014 Sb., resp. její novelizace č. 82/2018 Sb. kterou se: „*stanoví obsah a struktura bezpečnostní dokumentace pro informační systém kritické informační infrastruktury, komunikační systém kritické informační infrastruktury nebo významný*

informační systém, obsah bezpečnostních opatření, rozsah jejich zavedení, typy a kategorie kybernetických bezpečnostních incidentů, náležitosti a způsob hlášení kybernetického bezpečnostního incidentu, náležitosti oznámení o provedení reaktivního opatření a jeho výsledku a vzor oznámení kontaktních údajů a jeho formu". (Vyhláška o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (vyhláška o kybernetické bezpečnosti), 2018)

Vzhledem k faktu, že energetické systémy spadají do kritické informační infrastruktury státu, se energetická společnost stává povinnou osobou v oblasti kybernetické bezpečnosti a ukládají se jí povinnosti v oblasti kybernetické bezpečnosti. Povinnou osobou se dle §2, písm. b. Vyhlášky o kybernetické bezpečnosti rozumí *„orgán nebo osobu, které jsou povinny zavést bezpečnostní opatření podle zákona."* Příslušným zákonem je zákon o kybernetické bezpečnosti.

Dle §4, odst. 2 Bezpečnostní opatření zákona o kybernetické bezpečnosti je povinná osoba povinna „*zavést a provádět bezpečnostní opatření v rozsahu nezbytném pro zajištění kybernetické bezpečnosti informačního systému kritické informační infrastruktury, komunikačního systému kritické informační infrastruktury, informačního systému základní služby a významného informačního systému a vést o nich bezpečnostní dokumentaci."*

Při tvorbě zákona o kybernetické bezpečnosti a vyhlášky o kybernetické bezpečnosti byly zohledněny a převzaty z velké části organizační a technická opatření na řízení bezpečnosti informací (ISMS) standardu ISO 27000, zejména standardů ISO 27001 a ISO 27002.

ISO 27000 je celosvětově uznávaným a nejrozšířenějším systémem standardů, které se zabývají bezpečností informačních systémů. ISO 27001 definuje systém řízení bezpečnosti informací (ISMS). Jedná se o činnosti, týkající se řízení rizik v rámci informačních systémů, prostřednictvím kterých organizace identifikuje, analyzuje a reaguje na bezpečnostní rizika související s provozováním informačních systémů (Škeřík, 2016, s. 17). Standard obsahuje 11 základních částí, zahrnujících ověřené praktiky pro zajištění bezpečnosti informací v informačních systémech:

- bezpečnostní politiku,
- organizaci bezpečnosti informací,
- řízení aktiv,

- bezpečnost lidských zdrojů,
- fyzickou bezpečnost a bezpečnost prostředí,
- řízení komunikací a provozu,
- řízení přístupů,
- akvizice, vývoj a údržba informačních systémů,
- zvládání bezpečnostních incidentů,
- řízení kontinuity činnosti organizace,
- soulad s požadavky – shoda s předpisy a normami.

Vzhledem k požadavkům, které jsou definovány v zákoně o kybernetické bezpečnosti a vyhlášce o kybernetické bezpečnosti ohledně zajištění monitoringu činností, jsou povinné osoby povinni zajistit monitoring činností energetických systémech, resp. systémech kritické informační infrastruktury. Tato povinnost je definována zejména v §22 Zaznamenávání událostí informačního a komunikačního systému, jeho uživatelů a administrátorů vyhlášky o kybernetické bezpečnosti a § 23 Detekce kybernetických bezpečnostních událostí Povinnost koresponduje s požadavky normy ISO 27000, zejména s částí zabývající se zvládáním bezpečnostních incidentů.

Zákon o kybernetické bezpečnosti a vyhláška o kybernetické bezpečnosti definují pojem kybernetická bezpečnostní událost a současně s tím i pojem kybernetický bezpečnostní incident. Vzhledem k tomu, že tyto pojmy tvoří stěžejní část dané legislativy a jejich výklad je závazný pro všechny subjekty spadající pod gesci těchto legislativních předpisů, tedy i společnosti v energetickém sektoru, je nezbytným předpokladem vysvětlení těchto pojmů.

Kybernetická bezpečnostní událost je zákonem o kybernetické bezpečnosti definována v §7, odstavec 1 jako: „*Kybernetickou bezpečnostní událostí je událost, která může způsobit narušení bezpečnosti informací v informačních systémech nebo narušení bezpečnosti služeb anebo bezpečnosti a integrity sítí elektronických komunikací*.“

Kybernetický bezpečnostní incident je Zákonem o kybernetické bezpečnosti definován v §7, odstavec 2 jako: jako: „*Kybernetickým bezpečnostním incidentem je narušení bezpečnosti informací v informačních systémech nebo narušení bezpečnosti služeb anebo bezpečnosti a integrity sítí elektronických komunikací v důsledku kybernetické bezpečnostní události*.“

Současně zákon o kybernetické bezpečnosti stanovuje dle §7, odstavec 3 povinnost pro odpovědné osoby *„detekovat kybernetické bezpečnostní události v jejich významné síti, informačním systému kritické informační infrastruktury, komunikačním systému kritické informační infrastruktury, informačním systému základní služby nebo významném informačním systému“*. Odpovědné osoby jsou zároveň povinny hlásit kybernetické bezpečnostní incidenty Národnímu úřadu pro kybernetickou a informační bezpečnost.

Odlišný pohled na definici bezpečnostních událostí a incidentů je prezentován v rámci ISO 27001 a příručce NIST 800-61 s názvem Computer Security Incident Handling Guide.

ISO 27001 definuje bezpečnostní událost a bezpečnostní incident z hlediska informační bezpečnosti jako identifikovatelný stav systému, služby nebo sítě, ukazující na možné porušení bezpečnostní politiky, nebo selhání bezpečnostních opatření. Může se také jednat o jinou předtím nenastalou situaci, která může být důležitá z pohledu bezpečnosti informací. Bezpečnostní incident sestává dle ISO 27001 z jedné nebo více nechtěných nebo neočekávaných bezpečnostních událostí, u kterých existuje vysoká pravděpodobnost kompromitace činností organizace a ohrožení bezpečnosti informací.

Příručka NIST 800-61 definuje pojmy počítačová bezpečnostní událost a incident. V případě počítačové bezpečnostní události se jedná o pozorovatelnou událost v systému nebo v síti nebo jako nepříznivou událost s negativním následkem. Definici počítačového bezpečnostního incidentu lze volně přeložit jako porušení nebo reálně hrozící porušení bezpečnostní politiky, standardů a praktik.

V rámci společností působící v energetickém sektoru se můžeme v současné době setkat s různou interpretací pojmu bezpečnostní událost a bezpečnostní incident. Tyto interpretace však plně reflektují výše zmíněné mezinárodní standardy a platnou legislativu České republiky. V případě, že společnost spadá pod gesci zákona o kybernetické bezpečnosti je pro ni navíc závazná implementace pojmů kybernetická bezpečnostní událost a kybernetický bezpečnostní incident dle zákona do vlastní bezpečnostní politiky.

3.2.4 Legislativní požadavky na zaznamenávání činností a událostí

Z následující tabulky je patrné, že problematika týkající se zaznamenávání činností a událostí a její legislativní úprava, zejména v §22 Zaznamenávání událostí informačního a komunikačního systému, jeho uživatelů a administrátorů vyhlášky o kybernetické bezpečnosti a § 23 Detekce kybernetických bezpečnostních událostí, vychází ze standardu ISO 27002.

Tabulka 2 - Zaznamenávání činnosti v zákoně o kybernetické bezpečnosti a ISO 27002. Zdroj: vlastní zpracování

Zákon o kybernetické bezpečnosti	ISO 27002
§22 Povinná osoba zaznamenává bezpečnostní a potřebné provozní události důležitých aktiv informačního a komunikačního systému	Musí být pořizovány, uchovávány a pravidelně přezkoumávány záznamy událostí formou logů zaznamenávající aktivity uživatelů, výjimky, selhání a události bezpečnosti informací. Současně by měly být zaznamenávány formou logů aktivity systémového administrátora a systémového operátora a záznamy by měly být chráněny a pravidelně přezkoumávány.
Datum a čas včetně specifikace časového pásma; typ činnosti; identifikaci technického aktiva, které činnost zaznamenalo; datum a čas včetně specifikace časového pásma; jednoznačnou síťovou identifikaci zařízení původce; úspěšnost nebo neúspěšnost činnosti; přihlašování a odhlašování ke všem účtům, a to včetně neúspěšných pokusů; činnosti provedené administrátory; úspěšné i neúspěšné manipulace s účty, oprávněními a právy; neprovedení činností v důsledku nedostatku přístupových práv a oprávnění; činností uživatelů, které mohou mít vliv na bezpečnost informačního a komunikačního systému; zahájení a ukončení činnosti technických aktiv;	ID uživatele, činnosti systému, datum, čas a podrobnosti důležitých událostí, například odhlášení a přihlášení; identitu nebo umístění zařízení, pokud je to možné a identifikátor systému; záznamy o úspěšných a neúspěšných pokusech o přístup k systému; záznamy o úspěšných a neúspěšných pokusech o přístup k datům a dalším zdrojům; změny konfigurace systému; použití privilegií; použití systémových nástrojů a aplikací; soubory, ke kterým bylo přistupováno a typ přístupu; síťové adresy a protokoly; poplachy vyvolané systémem řízení přístupu; aktivace a deaktivace ochranných systémů jako jsou antivirové systémy a systémy detekce průniku;

Zákon o kybernetické bezpečnosti	ISO 27002
kritických a chybových hlášení technických aktiv a přístupů z záznamům o událostech, pokusy o manipulaci se záznamy o událostech a změny nastavení nástrojů pro zaznamenávání událostí.	záznamy transakcí provedených uživateli v aplikacích.

V §23 vyhlášky o kybernetické bezpečnosti jsou specifikovány požadavky na detekci kybernetických bezpečnostních událostí prostřednictvím nástroje, který zajišťuje ověření a kontrolu přenášených dat v rámci komunikační sítě a mezi komunikačními sítěmi, ověření a kontrolu přenášených dat na perimetru komunikační sítě a blokování nežádoucí komunikace.

Vyhláška o kybernetické bezpečnosti dále v §24 Sběr a vyhodnocování kybernetických bezpečnostních událostí určuje povinné osobě využívání nástroje, který slouží pro sběr a nepřetržité vyhodnocení kybernetických bezpečnostních událostí, který umožňuje:

- Sběr a vyhodnocování událostí zaznamenaných podle § 22 a 23.
- Vyhledávání a seskupování souvisejících záznamů.
- Poskytování informací pro určené bezpečnostní role o detekovaných kybernetických bezpečnostních událostech.
- Vyhodnocování kybernetických bezpečnostních událostí s cílem identifikace kybernetických bezpečnostních incidentů, včetně včasného varování určených bezpečnostních rolí.
- Omezení případů nesprávného vyhodnocení událostí pravidelnou aktualizací nastavení pravidel pro vyhodnocování kybernetických bezpečnostních událostí a včasné varování.

Zároveň povinná osoba využívá informace získané nástrojem pro sběr a vyhodnocení kybernetických bezpečnostních událostí pro optimální nastavení bezpečnostních opatření informačního a komunikačního systému.

Vyhláška o kybernetické bezpečnosti rovněž definuje dobu, po kterou se ukládá povinné osobě uchovávání událostí. V případě energetických společností je doba stanovena dle §22, odst. 3 na 18 měsíců.

Zajištění monitoringu činností v rámci energetických systémů minimálně v rozsahu úspěšných/neúspěšných přihlášení k systémům, neprovedení spuštění dané akce v systémů

a detekování škodlivého kódu definuje ve standardech CIP (Critical Infrastructure Protection), také společnost NERC (North American Electric Reliability Corporation), která je mezinárodní regulační autoritou pro zajištění spolehlivosti a bezpečnosti energetických systémů. Dalším posláním NERC je monitoring částí energetických systémů, každoroční hodnocení sezónní a dlouhodobé spolehlivosti energetických sítí, vzdělávání, školení a současně certifikace pracovníky v průmyslových odvětvích včetně energetiky. Oblastí působnosti NERC je území Spojených států amerických, Kanady a severní část Mexika. Dohled nad organizací NERC zajišťuje Federální energetická komise Spojených Států a současně vládní úřady Kanady. NERC se jako jedna z prvních organizací zaměřila i na oblast kybernetické bezpečnosti v oblasti energetiky s důrazem na ochranu těchto systémů před kompromitací systému, která by mohla mít za následek jeho nedostupnost nebo nestabilitu (NERC, 2016). Vydávaná sada standardů CIP která je široce uznávaná nejen ve Spojených Státech, ale i v jiných částech světa. (Knapp a Langill, 2015, s. 389) Standardy začali vznikat již v roce 2007 a o rok později byly schváleny Federální energetickou komisí Spojených Států. Od té doby byly několikrát revidovány. Roberts (2016) uvádí primární zaměření CIP standardů nikoli v oblasti kritické infrastruktury, ale především ve správě „kybernetických aktiv“. Většina současně využívané IT infrastruktury v energetických systémech je založena na IP protokolu a CIP standardy umožňují identifikovat a spravovat kritická kybernetická aktiva, včetně kybernetické bezpečnosti těchto aktiv.

Součástí NERC CIP je celkem 11 standardů které pokrývají oblasti hodnocení rizik aktiv, hlášení bezpečnostních incidentů, minimálními doporučenými opatřeními, monitorováním bezpečnostních událostí, zásady prosazování kontrol fyzického přístupu k aktivům, požadavky na dokumentaci atd. (CIP Standards, 2016). Tabulka 3 uvádí kompletní přehled NERC CIP standardů, přičemž požadavky na monitoring činností jsou součástí standardu CIP-007-6.

Tabulka 3 - Přehled NERC CIP standardů (zdroj: upraveno dle Knappa (2011, s. 250) a CIP Standards, 2016)

Název standardu	Účel
CIP-003-6	Kontrola řízení bezpečnosti
CIP-004-6	Osoby a školení
CIP-005-5	Elektronický bezpečnostní perimetr
CIP-006-6	Fyzická bezpečnost energetických systémů
CIP-007-6	Řízení bezpečnosti systémů
CIP-008-5	Hlášení bezpečnostních incidentů a plánování opatření
CIP-009-6	Plány obnovy energetických systémů
CIP-010-2	Management řízení změn a hodnocení zranitelností
CIP-011-2	Ochrana informací
CIP-002-5.1a	Kategorizace energetických systémů

Standardně využívanými a mezinárodně uznávanými normami používanými v oblastech informační a kybernetické bezpečnosti systémů kritické infrastruktury, nejen v prostředí energetiky, jsou kromě výše uvedených standardů CIP i standardy organizací NIST a IEEE.

Organizace NIST byla zřízena v roce 1901 a jejím hlavním úkolem je podpora inovací a konkurenceschopnosti Spojených států amerických, prostřednictvím standardů a technologií. Hlavním cílem mezinárodní neziskové profesní organizace IEEE, je vzestup technologií související s elektrotechnickým průmyslem.

Tabulka 4 uvádí stručný přehled standardů NIST a IEEE, které se zabývají problematikou bezpečnosti kritické infrastruktury.

Tabulka 4 - Standardy bezpečnosti energetických systémů. Zdroj: upraveno dle The 62443 series of standards (2016), Schlegela, Obermeiera a Schneidera (2017, s. 197) a Stouffera, Falca a Scarfoneho (2015)

Zkratka	Popis
ISA S99 / IEC 62443	Bezpečnost systémů průmyslové automatizace a řídicích systémů.
IEC 62351	Bezpečnost dat a komunikací – zejména se týká zabezpečení přenosů dat pomocí IEC61850 resp. IEC 60870-5-104 (Data and Communications Security).
NIST 800-82	Příručka bezpečnosti průmyslových řídicích systémů NIST.
IEEE PSRC H13	Požadavky na kybernetickou bezpečnost automatizace rozvoden elektrické energie, ochranné a řídicí systémy.
IEEE 1686	Standard pro možnosti kybernetického zabezpečení IED na rozvodnách elektrické energie.
ICSJWG	Doporučení pracovní skupiny ICSJWG (Industrial Control System Joint Working Group), která byla zřízena v rámci CSIRT týmu Ministerstva vnitřní bezpečnosti Spojených států amerických.

3.3 Bezpečnost energetických řídicích systémů

V současné době jsou v rámci energetických systémů, resp. průmyslových řídicích systémů, využívány operátory řídicího centra pracovní stanice vybavené HW komponenty a operačními systémy, které se využívají rovněž v rámci standardních IT systémů. Stejnou platformu využívají také HMI v rámci lokálního řídicího systému elektrických stanic. Tyto podpůrné IT systémy tvoří základ inteligentního centralizovaného dohledu, případně lokálního řídicího systému elektrické stanice a významně se podílejí na zajištění poskytování základní služby. Za tímto účelem využívají podpůrné IT systémy specificky vytvořené aplikace pro daný systém, které se v prostředí podnikových IT systémů nevyskytují (Lee a Huba, 2014).

Průmyslové řídicí systémy byly historicky koncipovány jako uzavřené systémy, které využívaly proprietární komunikační protokoly, bez existence síťového propojení do vnějšího světa. Jak bylo uvedeno v předchozích kapitolách této práce, proprietární komunikační protokoly začaly být s postupným vývojem nových komunikačních technologií (IP protokol, Ethernet) nahrazovány a průmyslové řídicí systémy se začaly propojovat s podnikovými informačními systémy, za účelem např. získávání dat týkající se poruch nebo dat o provozu energetické soustavy. Jednalo se o velmi významnou změnu, kdy se průmyslové řídicí systémy začaly podobat podnikovým IT systémům, které využívají stejné komunikační technologie (Cook et al., 2017, s. 467). Nejednalo se pouze o implementaci nových komunikačních technologií a protokolů – především IEC 61850 a IEC 60870. Pro zajištění poskytování základní služby, tedy dodávání stabilních dodávek elektrické energie je zapotřebí zajistit bezproblémový chod nejen průmyslových řídicích systémů, ale především podpůrných IT systémů.

Průmyslové řídicí systémy se s touto změnou stávají otevřenější a tím se zvyšuje jejich míra zranitelnosti (Canto et al., 2015, s. 13). Bezpečnostní řešení tedy nelze již navrhovat pouze pro část týkající se IT systémů, ale je nutné brát v potaz systém jako celek a pružně reagovat zlepšováním bezpečnosti v rámci dynamického prostředí, ve kterém tyto systémy fungují. (Technology assesments, 2015, s. 3)

S narůstající integrací standardních IT (PC) technologií a komunikačních protokolů je třeba důsledně monitorovat a analyzovat všechny komponenty daného systému na známé zranitelnosti – zejména v oblasti operačních systémů a SW pro komunikační prvky. Na úrovni komunikací je nutné zajistit monitoring vnějšího perimetru systému, tedy komunikačních zařízení, které propojují průmyslový řídicí systém do vnějšího světa.

Účelem je předcházení či zamezení napadení systému z vnější komunikační sítě. Pro maximalizaci eliminace hrozby[5] napadení systému z vnitřku organizace by měly být podpůrné IT systémy chráněny pomocí vhodného fyzického umístění a současného využití systémů technické ochrany. Tyto systémy v sobě zahrnují kamerové systémy, přístupové systémy, fyzické zábrany apod. Fyzický přístup k podpůrným IT systémům by měl být rovněž součástí celkového monitoringu. Dále je vhodné monitorovat a analyzovat neúspěšné a úspěšné přihlašování do podpůrných IT systémů, používání USB zařízení v souladu s vnitřními politikami organizace apod. V obecném pohledu sestává monitoring daného systému pro řízení energetické soustavy komplexní činností zahrnující monitoring podpůrných IT systémů, komunikací a průmyslových řídicích systémů s důrazem na minimalizaci možných rizik, které souvisejí s možností narušení daného systému a poskytování základní služby.

Tabulka 5 uvádí přehled požadavků, které jsou kladeny na průmyslové řídicí systémy a IT systémy.

Tabulka 5 - IT systémy versus ICS (zdroj: upraveno dle Stouffera, Falca a Scarfoneho, 2015, s. 2-17)

Kategorie	IT sytém	Průmyslový řídicí systém
Požadavky na výkon	Není vyžadována práce systému v reálném čase.	Je vyžadována práce systému v reálném čase.
	Odpověď musí být konzistentní.	Odpověď je časově kritická.
	Vyžadována vysoká propustnost komunikace.	Vysoká propustnost komunikace není vyžadována.
	Přijatelné velké zpoždění komunikace a nestabilita latence.	Nepřijatelné velké zpoždění komunikace a nestabilita latence.
	Interakce se systémem v případě nouzového stavu není kritická.	Možnost interakce obsluhy se systémem v případě nouzového stavu je kritická.
	Lze implementovat kontrolu řízení přístupu např. s využitím ACL.	Přístup k průmyslovému řídicímu systému by měl být přísně kontrolován. Nemělo by docházet k omezování nebo narušování interakce systému s obsluhou.

[5] Hrozba je v rámci výkladového slovníku kybernetické bezpečnosti definována jako *„Potenciální příčina nechtěného incidentu, jehož výsledkem může být poškození systému nebo organizace.“*

Kategorie	IT sytém	Průmyslový řídicí systém
Požadavky na dostupnost (spolehlivost)	Odpovědi systému (např. restart) jsou přijatelné.	Odpovědi systému (např. restart) nemusí být přijatelné z důvodů požadavku na dostupnost systému.
	Určitá časová nedostupnost systému je tolerována, v závislosti na provozních požadavcích systému.	Pro splnění požadavků na dostupnost je využívána redundance částí systému nebo systému jako celku.
		Plánované výpadky systému jsou plánovány dny až týdny předem.
		Vysoká dostupnost systému vyžaduje komplexní provedení testů před nasazením systému do provozu.
Požadavky na řízení rizik	Systém je koncipován pro správu dat.	Systém je koncipován pro správu řízeného procesu.
	Důvěrnost a integrita dat je prvořadá.	Ochrana člověka je prvořadá, následovaná ochranou řízeného procesu.
	Odolnost vůči chybám je méně důležitá. Momentální nedostupnost je méně závažné riziko.	Odolnost vůči chybám je nezbytná. Momentální nedostupnost nemusí být přijatelná.
	Hlavním dopadem na rizika je zpoždění obchodních činností.	Hlavními dopady na rizika jsou nedodržování předpisů, dopady na životní prostředí, ztráty na životech, zařízeních nebo výrobě.
Provoz systému	Systémy jsou navrženy pro použití s široce dostupnými operačními systémy.	Využívají rozdílné operační systémy, standardní i proprietární bez integrovaných bezpečnostních funkcí.
	Aktualizace systému jsou přímočaré s dostupností automatizovaných nástrojů pro nasazení.	Aktualizace SW jsou obvykle prováděny dodavatelem HW a SW kvůli přítomnosti specializovaných algoritmů, případně modifikovanému HW a SW.
Omezení zdrojů	Systémy jsou navrženy s dostatečným množstvím HW a SW zdrojů, které podporují přidávání aplikací třetích stran a bezpečnostních řešení.	Systémy jsou navrženy pro řízení průmyslového procesu a nemusí disponovat dostatečnými paměťovými a výpočetními prostředky pro integraci bezpečnostních funkcí.
Komunikace	Standardní komunikační protokoly.	Mnoho proprietárních a standardních komunikačních protokolů.
	Primárně kabelové sítě.	Více typů komunikačních technologií (vyhrazené spoje, satelitní spoje, apod.).

Kategorie	IT sytém	Průmyslový řídicí systém
	Využití typických postupů pro vytváření počítačových sítí v IT.	
Management změn	Aktualizace SW jsou aplikovány včas. Instalace jsou často automatizované.	Aktualizace SW musí být důkladně otestovány a postupně nasazeny tak, aby nedošlo k narušení integrity průmyslového řídicího systému. Výpadky je nutné plánovat dny až týdny předem. Mohou být používány operační systémy, pro které již nejsou vydávány bezpečnostní aktualizace.
Podpora systému	Umožňuje zajistit podporu systému od více dodavatelů.	Podpora systému je typicky od jediného dodavatele.
Životnost komponent	Životnost v rozmezí 3 - 5 let.	Životnost v rozmezí 10–15 let.
Umístění komponent	Komponenty jsou obvykle snadno přístupné lokálně.	Komponenty mohou být izolované, umístěné v geograficky oddělených lokalitách. Přístup k nim může vyžadovat fyzickou námahu.

Řada systémů, které jsou v současné době v provozním prostředí energetických systémů, je technicky zastaralá. Důvodem zastarání je dlouhodobá doba obnovy energetických systémů, která se typicky pohybuje v řádu desítek let a s tím spojená finanční náročnost této obnovy. Obnova energetických systémů je spojena s výměnou nikoli pouze dílčí části systému, ale často funkčních bloků provozovaného technologického systému jako celku. Další důvod lze spatřovat v potřebě spolehlivosti dodávky elektrické energie, kdy je a v minulosti byla často upřednostňována spolehlivost a správná funkčnost zařízení oproti splnění bezpečnostních požadavků (Cyber security solutions for critical infrastructure and industrial control systems, 2017). Z výše uvedených důvodů, kdy energetické systémy často nejsou schopny splnit nejnovější bezpečnostní doporučení, je pravděpodobnost provedení kybernetického útoku na tento druh systémů vyšší než v případě, kdy energetický systém splňuje jako celek nejnovější bezpečnostní požadavky a doporučení.

Eder-Neuhauser (2017, s. 14) doplňuje Česko v datech (2016) a uvádí další faktory, které jsou typické pro kybernetické útoky cílené na energetické systémy. Na rozdíl od kybernetických útoků, které jsou cíleny na klasické IT systémy, jejichž účelem je nejčastěji způsobení finanční ztráty, ztráty reputace a krádeže citlivých dat, mohou kybernetické útoky vedené na energetické systémy způsobit navíc narušení dostupnosti služby pro širokou veřejnost. S Ederem-Neuhauserem (2017, s. 14) se v pohledu na tuto problematiku shoduje i Cook et al. (2017, s. 468), který mimo jiné také uvádí, že kybernetický útok cílený na narušení důvěrnosti,

dostupnosti a integrity informací může vést k chybnému rozhodnutí operátora řídicího centra, který nemá k dispozici aktuální a správné informace o stavu elektrizační soustavě, následkem čehož může dojít k chybným manipulacím s prvky elektrizační soustavy, případně s úseky vedení elektrizační soustavy, a následně i ohrožení zdraví a majetku osob v případě, že na elektrizační soustavě probíhají plánované údržbové práce.

Typickým představitelem zranitelnosti u podpůrných IT systémů, resp. u standardních PC je možnost využití škodlivého software. Otuoze, Mustafa a Larik. (2018, s. 4) uvádí, že možností zavlečení škodlivého software do podpůrných IT systémů existuje celá řada. Typicky se jedná o hackerský útok, kdy útočník překoná obranu vnějšího perimetru, tedy zařízení (firewally), které oddělují komunikační infrastrukturu průmyslových řídicích systémů a vnější sítě (podniková síť, síť internet). Uvedený problém považuje za závažné ohrožení průmyslových řídicích systémů také Stouffer, Falco a Scarfone (2015, s. 3-5)

Sun, Hahn a Liu (2018, s. 53) definují další z cest, která potenciálně může vyústit v napadení průmyslového řídicího systému. Touto cestou je napadení systému z vnitřní komunikační sítě. Tato možnost vychází z detailní znalosti architektury systému a jeho nastavení. Baldwin et al. (2015, s. 12) má stejný pohled na tuto problematiku jako Sun, Han a Liu (2018, s. 53). Dle Baldwina et al.. (2015, s. 12) představují nejslabší místo pro napadení systému notebooky nebo parametrizační stanice dodavatelů systému, které jsou připojeny do systému prostřednictvím LAN sítě. Tyto stanice je třeba považovat za potenciální zdroj škodlivého software. Pro zamezení možnosti využití tohoto typu útoku je třeba důsledně vyžadovat, aby stanice dodavatelů vždy obsahovali nainstalovanou antimalwarovou ochranu s aktualizovanou virovou databází. S výše uvedeným pohledem na využívání antimalwarové ochrany plně koresponduje i názor Stouffera, Falca a Scarfoneho (2015, s. E-2). Baldwin (2015, s. 12) dále uvádí, že vyžadování těchto bezpečnostních pravidel by mělo být součástí smlouvy, která je uzavřená s dodavatelem konkrétního systému. Současně by měli být monitorovány všechny přístupové aktivity do energetických systémů, které souvisí s dodavateli. Je třeba důsledně využívat principy autentizace a autorizace těchto uživatelů a současně tyto aktivity monitorovat.

Další možnost napadení energetických systémů souvisí s možností zneužití fyzického přístupu k systému a využití otevřených USB portů a dalších paměťových médií, využívaných v rámci podpůrných IT systémů, pro zavlečení škodlivého software (diskety, CD disky, DVD disky), jak uvádí Moreira et al., (2016, s. 1553). S Moreirou et al. (2016, s. 1553) se shodují i Stouffer,

Falco a Scarfone (2015, s. C-8), kteří vidí jako největší potencionální problém právě možnost zneužití USB portů pro napadení systému. Stouffer, Falco a Scarfone (2015, s. C-8) dále uvádí, že instalací WiFi nebo GPRS modemů do USB portů vzniká otevřená komunikační cesta do systému, která není žádným způsobem monitorována bezpečnostními prvky chránícími vnější perimetr (firewally). Při vyšetřování tohoto typu incidentu v případě napadení systému nejsou tedy k dispozici relevantní informace z bezpečnostních prvků a ve většině případů je velice obtížné identifikovat původce útoku. Možnost předcházení těmto typům útoků vychází z pravidelného provádění školení bezpečnosti u obsluhy centrální úrovně řídicího systému. Školení by mělo být realizováno i na úrovni jednotlivých dodavatelů systémů. Vždy by měl být o provedeném školení realizován zápis. V rámci školení je třeba poučit obsluhu o bezpečném používání IT vybavení podpůrných IT systémů (zákaz používání USB portů, přihlašování do PC stanic, ochranu přístupových údajů, odhlašování z PC stanic při ukončení činností atd.). Pohled Boyera (2016) zahrnuje kromě výše uvedeného také techniku spear-phishingu[6], která v případě operátorů řídicího centra představuje další cestu k napadení energetických systémů, která zneužívá lidský faktor. Young (2015, s. 271–274) uvádí, že pro zmírnění rizika využití této techniky k napadení energetických systém je třeba důsledně oddělit infrastrukturu těchto systémů od podnikových sítí prostřednictvím firewallů s využitím technik monitorování a logování provozu na těchto firewallech.

Maglaras et al. (2018, s. 1). vidí potencionální hrozby zneužitelné pro napadení energetických systémů na úrovni elektrické stanice. Jako příklad uvádí možnost fyzického poškození zařízení. S Maglarasem et al. (2018, s. 1) se v pohledu na tuto problematiku shodují i Nezamoddini, Mousavian a Erol-Kantarci (2017, s. 329). Podle nich se jedná nejen o zařízení typu: IED, PLC, RTU, HMI a datové servery, ale také o podpůrnou infrastrukturu zahrnující klimatizační jednotky, napájení zařízení atd. Stejný pohled na tuto problematiku mají také Vaidya, Makrakis a Mouftah (2013, s. 6), kteří uvádí, že některá IED, PLC a RTU mají možnost úpravy konfigurace přímo prostřednictvím tlačítek a displeje umístěného na zařízení. Jako doporučení pro snižování hrozby, kterou představuje zneužití těchto zařízení, uvádí Vaidya, Makrakis a Mouftah (2013, s. 6) zabezpečení přístupu do těchto zařízení s využitím autentizačních mechanismů, tedy kombinace uživatelského jména a hesla. Pro zamezení nebo zmírnění útoku zaměřeného na fyzické poškození zařízení je třeba důsledně monitorovat a řídit přístup všech

[6]Principem spear-phishingu je cílené odesílání e-mailu jednomu příjemci. E-mail obsahuje přílohu se škodlivým kódem za účelem získání citlivých informací. Na rozdíl od klasického phishingového e-mailu, spear-phishingový email neobsahuje odkazy do internetu a od příjemce není požadováno zadání údajů, ale otevření přílohy obsahující škodlivý kód (Bimal, 2012, s. 8 – 9).

osob do technologických místností, kde jsou tato zařízení umístěna. Řízení přístupu do těchto prostor lze zabezpečit prostřednictvím systémů technické ochrany, které fungují na principu přístupu pomocí přístupové karty, kdy každá přístupová karta je vydávána do vlastnictví konkrétní osobě. Tím je zajištěna jednoznačná identifikace konkrétní osoby, která se v daném prostoru pohybuje. Součástí monitorovaných oblastí by neměly být pouze technologické místnost, ale celý vnější perimetr elektrické stanice. Přístup do oblasti vnějšího perimetru by měl být, stejně jako přístup do technologické místnost, povolen pouze na základě vlastnictví přístupové karty s příslušným oprávněním ke vstupu. Pro účely zvýšení zabezpečení a jednoznačné identifikace osob, vstupujících do elektrické stanice, a současně ochraně vnějšího perimetru je dále v elektrických stanicích typicky instalován kamerový systém se záznamem. V případě podezření na narušení fyzické bezpečnosti technologické místnosti je možné korelovat záznam z přístupového kartového systému a kamerového systému pro jednoznačnou identifikaci útočníka.

Ding et al. (2018, s. 1667–1668) se dívají na problematiku bezpečnosti energetických systémů z pohledu komunikací a komunikačních protokolů využívaných pro komunikaci mezi elektrickou stanicí a řídicím centrem energetické soustavy, tedy primárně v dnešní době využívané protokoly IEC 60870 a IEC 61850. Narušení dostupnosti, důvěrnosti a integrity dat souvisí především s využíváním technologie Ethernet a principů TCP/IP komunikace z elektrické stanice do řídicího centra, jak bylo uvedeno v předchozí části této práce věnované komunikacím a komunikačním protokolům. Riziko zneužití tohoto typů útoku se úměrně zvyšuje s přístupem útočníka do prostor, kde je umístěno technologické vybavení. Pokud bude mít útočník fyzický přístup do uvedených prostor, může využít volný port na aktivním prvku (switch, router) pro připojení dalšího zařízení (notebooku, laptopu, aktivního prvku), prostřednictvím kterého může útočník následně získat citlivá data nebo ovlivnit TCP/IP komunikaci směrem do řídicího centra. Pohled Stouffera Falca a Scarfoneho (2015, s. E1 – 2) na tuto problematiku zahrnuje pro zmírnění rizika zneužití komunikací využívání několika technických řešení. Jedná se o datovou diodu, šifrování, firewally, IDS a IPS systémy. Tento typ technologií doporučuje využít i Knapp a Broad (2011, s. 229–230)

- Datová dioda – jedná se o zařízení, které zajišťuje pouze jednosměrnou komunikaci. V oblasti energetických, resp. průmyslových řídicích systémů je její primární využití na rozhraní mezi průmyslovým řídicím systémem a podnikovými informačními systémy, ze kterých jsou čerpány informace o zákaznících apod.

- Šifrování komunikací – pokud to systém technicky umožňuje, doporučují Stouffer, Falco a Scarfone (2015, s. E-1) využívat šifrování komunikací.

- Firewally – firewally jsou běžně využívány pro zajištění oddělení komunikačních sítí za účelem ochrany a izolace průmyslových řídicích systémů. Využití nachází zejména u komunikací, které jsou založeny na protokolu TCP/IP, tedy IEC 60870 a IEC 61850. Stouffer, Falco a Scarfone (2015, s. E1) uvádí, že existují i specifické SW implementace firewallů pro protokol MODBUS.

- IDS a IPS systémy – jedná se o systémy, které analyzují datový provoz v komunikační síti a porovnávají jej se známými typy útoků, resp. signaturami, kterými disponují. IPS systémy navíc disponují možností přerušení komunikace v případě, že datový provoz vykazuje známky shodné se signaturami a jedná se tedy o potenciálně škodlivou komunikaci.

Zmírnění rizika zneužití tohoto typu útoku lze zajistit řízením přístupu a monitoringem prostor technologických místností a současně vypnutí všech nevyužívaných portů na aktivních prvcích. Komunikace na portech aktivních prvků by měla být povolována pouze na vyžádání v případě servisního zásahu. Staggs, Ferlemann a Shenoi (2017, s. 6) stejně jako Ding et al., (2018, s. 1667–1668) doporučují zavést autentizační mechanismy připojovaných zařízení do aktivních prvků např. pomocí technologie 802.1x a šifrování komunikace, pokud to daná zařízení podporují. Při zavedení technologie 802.1x je třeba důsledně monitorovat a logovat autentizaci klientů do komunikační sítě. Tato data slouží v případě napadení energetického systému jako jeden ze vstupů pro identifikaci útočníka v rámci vyšetřování příčin napadení systému.

Stouffer, Falco a Scarfone (2015, s. 5-25) se shoduje s Maglarasem et al. (2018, s. 1) a Vaidyou, Makrakisem a Mouftahem (2013, s. 6), kteří všichni vyzdvihují potřebu monitoringu, logování a auditování průmyslových řídicích systémů, komunikačních a bezpečnostních prvků, podpůrných IT systémů a systémů řízení přístupu tak, aby bylo v případě narušení jejich bezpečnosti k dispozici co nejvíce informací vedoucích k odhalení pachatele, příčin a technik, které vedli k narušení bezpečnosti.

Pro zajištění požadovaných informací z výše uvedených systémů existuje celá řada proprietárních i standardizovaných protokolů. V rámci síťových technologií a operačních systémů je v praxi nejpoužívanější protokol Syslog. Syslog je standardizovaný protokol, který je popsán v doporučení RFC5424 a umožňuje zařízením přenášet po počítačové síti informace

o prováděných operacích, aktivitách uživatelů apod. (Jarmakiewicz, Parobczak a Maślanka, 2017, s. 22) Většina komunikačních zařízení (routery, switche, firewally, RTU, IED) a operačních systémů v případě podpůrných IT technologií využívaných v energetických systémech je schopna produkovat syslog stream (Anastopoulos a Katsikas, 2017, s. 124).

3.3.1 Nástroje pro monitoring činností v energetických systémech

Zaznamenávání činnosti v energetických systémech s sebou přináší především problematiku velkého množství zařízení, ze kterých jsou zaznamenávány činnosti. Vzhledem ke komplexnosti a rozsáhlosti energetických systémů, počtu využívaných zařízení a využívaných technologií vzniká problém, kdy z takto velkého počtu zařízení je generováno velké množství záznamů, které není možné zpracovávat bez pomoci specializovaných nástrojů k tomu určených. Přidanou hodnotou využití těchto nástrojů je zejména zajištění využívání best-practises technik a postupů v oblasti řešení zaznamenávání činností a událostí..

V současné době zahrnují best-practises v oblasti zaznamenávání činností a událostí následující principy (Jarmakiewicz, Parobczak Maślanka, 2017; Madani, Rezayi a Gharaee, 2011):

- Dlouhodobé centrální ukládání zaznamenaných logů a událostí.
- Kontinuální analýza logů a událostí.
- Generování alarmových stavů v reálném čase.
- Vzájemná korelace událostí za účelem získání kontextu o určité aktivitě.
- Efektivní reakce na případné kybernetické útoky, úspěšnější detekce kybernetických útoků včetně vyšetřování hlavních příčin těchto útoků s využitím forenzní analýzy.
- Získávání automaticky vytvářených statistik o monitorované infrastruktuře.

Centrální zaznamenávání logů – princip je založen na zasílání definovaných logů ze zařízení využívaných v rámci infrastruktury, ve které mají být zaznamenávány činnosti. V rámci infrastruktury se typicky jedná o zařízení, aplikace a technologie, která jsou, nejen v případě energetických systémů vysoce heterogenní. Typicky se jedná o koncové stanice využívající různé operační systémy z rodiny Windows, případně Unix/Linux, dále komunikační zařízení typu router, switch, firewall, systémy pro detekci a prevenci průniku do komunikační sítě IDS/IPS servery, DLP servery, Honeypoty, antivirová řešení, e-mailové servery, proxy servery, load balancery, aplikační řešení apod. Heterogennost zařízení a aplikací spočívá nejen v účelu jejich použití ale i počet jejich výrobců je velice široký. Tato skutečnost se negativně promítá v syntaxi definující jednotlivé logy, kdy typicky

2 zařízení či aplikace sloužící ke stejnému či v případě aplikací podobného účelu od různých výrobců disponují odlišným formátem logování událostí. (Montesino, Fenz a Baluja, 2012, s. 250 - 252)

Dle Moosdijka a Wagenaara (2015) s sebou sběr logů z různých zdrojů přináší i nárůst počtu vyhodnocovaných bezpečnostních událostí. Jako příklad lze uvést proces autentizace uživatele k pracovní stanici. Autentizační proces generuje log záznamy na Active directory serveru, který ověřuje identitu uživatele. Dále je logován přístup na file server do domovské složky přihlášeného uživatele, přístup na SharePoint server apod. Proces přihlášení uživatele tedy v tomto konkrétním případě generuje velké množství logů a potenciálně velké množství bezpečnostních událostí, které musí být vyhodnocovány.

Analýza logů je založena na prezentaci logů, která jsou získávána z připojených zařízení. Analýza se stává při velkém množství připojených zařízení, a tedy nutnosti procházení velkého množství logů velice složitou záležitostí. Za účelem zjednodušení analýzy lze na logy, které jsou ukládány do centrální databáze aplikovat množinu filtrů a pravidel, které detekují odchylky od standardního stavu (Bryant a Saiedian, 2017, s. 198). Na základě detekované odchylky generují alarm, což vede ke urychlení v analýze kořenových příčin těchto událostí, protože operátor dohledu je automaticky upozorněn na podezřelou odchylku od normálního stavu. (Madani, Rezayi a Gharaee, 2011, s. 287-288)

Základem **korelace událostí** je automatická analýza ukládaných logů a především podmínek, které definují podezřelé aktivity, resp. bezpečnostní události včetně časového horizontu, ve kterém má být podmínka splněna. Podmínky jsou vyhodnocovány na základě výskytu typových logů, které jsou zaslány a uloženy do centrální databáze. Pokud je podmínka splněna, je bezpečnostní událost alarmována, což vede k urychlení analýzy příčin události a rychlejšímu rozhodování personálu ohledně aplikace reaktivních opatření. (Madani, Rezayi a Gharaee, 2011, s. 287–288; Qingrong Jason Wu et al.., 2017, s. 2334).

Reakce na bezpečnostní incidenty (Incident response) – jedná se o proces reakce na bezpečnostní incidenty. V rámci organizace je nutné mít jasně definovaná pravidla a postupy, které umožní adekvátně a v co nejkratším časovém úseku reagovat na bezpečnostní incident. V rámci procesu incident response by měly být zainteresovány všechny složky organizace, které proces implementují. Primárně se jedná o specialisty na bezpečnost, IT specialisty a administrátory systémů a aplikací. V rámci incident response procesu jsou často využívány i externí zdroje mimo danou organizaci. Využívání externích zdrojů souvisí zejména

s poskytováním specifických služeb v oblasti incident response těmito organizacemi. Jedná se především o služby v rámci zajištění důkazních materiálů z dohledových systémů pro případné soudní spory, specifické služby v oblasti provádění forenzní analýzy apod. Součástí některých systémů určených pro sběr a zpracování záznamů událostí, které jsou využívány v procesu reakce na bezpečnostní incidenty lze využívat i funkcionality tzv. aktivních odpovědí (akcí), které vedou ke zrychlení v procesu řešení bezpečnostních událostí. Praktickým příkladem je automatická akce zakázání uživatelského účtu v rámci Active Directory v případě zjištění bezpečnostní události ve formě nepovolené akce prostřednictvím konkrétního uživatelského účtu. Bez využívání aktivních odpovědí je nutné, aby v případě zjištění bezpečnostní události byla provedena daná konfigurační úprava (v tomto případě zakázání uživatelského účtu) správcem systému. Výhodou tohoto řešení je plná kontrola správce nad provedenými konfiguračními úpravami. Nevýhodou časová prodleva, která uplyne od zjištění bezpečnostní události až k provedení požadovaných konfiguračních úprav systému. V případě využívání aktivních odpovědí provede systém určený pro sběr a zpracování událostí automaticky příslušné konfigurační úpravy v daném systému s pomocí předem definované aktivní odpovědi. Vykonání automatické odpovědi je možné notifikovat příslušným pracovníkům prostřednictvím alarmového stavu, případně prostřednictvím emailových notifikací.

Forenzní analýza – Jedná se o hloubkovou analýzu při vyšetřování bezpečnostních událostí a incidentů. Cílem forenzní analýzy je detailní dokumentace, určení příčin a viníků jednotlivých bezpečnostních události a incidentů. V případě vyšetřování bezpečnostních incidentů prostřednictvím soudního dokazování slouží výstupy forenzní analýzy jako podkladové materiály v dokazovacím řízení.

Reporting – v případě využití centralizovaného přístupu ke kolekci logů je k dispozici komplexní pohled na monitorovanou infrastrukturu. Logy, resp. události se stávají cenným zdrojem informací o zajištění a nastavení bezpečnostních pravidel nejen infrastruktury jako celku ale také jejich dílčích částí. Pro účely reportování je nutné nalézt vhodnou formu, kterou budou informace prezentovány a reportovány. Na základě informací z reportů mohou být příslušné bezpečnostní parametry monitorovaných technologií upravovány a současně lze na základě získaných informací stanovit požadavky na monitorování činnosti u nově dodávaných systémů, případně rozšiřování stávajících systémů (Qingrong jason wu et al., 2017, s. 2334). Pro zajištění výše uvedeného je nezbytné disponovat reportovacím nástrojem obsahující sadu předdefinovaných reportů, které mohou být v případě potřeby modifikovány

nebo použity jako vzor při vytváření vlastních reportů. Součástí sady předdefinovaných reportů jsou v současných nástrojích ve většině případů i reporty reflektující shodu s právními předpisy – ISO 27000, GDPR[7], HIPAA[8], PCI/DSS[9] apod. (Reporting, 2019)

Pro zajištění efektivního monitoringu a naplnění požadavků definovaných v §24 vyhlášky o kybernetické bezpečnosti je vhodnou a doporučovanou technologií SIEM – Security information and event management. Využití nástrojů tohoto typu je doporučeno nejen vyhláškou o kybernetické bezpečnosti, ale je rovněž doporučeno v rámci pohledu na problematiku zaznamenávání činností v energetických systémech mezi odbornou veřejností.

Zejména Stouffer, Falco a Scarfone (2015, s. E1 - 2) doporučují za účelem zpracování a korektní intepretace shromažďovaných informací využít technologii SIEM. Zásadní předností SIEM řešení je možnost uživatelsky vytvářených korelačních pravidel, které kombinují informace z různých zdrojů, kdy při splnění definovaných podmínek je spuštěná předem definovaná akce a jsou tedy zajištěny požadavky definované v §24 vyhlášky o kybernetické bezpečnosti ohledně sběru, seskupování a vyhodnocování kybernetických bezpečnostních událostí včetně notifikací určených bezpečnostních rolí. Při správně nastavených korelačních a analytických funkcí SIEM je třeba podrobněji analyzovat pouze malé množství informací a nikoli celou získanou množinu informací ze všech zdrojů. Se Stoufferem, Falcem a Scarfonem (2015, s. E1) se v oblasti monitoringu a využívaných technologií pro monitoring v energetických systémech s důrazem na technologii SIEM plně shodují i Leszczyna (2018, s. 62), Jarmakiewicz, Parobczak Maślanka (2017, s. 22) a Nazir, Patel a Patel (2017, s. 449).

Technologie SIEM nepředstavuje jedinou možnou platformu, která je vhodná pro zaznamenávání činností a událostí v rámci energetických systémů. Za účelem zajištění provozního monitoringu je možné využívat i nástrojů, ze kterých se technologie SIEM postupně vyvíjela. Jedná se o nástroje typu SIM a SEM.

[7] GDPR – General Data Protection Regulation. Celým názvem Nařízení Evropského parlamentu a Rady (EU) č. 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů). V rámci GDPR jsou stanovena práva a pravidla pro ochranu osobních údajů fyzických osob, včetně definice, co je považováno za osobní údaje.

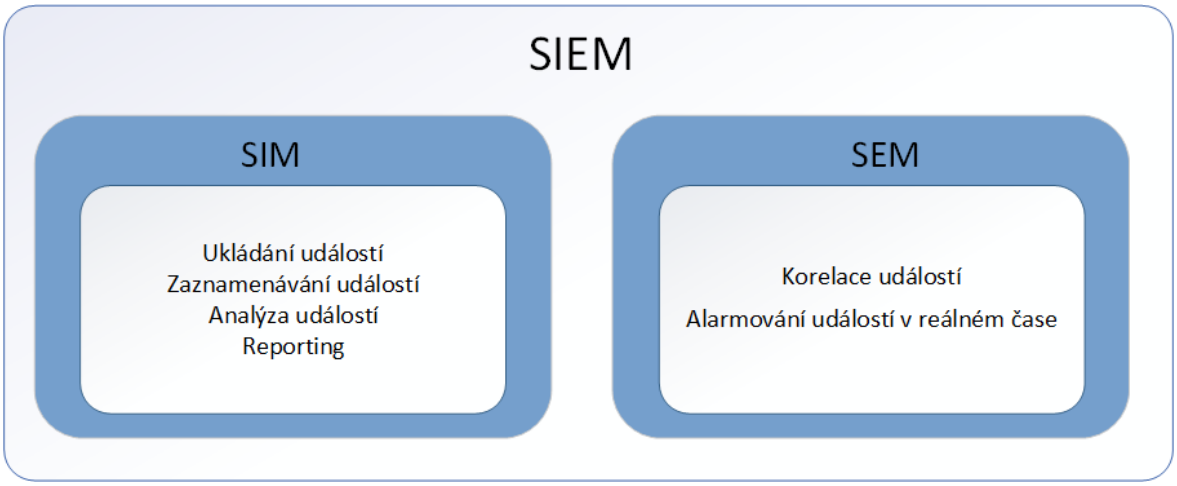
[8] HIPAA – Health Insurance Portability and Accountability Act. Jedná se o zákon na ochranu osobních údajů v oblasti zdravotnictví. V rámci zákona je vyžadována zabezpečená forma výměny lékařských záznamů a stanovuje pravidla ochrany záznamů uložených nejen elektronickou, ale rovněž papírovou formou

[9] PCI/DSS – Payment Card Industry Data Security Standard. Jedná se o soubor mezinárodních norem, který určuje požadavky na organizace, které uchovávají, zpracovávají nebo přenášejí data o držitelích platebních karet za účelem omezení zneužití těchto dat.

SIM představuje technologii, která slouží k dlouhodobému ukládání zaznamenávaných událostí, provádění analýz událostí a reportováním významných událostí. (Detken et al., 2015, s. 322). S Detkenem et al. (2015, s. 322) se shodují i Dairinram, Wongsawang a Pengsart (2016, s. 2) podle kterých se SIM systémy soustředí zejména na analýzu historických dat.

Základní rozdíl oproti technologii SIM je zaměření nástrojů typu SEM nejen na zaznamenávání událostí, ale především jejich vzájemných korelací a zajištění komplexního pohledu na vznik události včetně jejího alarmování v reálném čase prostřednictvím konzole aplikace (Detken et al., 2015, s. 322). Stejně jako v případě SIM systémů se v definici SEM systémů shodují s Detkenem et al. (2015, s. 322) i Dairinram, Wongsawang a Pengsart (2016, s. 2). V dnešní době jsou produkty typu SEM zastoupeny na trhu prostřednictvím segmentu produktů tzv. logmanagerů, které disponují uvedenými funkcionalitami typickými pro SEM systémy.

Obrázek 11 znázorňuje kombinaci technologií SIM a SEM, které společně tvoří základ pro systémy typu SIEM.



Obrázek 11 - Kombinace technologií SIM a SEM. Zdroj: vlastní zpracování

Porovnání dostupných SIEM systémů na trhu se dlouhodobě věnuje společnost Gartner Inc. Jedná se o vědecko-poradenskou společnost, zaměřující se na hledání optimálních řešení pro podnikání v oblasti informačních technologií. Společnost Gartner každoročně vydává Gartner Magic Qadrant, který srovnává pozice klíčových hráčů v různých oblastech informačních technologií z hlediska konkurenceschopnosti v definovaných oblastech informačních technologií a aktuálních trendů v dané oblasti. Základem Magic Quadrantu je úplnost vize dané společnosti, resp. produktu a jeho prostřednictvím tyto vize uvést na trh. Dle hodnocení společnost Gartner se tyto společnosti, resp. jimi dodávané SIEM systémy rozdělují do 4 kategorií – leadeři, vyzyvatelé, vizionáři a nevýznamní hráči. Obrázek

12 reflektuje Gartner Magic Quadrant pro rok 2018 v oblasti SIEM technologií. Mezi lídry se řadí SIEM systémy LogRhythm od stejnojmenné společnosti, Splunk's analytics-driven SIEM společnosti Splunk, IBM Security QRadar společnosti IBM a dále SIEM systémy společností Dell Technologies, Exabeam, McAfee a Securonix.

Obrázek 12 - Gartner Magic Quadrant SIEM 2018. Zdroj: Magic Quadrant for Security Information and Event Management (2019)

4 IMPLEMENTACE NÁSTROJŮ PRO MONITORING ČINNOSTÍ A UDÁLOSTÍ V ENERGETICKÝCH SYSTÉMECH

Při implementaci nástrojů, které reflektují požadavky na zaznamenávání činností v energetických systémech je nutné se zaměřit nejprve na obecná rizika, vyplývající z jejich implementace a dále na specifická rizika, která s sebou přináší implementace těchto řešení v rámci energetických systémů. Nástroje pro zaznamenávání činností a událostí mohou představovat velký přínos v rychlosti a schopnosti adekvátní detekce a reakce na bezpečnostní incidenty v rámci organizace, avšak efektivita návrhu, implementace, správy a využívání těchto systémů s sebou přináší mnoho problémů a výzev z technického, ekonomického a manažerského pohledu. Technický a ekonomický pohled zahrnují zhodnocení přínosů dané technologie, tedy nákladů z ekonomického pohledu a nástrojů pro efektivní provoz a správu dané technologie. K těmto účelům je vhodné využít standardizovaných přístupů, které se zaměřují na problematiku efektivního řízení s využitím principů IT Governance. Jedná se o zastřešující pojem, jehož cílem je umožnit dosažení efektivního využití efektivního využití dostupných zdrojů a současně minimalizaci rizik za využití ITSM (IT service management). IT governance disponuje zároveň přesahem do taktické a strategické úrovně řízení. Definuje principy pro zajištění strategických cílů organizace prostřednictvím procesního řízení. Z hlediska manažerského pohledu je klíčovou otázkou, jakým způsobem dosáhnout podpory procesu návrhu architektury systému, resp. řešení jako celku s vazbou na obchodní a strategické cíle organizace a současně maximalizovat efektivitu řešení po celou dobu jeho životnosti. V odborné literatuře jsou aplikovány přístupy se zaměřením na návrh architektury samotného řešení v kontextu zajištění plnění obchodních cílů společnosti. Návrh je založen na konceptech budování architektury rozsáhlých systémů, které se souhrnně označují jako rámce (frameworky) enterprise architektury.

4.1 Technický a ekonomický pohled

Z hlediska technického a ekonomického pohledu na danou problematiku lze spatřit zajímavé výsledky průzkumu z roku 2012, který se zabýval efektivitou nasazení nástrojů pro zaznamenávání činností a událostí s důrazem na SIEM systémy. Podle tohoto průzkumu z roku 2012, který citují Moosdijk a Wagenaar (2015), se 59 % respondentů setkalo se selháním implementace SIEM řešení z důvodu nedostatečných časových kapacit pro zajištění vyhodnocování bezpečnostních událostí a současně 40 % respondentů uvádělo jako velký problém časovou náročnost analýzy velkého množství dat. Moosdijk a Wagenaar (2015) dále citují průzkum z roku 2013, který provedla společnost EiQ Networks. Ve výsledcích průzkumu

je patrné, že ve 44 % dotazovaných organizacích byla doba nasazení SIEM řešení v řádu týdnů, resp. více než jednoho měsíce a současně bylo těmito organizacemi požadováno, aby se problematice správy SIEM řešení věnovali více než 2 zaměstnanci společnosti.

Odlišný pohled na problematiku nasazení a využívání SIEM v organizacích je součástí průzkumu, který realizovala v roce 2016 společnost Netwrix, která se zaměřuje na problematiku auditování IT systémů. Průzkumu proběhl v rámci 234 velkých společností, které působí ve více než 20 odvětvích podnikání (Netwrix Corporation, 2016). Součástí průzkumu byl rovněž výčet klíčových ukazatelů pro nasazení technologie SIEM, které korespondují s požadavky danými vyhláškou o kybernetické bezpečnosti a jsou tedy aplikovány i v rámci nasazení SIEM v energetických systémech. Jednalo se o detekci bezpečnostních hrozeb v reálném čase, efektivní analýzu příčiny bezpečnostních incidentů a reportování v souladu s ISO 27000. Výsledky průzkumu ukázaly, že pro 81 % zúčastněných organizací představovalo problém velké množství dat, která obsahují SIEM reporty. Na druhou stranu, pro 68 % organizací byly SIEM reporty nevyhovující a obsahovaly nekompletní data. Zároveň pro 63 % organizací bylo obtížné interpretovat data, která byla součástí SIEM reportů. Reportování požadovaných dat na vyžádání představovalo problém pro 65 % organizací. Za účelem eliminace těchto nevýhod a celkově lepšímu využívání SIEM technologie vnímalo 55 % organizací jako řešení zvýšení počtu kvalifikovaného personálu, případně zaškolení stávajícího personálu pro analytickou práci se SIEM řešením.

Podrobnější výzkum zaměřený na rizika implementace SIEM s názvem Dosažení optimalizace SIEM publikovaly v roce 2017 společnosti Ponemon Institute a Cyphort. Metodika výzkumu obsahovala dotazníkové šetření mezi 559 oslovenými IT specialisty v organizacích, které využívají SIEM řešení přičemž 11 % z nich podnikalo v oblasti energetiky a služeb s energetikou spojených. Z této množiny pracovalo se SIEM řešením na denní bázi 41 % respondentů. Administraci SIEM řešení se zabývalo 26 % z respondentů. Jako důležitý nástroj v oblasti monitoringu činností a analýzy příčin bezpečnostních incidentů SIEM vnímalo 76 % respondentů, ale pouze 46 % respondentů bylo spokojeno s rozsahem a přesností dat, která SIEM poskytuje pro efektivní analýzu příčin bezpečnostních incidentů. Celkově 30 % respondentů zároveň uvedlo, že nasazení SIEM nesplnilo očekávání organizace. V 51 % případů byla očekávání naplněna a v 19 % případů implementace SIEM předčila původní očekávání. (Ponemon institute, 2017)

Součástí výzkumu je také sedm problémů, které jsou organizacemi vnímány jako limitující pro efektivní využívání SIEM řešení. Jedná se o:

- Automatizování úloh generovaných systémem SIEM tak, za účelem jejich prioritizace.
- Zajištění větší viditelnost síťového provozu v rámci organizace pro zajištění komplexního pohledu na infrastrukturu.
- Vytváření přesnějších alarmových upozornění.
- Navýšení počtu pracovníků, kteří jsou schopni adekvátně analyzovat bezpečnostní události v SIEM.
- Zajištění uceleného pohledu na kontext týkající se uživatelů a zařízení, které jsou spojeny s bezpečnostními událostmi v SIEM.
- Omezení provozních dat které nesouvisí s bezpečnostními událostmi.[10]

Zajímavým výsledkem provedeného výzkumu je počet pracovníků, kteří mají v gesci administraci a údržbu SIEM řešení. Pouze 22 % respondentů uvedlo, že v dané organizaci je více než jeden pracovník, který se zabývá touto problematikou. Ve 36 % organizací je tato problematika v gesci pouze jednoho pracovníka a 42 % organizací má k dispozici méně než jednoho pracovníka.

Průměrné roční náklady související s provozováním SIEM v jedné organizaci byly 3,9 milionu USD. Největší část, 33 % z této částky tvořily náklady na lidské zdroje, především ve formě zaškolení pracovníků pro zajištění efektivní analýzy bezpečnostních událostí v SIEM. Náklady na instalaci a údržbu tvořily 34 % z celkové částky. Zbylých 33 % financí bylo využito na pořízení HW a SW vybavení potřebného pro provozování SIEM.

Na základě provedených průzkumů lze konstatovat, že nasazení a využívání SIEM systémů s sebou nese následující významná rizika, která rovněž uvádí MkaCyber (2019) a Inns (2014):

- SIEM řešení je finančně nákladné – dle výsledků průzkumu Ponemon institute tvoří náklady na pořízení HW a SW SIEM 25 % z celkově vynaložených finančních nákladů. Zbylých 75 % pak pokrývají náklady na údržbu, instalaci a lidské zdroje, kdy 78 % respondentů nemá k dispozici více, než jednoho pracovníka na administraci a údržbu SIEM řešení.

[10] Jedná se zejména o data na úrovni debug a information. V běžném provozu systémů aplikací je generováno velké množství těchto provozních dat, která typicky nemají charakter související s výskytem bezpečnostních událostí a v případě jejich integrace do SIEM řešení snižují přehlednost a orientaci v rámci analýz prováděných v systému.

- Implementace a administrace SIEM funkcionalit je náročná na lidské zdroje – vzhledem k datům z průzkumu společnosti Netwrix, kdy 68 % respondentů uvedlo, jako limitující faktor, nekompletnost reportů s požadovanými daty a zároveň pro 65 % respondentů představovalo problém získání požadovaných reportů ze SIEM na vyžádání. Tento problém lze částečně řešit s využitím vytvoření reportů prostřednictvím dodavatele SIEM řešení, což s sebou ale přináší zvýšené finanční náklady.

- Analýza bezpečnostních událostí vyžaduje kvalifikovaný personál – více než 44 % respondentů.

- Generování nepotřebných dat – SIEM řešení generují velké množství dat, která nejsou třeba k analýze bezpečnostních událostí a snižují přehlednost a orientaci v rámci prováděných analýz.

- Neexistence kontextu u alarmových stavů – v případě notifikace bezpečnostní události formou alarmů jsou postrádány informace o rozsahu problému v kontextu týkajícího se dotčených uživatelů a zařízení.

Rizika neefektivity nasazení nejen SIEM řešení, ale v obecné rovině nasazení a provozování nástrojů pro zajištění komplexního zaznamenávání činností v rámci energetických systémů, se ztotožňují s výše uvedenými riziky. V případě komplexnosti a nehomogennosti technologií, které jsou v rámci energetických systémů včetně podpůrných IT systémů využívány, je možnost nasazení nástrojů pro zaznamenávání činností a událostí velice rozsáhlá – od nasazení monitoringu činností v rámci řídicího centra, přes nasazení v rámci monitoringu činností na prvcích komunikačních tras mezi řídicím centrem a transformovnami/rozvodnami, případně komunikačních tras mezi řídicími systémy a podnikovou IT infrastrukturou až po nasazení a využívání v rámci zaznamenávání činností komunikačních prvků v rámci transformoven/rozvoden a technologických prvků (RTU, IED, PLC).

K implementaci nástrojů pro zaznamenávání činností a událostí systémů v energetických systémech tedy nelze přikročit chaoticky ale musí být zvolen systematických přístup, který zajistí nejen efektivní využívání zvoleného řešení, ale především bude mít pro společnost provozující energetické systémy také přidanou hodnotu ve formě rychlé a adekvátní reakce na bezpečnostní události a incidenty, včetně kontextových informací týkajících se dané události a především přehledných a komplexních reportů z provozovaných systémů jako celku.

4.2 Správa IT služeb

Nástroje a principy zabývající se problematikou efektivního provozu a správy dané technologie nebo poskytované služby jsou v odborné literatuře a rovněž širokou veřejností označovány pod souhrnným pojmem správa IT služeb. Správa IT služeb je konceptem, jehož snahou je maximální využití IT prostředků pro naplnění obchodních cílů organizace. Správa IT služeb pokládá za základní prostředky pro naplnění cílů organizace právě IT služby, kdy jejich prostřednictvím, resp. interním a externím využíváním vzniká přidaná hodnota pro organizaci. Správa IT služeb pokrývá celý životní cyklus služby od strategického návrhu služeb, přes zavedení služeb do provozu a jejich využívání na operativní úrovni, až po neustálé zlepšování služeb pro zajištění maximální efektivity práce a přidané hodnoty pro organizaci (Žáček, 2019). Nejlepší zkušenosti a postupy v řízení IT služeb popisuje mezinárodní standard ITIL®.

4.2.1 ITIL®

ITIL®[11] – information technology infrastructure library, (dále ITIL) – je mezinárodním standardem obsahující prověřené koncepty a postupy pro zajištění efektivního plánování a využití informačních technologií v rámci organizace i mimo ni prostřednictvím dodavatelů a zákazníků dané organizace (Vozdecký, 2013, s. 11–13). V literatuře je název volně překládán jako knihovna infrastruktury IT. V současné době se spíše setkáme s vazbou ITIL na pojem správa služeb IT (IT service management), kdy ITIL poskytuje rámec pro tuto správu. Pokud není citacemi uvedeno jinak, vychází tato kapitola z literatury Bucksteeg (2012) a školících materiálů ITIL® Foundation společnosti Axelos Limited.

Základním principem ITIL je orientace na procesní řízení a řízení životního cyklu IT služeb. ITIL není metodikou, poskytuje pouze rámec pro správu IT služeb založený na zkušenostech z nejlepší praxe. Velká výhoda ITIL je jeho plná kompatibilita s normami skupiny ISO 9000 který reprezentuje systém managementu jakosti, tedy schopnost dosáhnout v rámci výroby a distribuce produktů a služeb v požadované kvalitě ke koncovému zákazníkovi.

Vzhledem k tomu, že v rámci ITIL je pracováno s pojmy událost, incident a dalšími, které mají v rámci procesního řízení specifický význam, který zcela nekoresponduje s výše uvedenými

[11] ITIL® je registrovaná ochranná známka společnosti AXELOS Limited, používaná na základě povolení společnosti AXELOS Limited.

definicemi těchto pojmů z hlediska informační a kybernetické bezpečnosti, budou nejprve tyto pojmy definovány z hlediska ITIL.

Aktiva – zdroj nebo způsobilost. Aktiva poskytovatele služby zahrnují vše, co může přispět k dodávce služby. Typy aktiv mohou mýt následující: management, organizace, proces, znalost, lidé, informace, aplikace, infrastruktura a finanční kapitál.

Incident – neplánované přerušení služby IT nebo omezení kvality služby IT. Incidentem je rovněž porucha konfigurační položky, která dosud neovlivnila službu – například porucha jednoho ze zrcadlených disků v diskovém poli.

IT správa služeb – Implementace a správa kvality IT služeb prostřednictvím poskytovatelů IT služeb s využitím kombinace lidských zdrojů, procesů a informačních technologií.

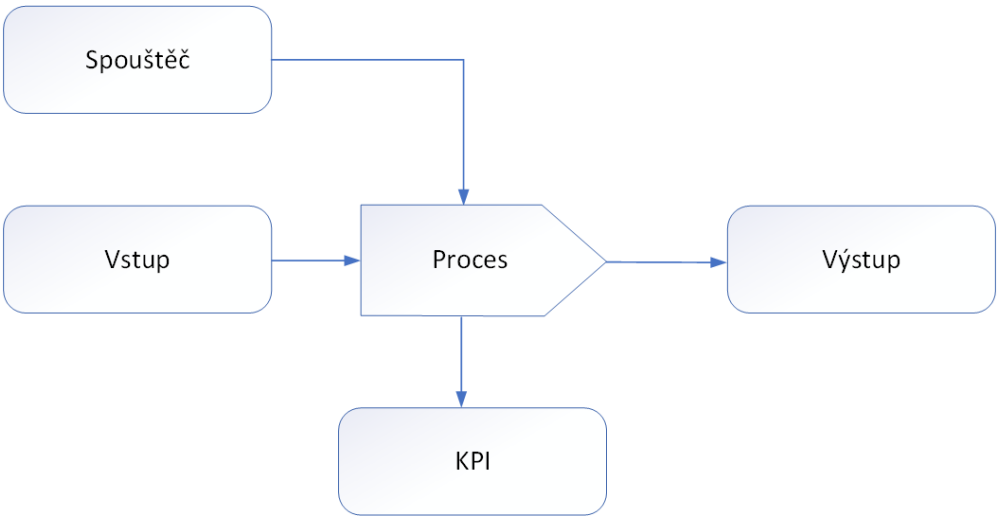
KPI (Key Performance Indicators) – metrika pro měření parametrů IT služby, procesu nebo činnosti.

OLA (Operational Level Agreement) – jedná se o popis IT služby a definici kvalitativních a kvantitativních parametrů mezi poskytovatelem IT služby a funkčním celkem v rámci organizace, který tuto službu využívá. Funkční celek může být v organizaci reprezentován například oddělením, odborem, útvarem apod.

Problém – příčina jednoho nebo více incidentů. Příčina obvykle není známa v čase vytvoření záznamu o problému a proces správy problémů je odpovědný za jeho další zkoumání.

Proces – strukturovaná množina činností navržená pro dosažení určitého specifického cíle měřitelným způsobem. Sestává z množství prostředků a činností. K prostředkům může patřit personál, finanční zdroje, zařízení, instalace, techniky a metody. Prostředky a činnosti jsou ve vzájemném vztahu. Každý proces musí mít vždy vlastníka. Proces může v případě potřeby definovat politiky, normy/standardy, směrnice, činnosti a pracovní instrukce. Proces je popsán postupem a pracovními instrukcemi. (Vozdecký, 2013, s. 10)

Obrázek 13 reprezentuje obecné schéma ITIL procesu. Součástí procesu je spouštěč, který vyvolává spuštění procesu a představuje vnější aktivity (triggery). Proces vyžaduje vstupy, se kterými pracuje a transformuje na výstupy představující přidanou hodnotu. Každý proces zároveň vytváří vstupy pro hodnocení PKI.



Obrázek 13 - Obecné schéma ITIL procesu. Zdroj: upraveno dle školících materiálů ITIL® Foundation

SLA (Service Level Agreement) – dohoda o úrovni služeb – jedná se o popis IT služby a definici kvalitativních a kvantitativních parametrů mezi poskytovatelem IT služby a zákazníkem. Praktickým příkladem je stanovení parametrů v případě nutnosti servisního zásahu u IT služby, u které jsou stanoveny úrovně závažnosti a kritičnosti dané IT služby dle následujícího rozdělení:

- Priorita A: reakce poskytovatele do 1 hodiny od zjištění problému v režimu 24 hodin / 7 dní v týdnu
- Priorita B: reakce poskytovatele do 4 hodin od zjištění problému v režimu 8 hodin / 5 dní v týdnu
- Priorita C: reakce následující pracovní den

SLA lze nastavit podle následujících kritérií. (Vozdecký, 2013, s. 11)

- Perspektiva služeb – SLA je vytvořena k příslušné službě a platí pro všechny zákazníky dané služby. Typickým příkladem jsou SLA týkající se připojení zákazníka k Internetu.
- Definice z pohledu orientovaného na zákazníka – SLA je vytvořena pro každého zákazníka v rámci všech služeb, které využívá.
- Definice z pohledu organizace – SLA je vytvořena pro balíček služeb, které podporují business organizace. Příkladem je podnikový informační systém dané organizace.

- Víceúrovňové SLA – jedná se o kombinaci výše uvedených. Pro skupinu zákazníků jsou dohodnuty obecné SLA, které jsou dále detailně rozpracovány do úrovně většího detailu pro jednotlivé služby.

Služba – prostředek pro tvorbu přidané hodnoty, kdy zákazník nemusí nést přímé náklady a rizika spojená se zavedením služby. Služby využívají způsobilosti a zdroje, resp. aktiva (Vozdecký, 2013, s. 11).

Událost – změna stavu, která je významná z hlediska řízení konfigurační položky nebo služby IT. Pojem je také používán ve významu výstrahy nebo upozornění pocházejících od služby IT, konfigurační položky nebo monitorovacího nástroje. Události obvykle vyžadují, aby pracovník provozu IT provedl nějakou činnost, a často vedou k registraci incidentu.

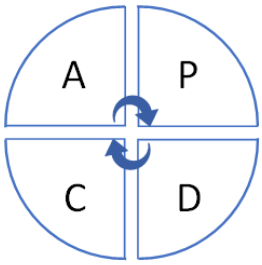
Zdroj – obecný termín zahrnující IT infrastrukturu, osoby, peníze nebo cokoli co umožňuje poskytování IT služby. Za zdroje jsou považovány aktiva organizace.

Způsobilost – schopnost organizace, člověka, procesu, aplikace, konfigurační položky nebo služby IT vykonávat činnost. Způsobilost je nehmotné aktivum organizace.

Historie ITIL se začala psát již v roce 1985 ve Velké Británii prostřednictvím agentury CCTA (Central Computer and Telecommunications Agency). Původní verze obsahovala soubor 40 publikací zaměřených na best-practices v oblasti doručení IT služeb. Projekt prošel postupným vývojem a v letech 2000 až 2002 byla představena ITIL verze 2 (v2). Obsahem ITIL v2 bylo osm knih. Základními stavebními kameny byly dvě knihy. Kniha Service Support se zaměřením na služby pro podporu koncových uživatelů a kniha Service Delivery se zaměřením na služby pro podporu podnikání zákazníka. Součástí dalších čtyřech knih je popis procesů, které tvoří podporu pro koncové uživatele a podporu podnikání prostřednictvím dodávaných služeb. Jednalo se o knihy Security Management, ICT infrastructure management, Application management a Software Asset management. Procesy plánování služeb a propojení s potřebami podnikání jsou součástí knih Planning to Implement Service Management a Bussiness Perspective. Součástí ITIL v2 je rovněž kniha popisující implementaci ITIL s názvem ITIL V2 Small-scale Implementation.

Spolu s vydáním verze 2 se ITIL rozšířil do s mnoha zemí celého světa. V roce 2007 byla vydána ITIL v3, která byla novelizována v roce 2011 a je často označována jako ITIL 2011 Edition. Základním principem ITIL v3 je orientace na životní cyklus služby. Novelizace provedená v roce 2011 reagovala na zpětnou vazbu uživatelů týkající se zřetelnější

evidence, srozumitelnosti a konzistentnosti v tematických oblastech a procesech ITIL. Cílem ITIL v3 je optimalizace a současně zlepšení celého procesu doručení IT služeb v požadované kvalitě. Pro tento účel využívá ITIL Demingův cyklus, který je také označován jako PDCA cyklus. Obrázek 14 zobrazuje Demingův cyklus, který je založen na formě postupného opakování čtyř činností zajišťující kontinuální zlepšování kvality služby. (Žáček, 2019)



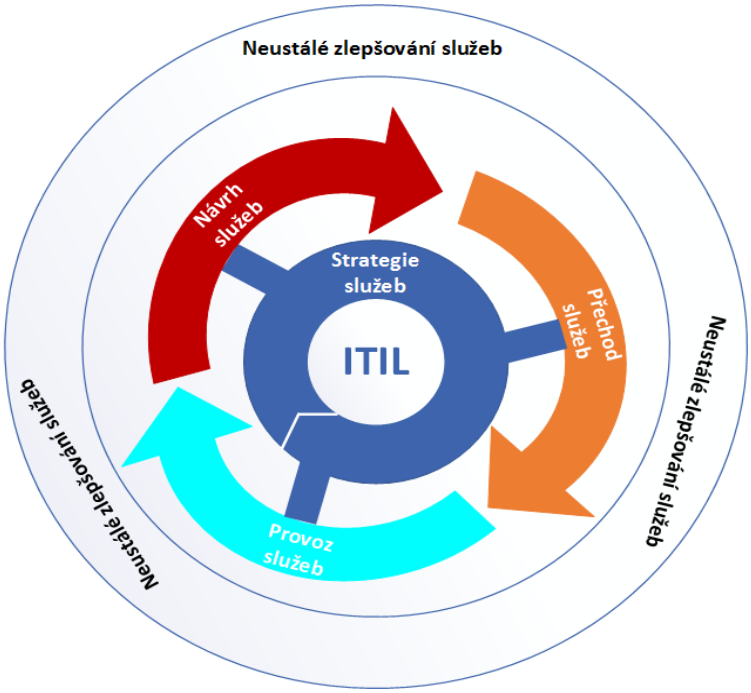
Obrázek 14 - PDCA cyklus. Zdroj: upraveno dle školících materiálů ITIL® Foundation

- P – Plan – plánování zlepšení IT služby formou záměru
- D – Do – plán je realizován
- C – Check – ověření, že realizace splňuje podmínky definované záměrem
- A – Act – na základě ověření jsou provedeny úpravy záměru a případně realizace.

Následuje implementace zlepšení do produkčního prostředí. Každá organizace, která chce implementovat ITIL si zároveň musí uvědomit, že neexistuje konkrétní ITIL řešení. Rámec ITIL musí být vždy přizpůsoben skutečným podmínkám v dané organizaci.

Součástí ITIL v3 je soubor 5 knih, které definují kompletní životní cyklus IT služeb. Obrázek 15 zobrazuje kompletní životní cyklus IT služeb dle ITIL v3.

- Service Strategy (strategie služeb)
- Service Design (návrh služeb)
- Service Transition (uvedení služeb do provozu)
- Service Operation (provoz služeb)
- Continual Service Improvement (systém neustálého zlepšování služeb)



Obrázek 15 – Životní cyklus ITIL. Zdroj: upraveno dle školících materiálů ITIL® Foundation

V době tvorby této práce bylo připravováno vydání další inovované verze ITIL s názvem ITIL v4. Vzhledem k faktu, že při psaní této práce nebyla ještě verze ITIL v4 plně vydána, je v práci dále popisována primárně verze ITIL v3. Dalším důvodem pro využití ITIL v3 je, že autor práce je současně držitelem certifikátu ITIL Foundation v3. V podnikové praxi je zároveň běžným faktorem využití již nasazené metodiky v co nejdelším časovém úseku z důvodu investic velkých finančních prostředků do její implementace, školení personálu apod. Jako hlavní argument pro přechod na novější verzi metodiky vidí Čermák (2013, s. 11) chybějící popis potřebných procesů nebo nové postupy, které nová verze přináší.

Součástí uvedených knih ITIL v3 je celkem 26 procesů, které podrobně definují kroky potřebné k zavedení jednotlivých oblastí dle ITIL.

Tabulka 6 udává komplexní přehled těchto procesů.

Tabulka 6 - Přehled procesů ITIL v3. Zdroj: vlastní zpracování

Strategie služeb	Návrh služeb	Přechod služeb	Provoz služeb	Neustálé zlepšování služeb
Strategie IT služeb	Koordinace návrhu	Plánování a podpora přechodu	Správa událostí	Proces zlepšování v 7 krocích
Správa financí	Správa katalogu služeb	Správa změn	Správa incidentů	
Správa portfolia služeb	Správa dostupnosti	Správa aktiv služeb a konfigurací	Správa problémů	
Správa poptávky	Správa kapacit	Správa releasů a nasazení	Plnění požadavků	
Správa vztahů s byznysem	Správa kontinuity IT služeb	Validace a testování služeb	Správa přístupů	
	Správa úrovní služeb	Vyhodnocení změn		
	Správa bezpečnosti informací	Správa znalostí		
	Správa dodavatelů			

Procesy v rámci **strategie služeb** specifikují využívání IT služeb k dosažení vlastních cílů prostřednictvím cílů svých zákazníků, kteří využívají IT služby. Správa IT služeb představuje strategické aktivum organizace. Účelem strategie IT služeb je definice pozice, plánů, perspektivy a vzorců chování za účelem naplnění výstupů byznysu organizace.

Správa strategie IT služeb – v rámci procesu správy strategie IT služeb jsou generovány strategické cíle společně s jejich vazbou na strategii organizace. Cílem je vytvoření strategie

IT služeb plně v souladu se strategií organizace. V rámci procesu probíhají analýzy interního a externího prostředí dané organizace s cílem identifikace potencionálních příležitostí pro poskytování IT služeb. Proces využívá koncept tzv 4P – perspective (perspektiva), position (pozice), plan (plán), pattern (vzorce chování organizace).

- Perspektiva – zahrnuje hodnoty a cíle organizace, které ovlivňují chování organizace jako celku
- Pozice – reprezentuje vnímání poskytovatele IT služby z pohledu zákazníka
- Plán – pozice organizace na konkurenčním trhu s výhledem jejího rozvoje ve vztahu ke konkurenci
- Vzorce chování organizace – reprezentují vzorce chování organizace, definované na základě perspektivy, pozice a plánu, které vedou k dlouhodobému úspěchu společnosti na trhu.

V rámci procesu správy strategie IT služeb je přidaná hodnota získávána formou správného určení priorit při zajištění investičních nákladů potřebných pro provozování a zlepšování IT služeb, což vede k úspoře finančních prostředků vzhledem k jejich účelovému a nikoli chaotickému plánování. Koordinace činností v rámci procesu správy strategie IT služeb je v kompetenci vlastníka tohoto procesu.

KPI definují aktuálnost strategických, operativních a taktických plánů a případné odchylky od těchto plánů.

Správa financí – v rámci procesu správy financí je zajištěno sestavení a dodržování finančního plánu potřebného pro zavedení nové IT služby, případně úpravy stávající IT služby. Proces správy financí je zodpovědný za rovnováhu mezi vynaloženými finančními náklady a zajištění IT služby v požadované kvalitě a s požadovanými parametry. Cílem procesu správy financí je rovněž dohledatelnost všech finančních operací souvisejících se zavedením, resp. úpravě poskytované IT služby. KPI jsou stanoveny vedením organizace. Mezi klíčové ukazatele patří aktuální náklady na provoz IT služeb včetně dodržování finančního plánování. Účtování služeb zákazníkům a nastavení procesu správy financí je v kompetenci finančního manažera.

Správa portfolia služeb – proces zajišťuje správu nejen katalogu služeb, tedy služeb, které jsou nasazeny v rámci produktivního provozu, ale také zásobníku služeb, který obsahuje

IT služby ve fázi plánování nebo vývoje, ale tyto nejsou nasazeny v rámci produktivního provozu, a tedy dostupné zákazníkům. Součástí správy portfolia služeb je i seznam stažených služeb, které nejsou poskytovány zákazníkům, ale existuje předpoklad jejich budoucího využití. Správa portfolia služeb se řídí pomocí PDCA cyklu.

Správa poptávky – v rámci procesu poptávky jsou analyzovány uživatelské požadavky na poskytované IT služby a identifikovány příležitosti pro zlepšení poskytování stávajících IT služeb, resp. zavedení nových služeb, které korespondují se strategií poskytování IT služeb a zhodnocení přínosu jejich zavedení pro organizaci, resp. poskytovatele.

Proces správy poptávky úzce spolupracuje s procesem správy kapacit, který je odpovědný za převod poptávky po IT službách do konkrétních plánů a aktivit, které jsou potřebné k realizaci.

Správa vztahů s byznysem – cílem procesu je pochopení klíčových potřeb zákazníka a zajistit podporu při zavedení nových IT služeb prostřednictvím zajištění odpovídající nabídky na zákaznickou poptávku včetně dosažení dohody o úrovni poskytovaných služeb. Za tímto účelem je vhodné využívání dohodnutého komunikačního kanálu, prostřednictvím kterého budou řešeny požadavky zákazníka, případně stížnosti a reklamace v rámci poskytovaných IT služeb. Dílčím cílem procesu je sledování nových a vylepšení stávajících využívaných technologií, které mohou přispět ke zlepšení poskytování stávajících IT služeb.

Procesy v rámci **návrhu služeb** jsou zaměřeny na návrh a tvorbu IT služeb, které tvoří přidanou hodnotu pro zákazníka a současně plně reflektují **strategii služeb**. Návrh, přechod a provoz služby tvoří životní cyklus služby. V rámci návrhu služby jsou pokryty obchodní požadavky, jejich analýza a dokumentace. Dalším krokem je vytvoření služby zahrnující zajištění technologií, procesů a vhodných metrik pro měření kvality. Součástí vývoje je dokumentace a přehled všech relevantních dokumentů pro vývoj a implementaci služby včetně dokumentace souladu návrhu služby se strategií organizace. Tato dokumentace je obsažena v tzv. Service Design Package (balíček návrhu služby), který je vytvářen pro každou novou IT službu, resp. velkou změnu týkající se IT služby. Součástí balíčku návrhu služby je mimo výše uvedenou dokumentaci také soubor vstupů popisujících požadavky byznysu, funkční a provozní požadavky na IT službu, návrh komponent IT služby, plán přechodu služby do produkčního provozu, SLA a OLA, kritéria pro akceptaci služby a posouzení připravenosti organizace pro zavedení a provoz IT služby z hlediska obchodního, finančního a technického.

Koordinace návrhu – cílem procesu koordinace návrhu je zajištění jednotného místa, které koordinuje návrh služby jako celek. Jedná se především o koordinaci a kontrolu architektonického řešení, výběru vhodných technologií, definici procesů a metrik použitých v rámci návrhu IT služby. Koordinace návrhu zahrnuje rovněž plánování a hodnocení zdrojů potřebných pro návrh a hodnocení rizik v případě výskytu otevřených otázek při návrhu IT služby. Přidaná hodnota procesu spočívá především v zajištění jednotného architektonického řešení poskytovaných IT služeb.

Správa katalogu služeb – proces zajišťující správnost a aktuálnost informací v rámci katalogu služeb, zejména detail popisu služby, stav IT služby, rozhraní, závislosti na dalších využívaných a plánovaných službách, podpůrnými komponenty a konfiguračními položkami. Katalog služeb obsahuje všechny IT služby v přechodu a produkčním provozu. Cílem procesu správy katalogu služeb je dále především koordinace a odsouhlasení portfolia služeb a katalogu služeb s odpovědnou osobou procesu Správy portfolia služeb. ITIL doporučuje v rámci procesu správy katalogu služeb udržovat hierarchickou strukturu ve formě služeb směřovaných k zákazníkům na jedné straně a podpůrných služeb na straně druhé. Služby směřované k zákazníkovi jsou služby viditelné zákazníkem. Podpůrné služby poskytují podporu služeb směrovaných k zákazníkům, ale zákazníci je nevidí. Jedná se zejména o služby infrastruktury a aplikací, které tvoří zázemí pro služby směrované k zákazníkům.

Správa dostupnosti – proces kontroly dostupnosti IT služby vzhledem k dohodnutým parametrům dostupnosti IT služby. Proces pokrývá celý životní cyklus dostupnosti IT služby zahrnující definici, plánování, implementaci a měření. Součástí procesu je definice plánu dostupnosti vzhledem k požadavkům na údržbu IT služby a posouzení vlivu na dostupnost v případě nutnosti provedení změny v rámci IT služby. Správa dostupnosti zahrnuje také analytickou podporu zákazníkům při problémech týkajících se dostupnosti IT služby.

Správa kapacit – cílem procesu správy kapacit je nalezení efektivního využívání a plánování IT služeb ve vztahu k zajištění potřebné IT infrastruktury a lidských zdrojů tak, aby IT služby byly dodány s požadovanými parametry, včas a s využitím přiměřených finančních prostředků. Kapacita představuje maximální propustnost, kterou poskytuje IT služba nebo konfigurační položka, při dodržení dohodnuté úrovně poskytovaných služeb. Příkladem kapacity konfigurační položky je maximální prostor diskového uložiště.

Proces správy kapacit lze implementovat dvěma způsoby, případně jejich kombinací. Proaktivní způsob předpokládá vytváření prediktivních analýz využití stávajících zdrojů a změnových požadavků na IT služby. Tímto způsobem lze odhalit kapacitní a výkonnostní problémy s časovým předstihem a zajistit adekvátní reakci např. formou pořízení nového HW vybavení, zajištění lidských zdrojů apod. Reaktivní způsob je založen na monitorování a reportování kapacit zdrojů. Kapacitní nebo výkonnostní problémy jsou řešeny až v době jejich výskytu.

Spouštěčem procesu je překročení prahových hodnot týkající se výkonových problémů, případně požadavky na novou nebo změněno službu, která vyžaduje navýšení stávajících kapacit. Vstupy procesu jsou tvořeny zejména informacemi o službách, informace o komponentách IT infrastruktury, informace z procesů správy incidentů, událostí a problémů apod. Výstupem procesu jsou kapacitní plány, kapacitní reporty a CMIS (informační systém správy kapacit) který zaznamenává výsledky aktivit jednotlivých procesů. Kapacitní plány obsahují scénáře odpovídající současným a budoucím požadavkům organizace a zákazníků na dodávku IT služeb, kdy jsou zohledněny zdroje potřebné pro zajištění současných a budoucích požadavků.

KPI jsou reprezentovány ukazateli vytíženosti, kapacitními plány, seznamy volných kapacit apod.

Správa kontinuity IT služeb – proces podporující Business Continuity Management (správu kontinuity byznysu). Vzhledem k faktu, že poskytování IT služby je závislé na využívání informačních technologií, je třeba zajistit zabezpečení proti selhání klíčových komponent, které se podílí na zajištění dodávky IT služby. Na základě identifikace klíčových komponent je provedena Business Impact Analýza (BIA), která zohledňuje dopad na obchodní procesy v případě negativní události, které mohou ovlivnit poskytování IT služby. Součástí procesu je také hodnocení rizik aktiv a IT služeb.

Cílem procesu správy kontinuity IT služeb je předcházení nouzovým stavům, tedy nedostupnosti IT služby v důsledku selhání klíčových komponent pomocí snižování míry identifikovaných rizik na akceptovatelnou úroveň a definice strategie obnovy v případě nouzového stavu nebo mimořádné situaci.

Spouštěčem procesu jsou zejména nové nebo změněné cíle v SLA a OLA, výskyt velkého množství incidentů a hodnocení rizik jednotlivých aktiv a služeb. Vstupem procesu jsou

zejména informace o službách, strategické informace o organizaci, informace ze správy kapacit a správy financí. Výstupem procesu je aktualizovaná strategie kontinuity IT služeb, aktualizovaná BIA a analýza rizik, plány testování a plány kontinuity.

Správa úrovní služeb – proces zajišťující smluvní ošetření požadavků na poskytovanou úroveň dostupnosti služeb. Realizace všech aktuálně využívaných a plánovaných IT služeb podle domluvené úrovně jejich dostupnosti. Mezi poskytovatelem a zákazníkem jsou odsouhlasena SLA včetně metod jejich vyhodnocování. Obsahově se SLA skládají z popisu a definice služby včetně definice povinností poskytovatele a zákazníka. Nedílnou součástí SLA je dále definice vyjádření kvality služeb (typicky prostřednictvím požadované procentuální dostupnosti služby ve sledovaném časovém období), postupy schvalování změn IT služby, definice a formát zprávy sloužící pro finanční vyúčtování IT služby, platební podmínky, ceny a předpisy týkající se autorských práv, odstoupení od smlouvy, výpovědní lhůty, utajení a zveřejňování informací apod.

Spouštěčem procesu jsou zejména změn v portfoliu služeb a nové nebo upravené SLA a OLA. Vstupem do procesu jsou zejména informace z byznysu společně s portfoliem a katalogem služeb. Výstupy procesu jsou tvořeny zejména reporty o službách a přepracované smlouvy a dohody o úrovni poskytovaných služeb.

KPI jsou vyhodnocovány například na základě průzkumu spokojenosti zákazníků s využívanými IT službami, případně počet dodržených SLA.

Odpovědnou osobou za proces správy úrovní služeb je manažer úrovní služeb.

Správa bezpečnosti informací – účelem tohoto procesu je zajištění bezpečnosti aktiv, informací a dat z hlediska důvěrnosti, dostupnosti a integrity. Hodnotu aktiv, informací a dat musí specifikovat sama organizace. Součástí ochrany je vytvoření politiky bezpečnosti informací, která jasně definuje práva a povinnosti pro nakládání s daty a informacemi. Vhodným doplněním je zavedení systému správy bezpečnosti informací (ISMS), který mimo politiku bezpečnosti informací obsahuje také ověřené praktiky pro zajištění bezpečnosti informací v informačních systémech, jak již bylo uvedeno dříve. Bezpečnostní požadavky by měly být zahrnuty do příslušných SLA včetně definice odpovědností poskytovatele a zákazníka IT služby.

Spouštěčem procesu jsou zejména změny v interních bezpečnostních předpisech a porušení definovaných bezpečnostních pravidel. Vstupy procesu jsou tvořeny zejména interními

bezpečnostními předpisy organizace, portfolio a katalog služeb, porušení SLA, informace o provedených změnách případně informace o dodavatelích. Výstupem procesu jsou aktualizované bezpečnostní předpisy, management bezpečnosti informací a bezpečnostní audity.

KPI reprezentují počet identifikovaných bezpečnostních incidentů.

Správa dodavatelů – proces zajišťuje dodržování smluvních závazků s dodavateli, případně třetími stranami tak, aby organizace byla schopna plnit cíle a parametry poskytovaných IT služeb svým zákazníkům a současně všechny smlouvy s dodavateli a třetími stranami podporovaly strategii a potřeby organizace. Organizace musí mít k dispozici jasná pravidla pro práci s dodavateli, která jsou spolu s ostatními daty uchovávána v SCMIS (informační systém správy dodavatelů a smluv). Za účelem určení kritičnosti a závislosti organizace na dodavatelích je nutno provádět analýzu rizik jednotlivých dodavatelů a jejich kategorizaci. Kategorizace může být prováděna dle různých klasifikačních kritérií, např. dle rizikovosti na úroveň strategickou (strategické partnerství), taktickou (dodavatel HW a SW) a operativní (dodavatel kancelářských potřeb).

Procesy v rámci **přechodu služeb** jsou zaměřeny na správu a koordinaci funkcí, procesů a systémů, které jsou nezbytné pro sestavení, testování a nasazení nových IT služeb do produkčního prostředí. Cílem procesu je plánování, řízení a provádění nasazení nových IT služeb. Všechny změny IT služby musí probíhat řízeným způsobem pomocí procesu právy změn.

Plánování a podpora přechodu – v rámci tohoto procesu jsou zajištěny plány a koordinace potřebných zdrojů pro přechod IT služby do produkčního provozu tak, aby byly naplněny požadavky vytvořené při návrhu IT služby. Vstupem do procesu plánování a podpory přechodu je Service Design Package (balíček návrhu služby).

Spouštěčem procesu je schválené RFC nebo balíček návrhu služby. Vstupem do procesu plánování a podpory přechodu je schválený balíček návrhu služby nebo RFC. Výstup procesu je tvořen strategií přechodu služby včetně plánu přechodu obsahující finanční náročnost.

KPI jsou definovány prostřednictvím splnění požadavků na přechod služby z hlediska finančních nákladů, rozsahu, kvality, dodržení termínů a spokojenosti zákazníků s komunikací

mezi poskytovatelem a zákazníkem týkající se plánování přechodu IT služby do produkčního provozu.

Správa změn – principem správy změn je snaha o minimalizaci počtu incidentů a výpadků, které jsou způsobeny změnami v rámci IT služeb. Management změn zajišťuje zaznamenávání, posuzování, schválení, prioritizaci, plánování, testování, implementaci a dokumentaci změn kontrolovaným způsobem. Všechny změny konfiguračních položek jsou zaznamenávány, za účelem zajištění správnosti a aktuálnosti informací. ITIL rozlišuje tři typy změnových požadavků.

Prvním typem je normální změna, která se týká jedné nebo více konfiguračních položek nebo služby. Normální změna vyžaduje zadání požadavku na změnu a jeho schválení schvalovací autoritou změny. Druhým typem změny je standardní změna. Jedná se o změnu s nízkým rizikem vzniku incidentu a je vyřízena prostřednictvím standardních postupů pro zpracování, u kterých v minulosti proběhl schvalovací proces. Třetím typem změn je změna naléhavá, která je třeba provést rychle. Doporučení v rámci ITIL je minimalizovat počet naléhavých změn.

Schvalování změn je dvojího typu. Ke schvalování normálních, resp. standardních změn dochází v rámci poradního výboru pro změny. Členové představují zainteresované strany v procesu managementu změn, kteří hodnotí a schvalují požadavky na změny z hlediska své odbornosti. Schvalování naléhavých změn je pověřen poradní výbor pro naléhavé změny. Ve srovnání s poradním výborem pro změny je počet jeho účastníků nižší z důvodu rychlejšího svolání členů v případě potřeby.

Spouštěčem procesu je RFC. Vstupem do procesu správy změn je RFC. Na základě typu změny probíhá schvalovací proces, jehož výstupem je schválení změny, odmítnutí změny, případně provedení změn nebo vytvoření nových konfiguračních položek.

KPI jsou vyhodnocovány na základě četnosti změn a podílu úspěšně zavedených změn.

Správa aktiv služeb a konfigurací – pro zajištění dodávky služeb je nezbytné mít komplexní přehled o aktivech, která jsou v rámci služeb využívána. Informace o aktivech musí být spolehlivé a správné. Základem konfiguračního managementu je konfigurační databáze (CMDB) a konfigurační položka. Konfigurační položka je aktivem služby, které musí být spravováno za účelem dodávání služby v požadovaných parametrech. Každá konfigurační položka obsahuje několik atributů, které jsou nositeli informací o dané

položce. Pro správu konfiguračních položek slouží konfigurační databáze. Součástí konfigurační databáze je rovněž definování vazeb mezi jednotlivými konfiguračními položkami pro zajištění komplexního přehledu konfiguračních položek zajišťujících dodávku služby.

Spouštěčem procesu jsou zejména aktualizace z procesu správy změn, aktualizace z procesu správy releasů a nasazení a požadavků na službu. Vstupem do procesu správy aktiv služeb a konfigurací jsou zejména obsahy balíčků návrhu služby, informace z registru aktiv apod. Výstupem procesu je nový nebo změněný záznam konfigurační položky, dále aktualizované záznamy o aktivech, případně aktualizované informace o atributech a vztazích konfiguračních položek.

Správa releasů a nasazení – jedná se o proces, který zodpovídá za plánování a řízení sestavení, testování a nasazení IT služby. Hlavním cílem managementu nasazení nových verzí a služeb je dodávka služby zákazníkovi v rozsahu specifikovaném v návrhu služby. Nové verze – release – jsou nasazovány na základě jedné nebo více autorizovaných požadavků na změnu služby. Obsah nové verze je uložen v bezpečném uložišti, kterým je knihovna médií (data management library), ze kterého je uvolněn do produkčního prostředí.

Validace a testování služeb – proces zajišťující, že nové, případně upravené IT služby splňují požadavky organizace a odpovídají návrhu. Principem validace služeb je ověření IT služby z hlediska plnění stanoveného účelu a cílů specifikovaných v návrhu. Současně s validací se ověřuje i verifikace, tedy potvrzení, že IT služba správně plní stanovené požadavky. V rámci testování IT služby před nasazením do produkčního provozu jsou definovány testovací scénáře a akceptační kritéria pro akceptaci služby. Smyslem testovacích scénářů je zajištění opakovatelnosti testů s totožnými parametry kdykoli v budoucnu.

Vyhodnocení změn – cílem procesu je koordinace poskytovatele a zákazníka ve smyslu očekávání od nasazených změn IT služeb. Změny IT služby by měly být vždy vyhodnoceny před její samotnou implementací. Kritéria vyhodnocení jsou reprezentována zejména přidanou hodnotou změny dané služby a dopadem na fungování ostatních IT služeb. V případě zjištění významných rozdílů mezi skutečnou a očekávanou přidanou hodnotou dané změny je třeba konzultace poskytovatele a zákazníka IT služby a nalezení kompromisního řešení.

Spouštěčem procesu je požadavek na provedení vyhodnocení změny. Vstupem procesu může být balíček návrhu služby, případně návrh na změnu spolu s dokumentací změny. Výstup procesu reprezentuje závěrečná zpráva o vyhodnocení změny.

Správa znalostí – účelem procesu správy znalostí je sdílení zkušeností, poznatků a informací během celého životního cyklu IT služby napříč organizací, za účelem zajištění informovaného rozhodnutí v době, kdy je vyžadováno. Za účelem správy znalostí, informací a dat je využíván Service Knowledge Management System (systém správy znalostí o službách). Součástí tohoto systému je Knowledge base (znalostní báze) reprezentovaná databázovou strukturou obsahující data využívaná systémem správy znalostí o službách. Nezbytnou součástí procesu je definice komunikačního plánu, který definuje postupy poskytování informací včetně popisu, komu mohou být informace poskytnuty, v jakém časovém intervalu, v jaké formě a za jakým účelem.

Spouštěčem procesu je například aktualizace katalogu služeb, vytvoření kapacitního plánu apod. Vstupem do procesu jsou všechny využívané informace a znalosti. Spouštěčem procesu jsou zejména požadavek na aktualizaci katalogu a portfolia služeb. Výstupem jsou znalosti uložené v systému správy znalostí o službách.

Procesy v rámci **provozu služeb** reprezentují část životního cyklu služby, která je pro zákazníka klíčová. Účele je koordinace a plnění aktivit a souvisejících procesů pro zajištění dodávky IT služby zákazníkům v požadované úrovni dostupnosti. Důležitým faktorem provozu služeb, který organizace v mnoha případech opomíjejí je vytváření povědomí o existenci a správné funkčnosti IT služby jak interně v rámci organizace, tak externě v rámci stávajících a potencionálních zákazníků. Součástí provozu služeb je také kontinuální prosazování jejich zlepšování a rozvoje ale také školení zaměstnanců. Zajištění provozu služeb je dle ITIL založeno na využívání čtyř funkcí. Funkce jsou organizační jednotky (oddělení, týmy) disponující specifickými znalostmi z dané oblasti, které jsou odpovědné za provádění procesu. Jedná se o funkce Service Desk, technická správa, správa provozu IT a správa aplikací.

- Service Desk reprezentuje jediné kontaktní místo mezi poskytovatelem IT služeb a zákazníkem. Typický Service Desk spravuje incidenty a požadavky na IT službu a obstarává komunikaci s uživateli. Hlavním cílem Service Desku je obnovit normální režim služeb uživatelům co nejdříve, jak je to možné. Důležitým faktorem úspěchu je především okruh zaměstnanců Service Desku. Je třeba sladit potřeby organizace,

personální obsazení, úroveň dovedností a trénink (Vozdecký, 2013, s. 10). KPI jsou v rámci Service Desku variabilní. Typicky jsou reprezentovány procentem vyřešených incidentů, spokojenost uživatelů, čas do přijetí telefonického hovoru apod.

- Účelem technické správy je správa a rozvoj technické infrastruktury a technických týmů které mají infrastrukturu v gesci. Cílem funkce technické správy je plánování, implementace, správa a provoz stabilní technické infrastruktury nezbytné pro provoz IT služeb. V každodenní praxi se pro technickou správu v dnešní době používá termín technická podpora. KPI jsou vyhodnocovány na základě výkonnosti technologie (míra využití, výkonnost platforem, dostupnost), případně ukazateli údržby a střední dobou mezi poruchami.

- Správa provozu IT zodpovídá za každodenní údržbu a správu IT infrastruktury zajišťující poskytování služeb dle dohodnutých SLA. KPI jsou vyhodnocovány prostřednictvím počtu bezpečnostních narušení infrastruktury, spotřeby elektrické energie a finančních nákladů.

- Správa aplikací je zapojena v každé fázi životního cyklu služby aplikace od návrhu, přes přechod, provoz a neustálé zlepšování. Správa aplikací je podporou při návrhu aplikace, jejím testování a nasazení do produkčního provozu. Samotná aplikace může být součástí více než jedné poskytované IT služby. Aplikace může pro svůj běh využívat více než jeden server. Mezi KPI se řadí spokojenost uživatelů, čas odezvy aplikace, dostupnost aplikace, čas řešení incidentů a počty transakcí.

Správa událostí – účelem procesu správy událostí je detekce, kategorizace, rozhodování o reakci na událost, porovnání vazeb mezi událostí a dalšími událostmi včetně nalezení vazeb a řízení životního cyklu událostí. Událost je dle ITIL definována jako *„změna stavu, mající význam pro konfigurační položku nebo IT službu“*. Sledování událostí probíhá na základě detekce nastavených prahových hodnot u konfigurační položky, IT služby nebo monitorovacího nástroje. ITIL doporučuje řízení životního cyklu události prostřednictvím Service Desku. Evidence událostí je soustředěna na jednom místě. V rámci Service Desku lze definovat klasifikaci událostí, kroky eskalace, zapojení správy incidentů a problémů, správa znalostí apod. V rámci ITIL jsou definovány čtyři typy událostí:

- Informace – jedná se o událost, která představuje korektní akci a nevyžaduje žádnou reakci. Příkladem takové události může být přihlášení uživatele do systému, doručení emailu, spuštění aplikace apod.

- Varování – událost vyvolaná dosáhnutím prahové hodnoty u konfigurační položky nebo IT služby. Událost vyvolává potřebu sledování situace a přijetí vhodných opatření, která sníží riziko poruchy konfigurační položky, resp. IT služby.

- Výjimka – událost, kdy konfigurační položka, resp. IT služba nefunguje korektně. Příkladem může být výpadek serveru, velká časová prodleva při používání aplikace apod. Tyto události jsou předávány do procesu správy incidentů.

- Alarm – jedná se o automatickou notifikaci konkrétní osoby o tom, že nastala určitá událost. Notifikace jsou zasílány prostřednictvím emailových nebo SMS zpráv a obsahují všechny relevantní informace o dané události.

Spouštěčem procesu správy událostí je notifikace, která je kvalifikována jako výjimka, varování nebo informace. Vstupem procesu jsou zejména požadavky na úroveň služby, prahové hodnoty a požadavky z návrhu a přechodu IT služby. Pokud je událost vyhodnocena jako neplánované porušení nebo snížení kvality IT služby jedná se o incident a v Service Desku je vytvořen odpovídající záznam o incidentu. Výstupem procesu je záznam události v Service Desku, eskalace událostí, zahájení incidentu či problému.

KPI reprezentuje počet, případně podíl událostí, které byly vyhodnoceny jako incidenty nebo problémy.

Správa incidentů – primárním cílem incident managementu je sledování a kategorizace neplánovaných porušení nebo snížení kvality IT služby. K incidentu vždy existuje záznam obsahující detailní známé informace o incidentu, životní cyklus incidentu. Záznam v průběhu výskytu incidentu nabývá různých stavů (otevřeno, zpracovává se, předáno, vyřešeno, uzavřeno). Hlášení incidentu je vždy zaznamenáno v Service Desku, kde je současně evidován celý životní cyklus incidentu. Zásadní vliv na následné kroky v procesu řešení incidentu má určení jeho kategorizace, která určuje, jaké znalosti budou potřeba k vyřešení incidentu. Stejný vliv jako kategorizace má i určení priority, která určuje rychlost zpracování incidentu dle SLA definovaných u dané služby. Priorita může během procesu řešení incidentu nabývat různých hodnot. Za účelem řešení incidentu jsou k dispozici tři úrovně podpory,

kdy každá vyšší úroveň má k dispozici lidské zdroje s hlubšími znalostmi, vice času a dalších zdrojů potřebných pro řešení incidentů.

Vstupem a současně spouštěčem procesu je nahlášený incident. Výstupem procesu je obnovení IT služby, uzavření incidentu a zpětná vazba od uživatelů IT služby o jejím obnovení.

KPI jsou hodnoceny za základě počtu hlášených incidentů a jejich kategorizace, případně podle zaznamenávání dostupnosti IT služeb a porušených SLA.

Správa problémů – jedná se o proces, který zodpovídá za správu problémů v rámci jejich životního cyklu. Problém vzniká jako příčina výskytu jednoho nebo kombinací více incidentů, kdy není v čase vytvoření problému známé řešení a nelze tedy incident vyřešit a zajistit obnovení služby v rámci dohodnutých SLA. V případě potřeby se v průběhu řešení problému vystavuje požadavek na změnu v rámci managementu změn.

Spouštěčem procesu je jeden nebo kombinace více incidentů, kdy není známá příčina jejich výskytu. Vstupem do procesu jsou záznamy problému, záznamy o známých chybách a informace z procesu správy událostí a incidentů. Výstupy procesu tvoří aktualizované záznamy o problému, aktualizované záznamy ve znalostní bázi, požadavek na změnu, případně využití náhradního řešení, které zajistí obnovení IT služby v co nejkratším čase.

KPI jsou vyhodnoceny na základě snížení četnosti poruch na základě vyřešení problémů, času a nákladům potřebným na vyřešení problémů.

Správa požadavků – cílem procesu správy požadavků je zajištění kanálu pro uživatele IT služeb, prostřednictvím kterého mohou žádat o informace, rady, případně zpřístupnění IT služby. V tomto případě není vyžadováno zadání požadavku na změnu služby. Příkladem může být reset hesla konkrétního uživatele, zpřístupnění IT služby novému uživateli, dodávka standardního vybavení zaměstnanci apod. Jako standardní komunikační kanál je využíván Service Desk. Proces přináší přidanou hodnotu ve formě efektivního přístupu ke standardním službám s využitím centralizovaného přístupu prostřednictvím Service Desku.

Vstupem a současně spouštěčem procesu správy požadavků je uživatelský dotaz na poskytnutí informace nebo rady týkající se IT služby. Výsledkem je vyřešený požadavek obsahující pozitivní nebo negativní výsledek dotazu. Výsledek dotazu může ovlivnit i další komponenty, jako aktualizaci konfiguračních položek, požadavek na změnu apod.

KPI jsou vyhodnocovány podle počtu zpracovaných požadavků, času vyřešení požadavků, nákladů na vyřešení a spokojenosti zákazníků.

Správa přístupů – proces odpovědný za to, že uživatelé mohou využívat IT služby, data a aktiva. Prostřednictvím procesu je napomáháno k zajištění důvěrnosti, dostupnosti a integrity dat. Přístup je typicky definován na základě úrovní, které specifikují rozsah funkcí a dat, ke kterým má uživatel přístup. Přístup je přidělován uživatelské identitě. Uživatelská identita reprezentuje unikátní jméno identifikující uživatele, osobu nebo roli. Uživatelská identita má přiděleny kromě přístupu i práva, která definují povolené akce nad dostupnými funkcemi a daty. Uživatelé, kteří disponují stejnými přístupovými právy mohou být seskupovány do uživatelských skupin.

Proces neustálého zlepšování služeb – proces odpovědný za průběžné přizpůsobování IT služeb na měnící se byznys požadavky. Zaměřuje se primárně na efektivnost IT služby, sekundárně na optimalizaci nákladů na služby a maximalizaci účinnosti. Implementace procesu neustálého zlepšování služeb s sebou často přináší nutnost organizačních změn, které mění způsob práce v organizaci. Za účelem zlepšování služeb je nutné identifkovat příležitosti pro zlepšení a s nimi související IT služby, procesy, systémy apod.

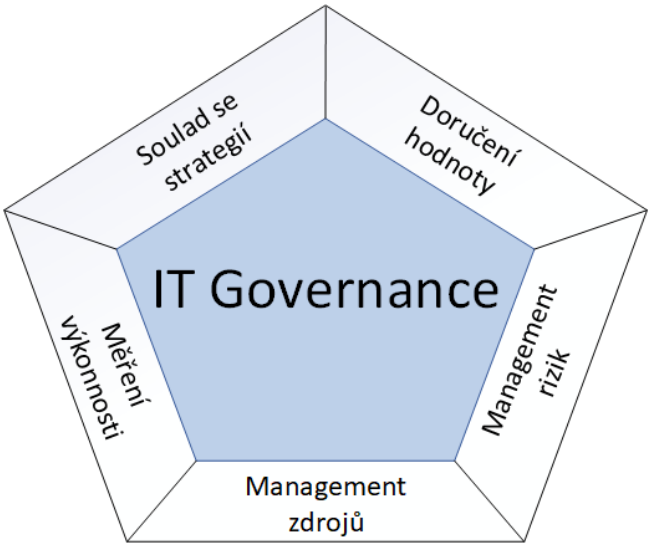
Proces neustálého zlepšování je založen na 7 krocích:

1. Určení strategie – identifikace vizí a potřeb byznysu a cílů týkajících se provozu IT služeb.
2. Identifikace co, kdy a jak se bude měřit.
3. Sběr dat – určení kdo využívá jaká data, kdy jsou data využívána a jakým způsobem.
4. Zpracování dat – určení frekvence zpracování dat, formát zpracování a nástroje a systémy pro zpracování dat.
5. Analýza dat a informací – identifikace trendů, cílů a potřeba zlepšení.
6. Prezentace a využití informací – souhrnné posouzení analýzy dat a informací.
7. Implementace řešení.

4.2.2 COBIT

COBIT představuje další ze standardů zaměřených na oblast informačních technologií s vazbou na zajištění IT služeb. Na rozdíl od ITIL je COBIT zaměřen na evoluci IT služeb s využitím principů jejich proaktivního řízení a zaměření na dlouhodobé cíle organizace Standard COBIT představuje rámec pro tzv. IT Governance. Vydavatelem a současně vlastníkem autorských práv COBIT je mezinárodní organizace ISACA a publikace COBIT tedy nejsou veřejně přístupné. ISACA je nezisková globální asociace založena již v roce 1969. Hlavní činností ISACA je vydávání a používání best-practise postupů v oblasti informačních systémů a informačních technologií jako celku. V současné době se ISACA zabývá oblastmi informační bezpečnosti, kybernetické bezpečnosti, IT Governance, řízení rizik, inovací a výkonností organizací jako celku.

Obrázek 16 identifikuje 5 základních oblastí zaměření IT Governance dle Hosseinbeiga, Karimzadgan Moghadama a Moghadama (2011, s. 3) a Rychlého (2015, s. 9). Stejný pohled na tuto problematiku mají i Alkhaldi, Hammami a Ahmar Uddin (2017, s. 1)



Obrázek 16 - 5 oblastí zaměření IT Governance. Zdroj: upraveno dle (Rychlý, 2015, s. 9)

- Strategic Alignment (soulad se strategií) – IT Governance by měla podporovat strategické cíle organizace
- Value Delivery (doručení hodnoty) – IT Governance by měla přinášet přidanou hodnotu zákazníkům služeb a byznysu
- Risk Management (management rizik) – Součástí IT Governance by mělo být řízení rizik

- Resource Management (management zdrojů) – IT Governance by měla řídit zdroje zahrnující infrastrukturu, informace, aplikace a personál
- Performance Measurement (měření výkonnosti) – Součástí IT Governance by mělo být stanovení měřitelných cílů a jejich měření

Celkovou zodpovědnost za rozvoj informačních technologií tak, aby bylo dosaženo strategických cílů má dle IT Governance nejvyšší vedení organizace, resp. příslušné statutární orgány (Čermák, 2013, s. 6). S Čermákem se v tomto pohledu shodují i Fazlida a Said (2015, s. 246). Jiný pohled na tuto problematiku má Rychlý (2015, s. 7–8), který rozšiřuje seznam účastníků IT Governance o další zainteresované strany:

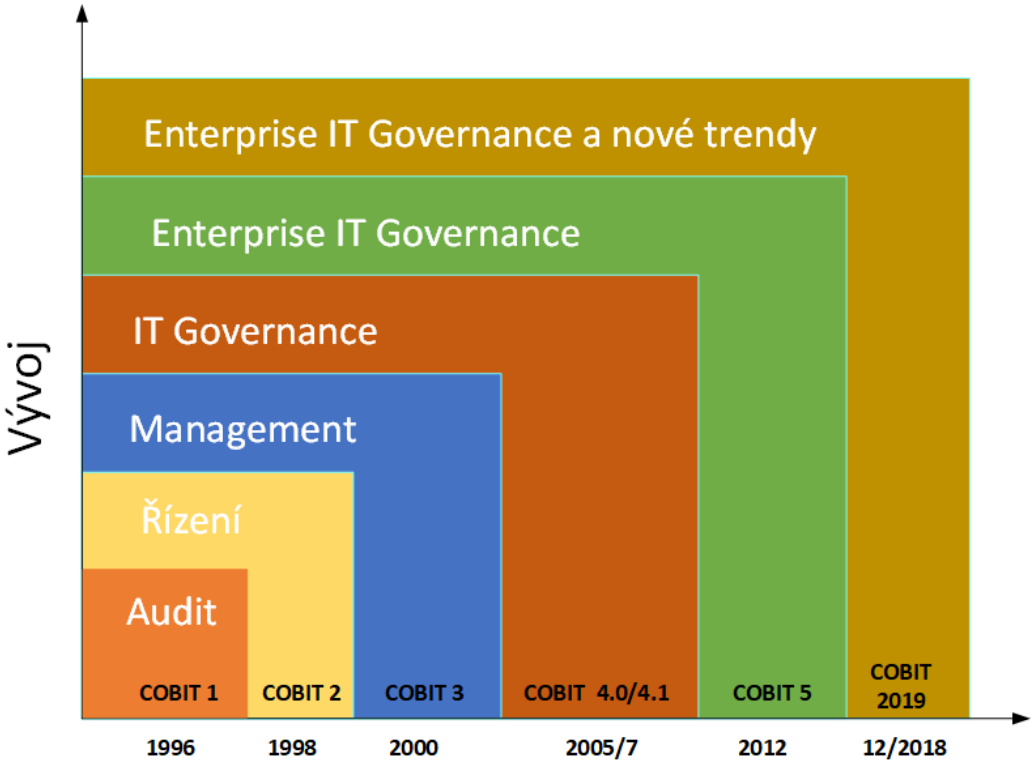
- Byznys manažeři – definují byznys požadavky na IT, zaručují doručení hodnoty a správy rizik.
- IT manažeři – dle požadavků byznysu zajišťují dodávky IT služeb.
- Interní IT auditoři – zajišťují nezávislou kontrolu poskytování IT služeb.
- Manažeři rizik a Compliance manažeři – monitorují a vyhodnocují rizika a dodržování shody IT se závazně platnými předpisy.

COBIT je zároveň využíván odbornou veřejností při provádění IT auditů.

Mezi základní vlastnosti COBIT jako rámce pro IT Governance patří (Rychlý, 2015, s. 11):

- Orientace na procesní řízení.
- Zaměření na podporu byznysu formou mapování procesů na byznysové cíle.
- Definice jednoznačného názvosloví procesů, rolí apod. a současně významového slovníku.
- Podpora integrace se standardy, legislativními předpisy, interními a externími audity.

Historie COBITu sahá do roku 1996 kdy byla vydána první verze zaměřená na provádění auditů informačních technologií. Obrázek 17 zobrazuje postupný vývoj COBITu, který byl spolu s novými verzemi rozšiřován o další auditní postupy nebo implementační nástroje.



Obrázek 17 - Vývoj COBIT. Zdroj: upraveno dle Čermáka (2013, s. 11)

Zaměření COBIT na problematiku IT Governance je patrné od roku 2012 s příchodem verze COBIT 4.0, která byla roku 2007 upravena a vydána jako verze 4.1. V roce 2012 byla vydána verze COBIT 5.0, která rozšiřovala verzi 4.1 a byla více zaměřena na problematiku podnikové IT Governance. V prosinci roku 2018 bylo oznámeno vydání zatím poslední verze označovaná jako COBIT 2019.

Vzhledem k faktu, že při psaní této práce nebyla ještě verze COBIT 2019 plně vydána, je v práci dále popisována primárně verze COBIT 5. V podnikové praxi je zároveň běžným faktorem využití již nasazené metodiky v co nejdelším časovém úseku z důvodu investic velkých finančních prostředků do její implementace, školení personálu apod. Jako hlavní argument pro přechod na novější verzi metodiky vidí Čermák (2013, s. 11) chybějící popis potřebných procesů nebo nové postupy, které nová verze přináší.

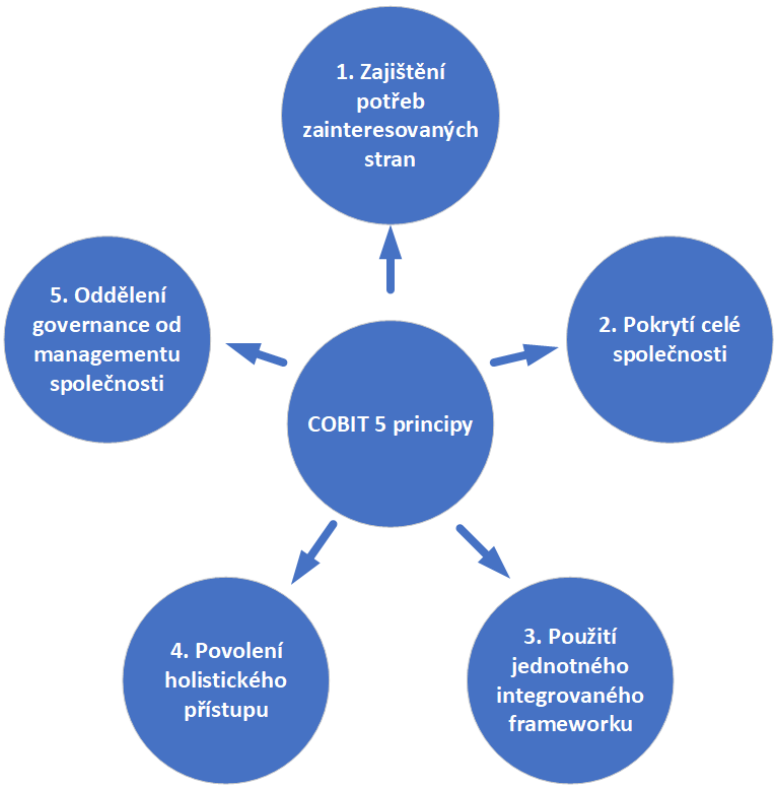
COBIT 5 je tvořen sadou následujících dokumentů:

- COBIT 5 Framework – popis základního rámce (principy, předpoklady a vazby na jiné rámce).
- COBIT 5 Enablers Guides (Enabling Processes, Enabling Information) – obecné rady a doporučení pro efektivní správu IT.

- COBIT 5 Professional Guides (Implementation, Information Security, Assurance, Risk) – dokumenty určené pro specialisty.

- COBIT 5 Online Collaborative Enviroment – on-line dokumenty, ve kterých mají uživatelé možnost sdílení zkušeností a poznatků z výše uvedených dokumentů.

Hlavní změnou v rámci COBIT 5 oproti verzi COBIT 4 je bylo zavedení nových principů (De Haes, 2013, s. 15–24). Obrázek 18 uvádí sadu 5 principů COBIT 5.



Obrázek 18 - COBIT 5 principy. Zdroj: upraveno dle De Haes et al. (2013, s. 15)

Zajištění potřeb zainteresovaných stran – (vedení společnosti, zaměstnanců, zákazníků, dodavatelů apod.) s využitím rovnováhy mezi realizací přínosů, mírou rizika a využití zdrojů tak, aby snaha o zajištění potřeb zainteresovaných stran byla realizovatelná. COBIT 5 dává organizaci k dispozici sadu procesů, které tyto potřeby podporují prostřednictvím využívání IT. COBIT 5 zároveň poskytuje informačně-centrický pohled na podnik. Informace by měly podporovat podnikové cíle a zajistit hodnotu pro zainteresované strany. Kaskáda cílů COBIT 5 převádí cíle podniku na konkrétnější cíle. Za účelem realizace potřeb zainteresovaných stran jsou tyto strany transformovány do firemní strategie a jejich potřeby jsou specifikovány prostřednictvím sady obecných cílů, které jsou kaskádovány, resp. transformovány do specifických IT cílů a cílů jednotlivců, které jsou zvládnutelné.

Cíle zainteresovaných stran jsou kaskádovány do cílů společnosti. Proces kaskádování je detailně popsán v (Lainhart, 2012, příloha D) Cíle společnosti jsou dále kaskádovány do cílů souvisejících s IT (Lainhart, 2012, příloha B) a cíli jednotlivců (Lainhart, 2012, příloha C).

Pokrytí celé společnosti (byznysu, organizace) – zaměření COBIT 5 není soustředěno pouze na funkce a cíle související s IT, ale na pokrytí všech procesů a zapojení všech zaměstnanců v organizaci. V rámci pokrytí celé společnosti je třeba zajistit zdroje (enablers), definovat rozsah (scope) a určit odpovědnosti (roles, activities and relationships).

Zdroje představují prostředky, sloužící pro správu rámců, principů, struktur nebo procesů včetně IT infrastruktury, aplikací a lidských zdrojů. Stanovení rozsahu je závislé na identifikaci pohledu, který definuje oblast, na kterou budou aplikována pravidla řízení (organizace jako celek, subjekt apod.). V rámci odpovědností definuje odpovědnosti rolí a vzájemné vztahy v rámci organizace.

Použití jednotného integrovaného frameworku – v současné době existuje velké množství rámců pro návrh enterprise architektury, IT Governance a řízení služeb IT. Vhodné je využívat pouze jednoho rámce pro danou oblast za účelem zjednodušení nasazení a případné reakce na změny.

Povolení holistického přístupu – efektivní správa a řízení podnikového IT je zajištěna prostřednictvím využití holistického (jednotného) přístupu, který využívá spolupracujících komponent. Za tímto účelem definuje COBIT 5 sadu aktivátorů (enablerů), které významným způsobem napomáhají zajišťovat cíle byznysu. COBIT 5 specifikuje celkem 7 kategorií aktivátorů:

- Principy, politiky a rámce – definují pravidla a pokyny pro identifikaci, implementaci a přezkoumávání potřeb uživatelů, resp. potřeb byznysu.
- Procesy – definice procesů, které transformují potřeby uživatelů do činností a postupů, kterými jsou tyto potřeby realizovány, a tedy je dosaženo definovaných cílů.
- Organizační struktura – definuje organizační strukturu v rámci organizace.
- Kultura, etika a chování – kategorie zaměřená na identifikaci firemní kultury, která je zaměřena na identifikaci a vývoj rizik spojených se zajišťování potřeb uživatelů.

- Informace – kategorie zaměřená na životní cyklus informací. Je nutno stanovit, kde informace vznikají, kdo je jejich vlastníkem, povolené metody práce s informacemi a identifikace osob, které jsou oprávněné s informacemi pracovat. COBIT 5 doporučuje využít pro tuto oblast principy systému řízení bezpečnosti informací (ISMS)

- Služby, infrastruktura a aplikace – kategorie zaměřená na návrh a implementaci technických opatření pro zajištění přístupu k informacím.

- Lidé, znalosti a kompetence – kategorie, která definuje počet zaměstnanců organizace, jejich pracovní zařazení a potřebné kompetence a znalosti, které jsou nezbytné pro naplnění stanovených cílů.

Oddělení governance od managementu společnosti – za účelem rozdělení odpovědností a rozhodovacích mechanismů při plnění dílčích úkolů, které vedou ke stanoveným cílům, jsou odděleny zodpovědnosti governance a managementu společnosti.

Governance společnosti odpovědné za posuzování, řízení a monitorování stanovených cílů a požadavků byznysu (EDM). Požadavky na governance společnosti zahrnují nastavení a údržbu zvoleného rámce (frameworku), posouzení výhod a přidané hodnoty, které s sebou přináší realizace stanovených cílů, zajištění procesu optimalizace rizik, zajištění optimalizace zdrojů a transparentnost zúčastněných stran.

Management společnosti nese odpovědnost za plánování, implementaci, spouštění a monitorování příslušných aktivit, které vedou k dosažení stanovených cílů.

Vzhledem k rozsáhlosti problematiky nejsou dále podrobně popisovány jednotlivé procesy a matice odpovědnosti s nimi související. Detailní popis procesů popisuje Lainhart (2012, s. 25–216).

Jak již bylo uvedeno, základním stavebním kamenem COBIT 5 je zaměření na dosažení stanovených cílů s využitím procesního řízení.

COBIT 5 definuje proces jako „soubor postupů ovlivňovaných politikami a praktikami organizace, který na základě manipulací se vstupy z mnoha zdrojů (včetně jiných procesů) produkuje výstupy (např. produkty, služby atd.).“ (Lainhart, 2012, s. 19)

K vyhodnocení úrovně způsobilosti procesů využívá COBIT souhrnné pojmenování proces capability levels. Hodnocení je prováděno na základě mezinárodní normy ISO/IEC 15504.

Hodnocení je založeno na 6 stupňové škále. Některé stupně škály zároveň obsahující atributy výkonnosti (PA), které napomáhají definovat úroveň způsobilosti procesu (Putri a Surendro, 2015, s. 3; Patón-Romero et al., 2018, s. 30).

4.3 Manažerský pohled

Z hlediska manažerského pohledu, který je určující pro vrcholové vedení organizace jako celku, by přístupy k efektivnímu návrhu implementace systémů, které zajišťují zaznamenávání činností a událostí v energetických systémech, měly vycházet z obecně platných standardů které se zabývají efektivním procesem návrhu a implementace těchto systémů, resp. architektonických řešení jako celku v kontextu s potřebami konkrétní organizace. Touto oblastí a problematikou se v současné době zabývá enterprise (podniková) architektura. Mezi základní rámce (frameworky), resp. standardy, metodiky a normy, které se zabývají architektonickými návrhy a efektivním provozem technologií a IT služeb a patří v dnešní době k nejrozšířenějším se řadí TOGAF, DODAF, TODAF, TEAF, FEAF, IAF, E2AF apod. Společným jmenovatelem rámců je zaměření na komplexní problematiku architektury systémů s vazbou na potřeby a obchodní cíle organizace, které tvoří základní pilíře v oblasti enterprise architektury.

4.3.1 Enterprise architektura

Pojem Enterprise architektura (Enterprise Architecture) je v současné době v České republice často chybně pochopen z důvodu nepřesného překladu tohoto pojmu. Překlady definují tento pojem jako podniková architektura nebo byznys architektura (Bejšovec, 2010, s. 9). Vlivem uvedeného překladu je často pojem Enterprise architektura mylně chápán jako architektura organizace jako celku. Za účelem nalezení standardizované definice je možné využít definici uvedenou v rámci mezinárodních norem a případně standardů. Pojem Enterprise architektura je definován v mezinárodní normě ISO/IEC/IEEE 42010:2011(Systems and software engineering – Architecture description) následovně: „*přístup, koncept, prostředek a nástroj, kterým vyjadřujeme fundamentální uspořádání vztahu mezi byznysem a jeho informačním systémem, které vede k naplnění mise organizace, přičemž respektuje okolní prostředí a konzistentně dodržuje formulované principy návrhu a rozvoje systému.*“

Z výše uvedené definice vyplývá, že hlavním cílem Enterprise architektury je vytvoření vztahů mezi architekturou informačního systému, která přímo podporuje obchodní cíle organizace, reprezentované ve formě obchodní strategie, (Van Den Berg et al., 2019, s. 134) prostřednictvím zavádění standardizace procesního řízení a využití stávajících prostředků

informačních technologií (aplikací, databází apod.) za účelem podpory hlavních procesů organizace.

Pojem architektura informačního systému je rovněž definován v mezinárodní normě ISO/IEC 42010/2011 jako „*Architektura je fundamentálnĺ uspořádání systému, které tvoří komponenty a vztahy mezi nimi, včetně vztahu k prostředĺ, a principy, které řídí jeho návrh a rozvoj.*“

Mírně odlišný pohled na problematiku Enterprise Architektury má společnost Gartner. Dle společnosti Gartner je Enterprise architektura založena na identifikaci a analýze úprav v projektech a politikách organizace, za účelem dosažení obchodních výsledků.

Z výše uvedeného je patrné, že i přes existenci různých pohledů na definici Enterprise architektury je základ těchto pohledů vždy soustředěn na problematiku informačních technologií a systémů a jejich využití za účelem podpory obchodních cílů organizace (Ferrugento a Rocha, 2015, s. 351).

Výsledkem chybně navržené Enterprise architektury jsou nestabilní a padající aplikace, problémy s upgradováním systémů, chybějící dokumentace rozhraní mezi jednotlivými systémy a zejména různorodost využívaných platforem, která přináší zvyšování finančních nákladů na jejich provoz, rozvoj a údržbu apod. V současné době existuje velká množina architektonických rámců, která se soustředí na problematiku efektivního návrhu Enterprise architektury za účelem eliminace výše uvedených problémů.

Architektonický rámec je tvořen „*základní strukturou nebo sadou struktur, které mohou být použity pro vývoj široké škály různých architektur. Měl by popsat metodu navrhování cílového stavu organizace z hlediska sady stavebních bloků a pro zobrazení toho, jak stavební bloky zapadají do sebe. Měl by obsahovat sadu nástrojů a poskytovat společný slovník. Měl by také obsahovat seznam doporučených norem a vyhovujících produktů, které lze použít k realizaci stavebních bloků.“ (*Welcome to the TOGAF® Standard, Version 9.2, a standard of The Open Group, 2018)

Tabulka 7 reprezentuje příklady architektonických rámců pro enterprise architekturu.

Tabulka 7 - Rámce pro Enterprise architekturu. Zdroj: upraveno dle Bejšovce (2010, s. 21) a Lapalme (2016, s. 104)

Název architektonického rámce	Zkratka
The Open Group Architecture Framework	TOGAF
Federal Enterprise Architecture Framework	FEAF
Treasury Enterprise Architecture Framework	TEAF
DoD Architecture Framework	DoDAF
Zachman Enterprise Architecture Framework	ZEAF
Extended Enterprise Architecture Framework	E2AF
Enterprise Architecture Planning	EAP
Integrated Architecture Framework	IAF
Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance	C4ISR
Technical Architecture Framework for Information Management	TAFIM
Purdue Enterprise Reference Architecture	PERA
European Union—IDABC & European Interoperability Framework	
IEEE Std 1471-2000 IEEE Recommended Practice for Architectural Description	
ISO/IEC 14252 (IEEE Std 1003.0)	

Architektonické rámce lze členit do 3 základních druhů.

- Klasifikační rámce – jsou založeny na rozpadu složitého systému (organizace, podniku) na dílčí pohledy a hlediska, která jsou vázána na pohledy. Klasifikační rámce jsou typicky reprezentovány tabulkovou formou, kde sloupce tabulky reprezentují pohledy a řádky hlediska. Prvky matice jsou reprezentovány prostřednictvím modelu. Mezi typické představitele klasifikačních rámců řadíme Zachmanův rámec.

- Procesní rámce – jejich zaměření je soustředěno na oblast procesů, resp. postupů využívaných při řízení životního cyklu podnikové architektury. Typickými představiteli procesních rámců jsou například TOGAF a FEAF.

- Obsahové rámce – zaměřují se pouze na určité odvětví podnikání, resp. lidské činnosti. Příkladem může být rámec IAA využívaný v oblasti pojišťovnictví.

Z výše uvedených rámců jsou dle Bejšovce (2010, s. 21) a Lapalme (2016, s. 104) v současné době nejvíce využívány rámce TOGAF, FEAF, MODAF, DoDAF a Zachman.

S Bejšovcem a Lapalmem se v uvedené problematice shodují také Hinkelmann (2016, s. 79), Dang a Pekkola (2015, s. 141) a (Ferrugento a Rocha, 2015, s. 351).

U všech výše uvedených rámců lze nalézt společný jmenovatel ve formě dělení Enterprise architektury na čtyři funkční celky (Welcome to the TOGAF® Standard, Version 9.2, a standard of The Open Group, 2018; Dey, 2017):

- Byznys architektura – definuje klíčové procesy organizace, strategii řízení organizace a obchodní strategii organizace.
- Datová/informační architektura – obsahuje popis prostředků, které jsou využívány pro ukládání dat, jejich formát, možnosti jejich zpracování, způsoby přístupu a zabezpečení.
- Aplikační architektura – definuje a popisuje plán nasazení jednotlivých aplikací. Součástí popisu je popis vzájemných vazeb aplikací a jejich vztah ke klíčovým procesům organizace.
- Technologická architektura – zahrnuje popis HW a SW infrastruktury, která je využívána pro běh aplikací a služeb. Součástí popisu jsou komponenty IT infrastruktury, komunikační prvky apod.

Výše uvedené 4 celky jsou klíčové pro efektivní fungování informačních technologií a systémů ve vazbě na obchodní strategii organizace (byznysu). V případě, že se zainteresované osoby soustředí pouze na jeden funkční celek, typicky pouze na IT infrastrukturu, bez vazby na podnikovou strategii, není možné efektivním způsobem budovat Enterprise architekturu (Bejšovec, 2010, s. 11). Důsledkem je zejména ztráta velkého množství finančních prostředků vynaložených na vyvolané potřeby změn služeb a aplikací, které jsou vyvolány podnikovou strategií, protože není efektivně udržováno prostředí pro chod služeb a aplikací ve vazbě na podnikovou strategii.

4.3.2 Modelování enterprise architektury

Pro účely efektivního návrhu a rozvoje enterprise architektury je nezbytné zajistit vizualizaci jednotlivých elementů architektury včetně jejich vzájemných vazeb. V současné době existuje mnoho modelovacích jazyků a současně nástrojů pro modelování, resp. vizualizaci enterprise architektury. Modelovací jazyk poskytuje jednotný nástroj pro syntaktické a zároveň sémantické vyjádření modelu.

V současné době lze využít např. následující modelovací jazyky:

- Design & Engineering Methodology for Organizations (DEMO),
- Baan Dynamic enterprise modeling (DEM),
- Business Process Modelling Language (BMPL),
- Archimate,
- Architecture of Integrated Information Systems,
- Reference Model of Open Distributed Processing (RM-ODP),
- Multi-Perspective Enterprise Modelling (MEMO),
- Extended Enterprise Modeling Language (EEML) apod.

Pro účely vizualizace enterprise architektury slouží modelovací nástroje. Těchto nástrojů existuje velké množství, stejně jako modelovacích jazyků. Modelovací nástroje typicky podporují pouze jeden, případně úzkou množinu rámců enterprise architektury. Výběr modelovacího jazyka a nástroje musí reflektovat zvolený rámec enterprise architektury a tvoří klíčovou prerekvizitu před samotným začátkem procesu návrhu enterprise architektury jako celku.

Problematikou porovnání dostupných nástrojů pro enterprise architekturu, resp. jejich výrobců, se dlouhodobě věnuje společnost Gartner Inc. Společnost Gartner každoročně vydává Gartner Magic Qadrant. Obrázek 19 reprezentuje Gartner Magic Quadrant výrobců nástrojů pro enterprise architekturu za rok 2019.

Příklady uvedených výrobců a jejich produktů:

- Abacus – Avolution,
- Alfabet – Strategic IT Manager Solution Network,
- Orbus Software's – iServer Suite,
- Sparx System – Enterprise Architect.

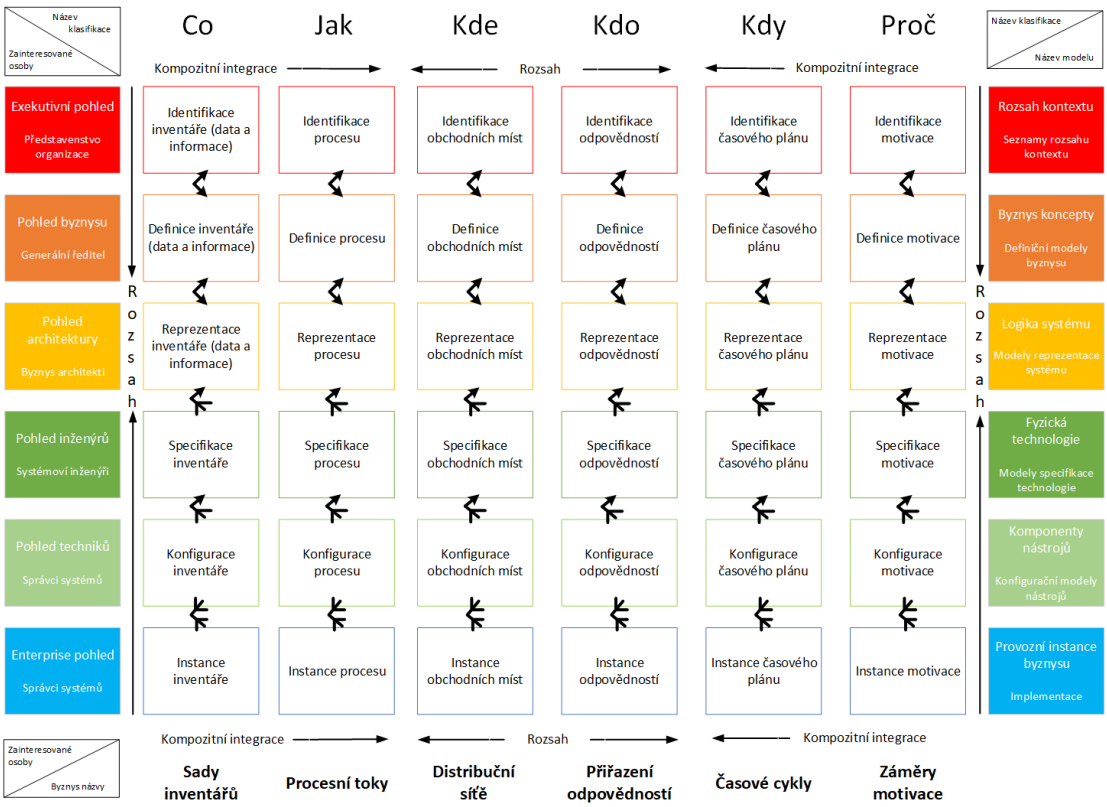
Obrázek 19 - Gartner Magic Quadrant for Enterprise Architecture Tools 2019. Zdroj: Magic Quadrant for Enterprise Architecture Tools (2019)

5 RÁMCE ENTERPRISE ARCHITEKTURY

5.1 Zachman

Rámec pro enterprise architekturu Zachman (Zachman Enterprise Architecture Framework, ZEAF) je odbornou veřejností chápán jako první rámec pro enterprise architekturu (Okhrimenko, 2017, s. 18). První návrh byl vytvořen Johnem Zachmanem v roce 1984. Pokud není uvedeno jinak, vychází tato kapitola primárně z oficiální dokumentace rámce Zachman (Zachman, 2008). První verze s názvem Framework for Information Systems Architecture byla publikována o 3 roky později v časopise IBM Systems Journal. Rámec se v průběhu času vyvíjel a byl několikrát aktualizován. V současné době je poslední verze datována do roku 2011. Rámec Zachman napomáhá vedení organizace zobrazovat v grafické formě současný stav organizace prostřednictvím rolí v klíčových procesech organizace a jejich vzájemné interakce. Rámec definuje vlastníka procesu, analytika procesu, tvůrce procesu a současně komponent procesu, osoby zodpovědné za komponenty, způsob práce s komponentami a tým, který je oprávněn s komponentou pracovat. Orientace rámce Zachman je především na oblast operativního plánování a lepšího rozhodování a nikoli na oblast strategie a Governance v rámci organizace.

Rámec Zachman je reprezentován graficky ve formě matice o rozměrech 6×6. Obrázek 20 reprezentuje grafickou podobu Zachman rámce.



Obrázek 20 - Zachman rámec. Zdroj: upraveno dle Zachmana (2008) a Okhrimenko 2017, s. 18–19)

V rámci horizontální osy je definováno 6 hledisek zúčastněných stran (Okhrimenko, 2017, s. 18–19; What is Zachman Framework, 2019):

- Co (data) – jaká data a informace jsou pro byznys klíčová.
- Jak (funkce) – jaké jsou podnikové procesy.
- Kde (síť) – kde jsou aktuální a potencionální místa byznysu a obchodních aktivit organizace.
- Kdo (lidé) – kdo jsou lidé, kteří jsou zainteresováni v byznysu organizace a odpovědní za implementaci nové architektury.
- Kdy (čas) – kdy jsou prováděny plány byznysu organizace.
- Proč (motivace) – motivace byznys cílů a strategie organizace.

Vertikální osa Zachman rámce reprezentuje pohledy (perspektivy) na byznys organizace z pohledu zúčastněných stran.

- Exekutivní pohled (executive perspective) – jedná se o pohled na úrovni výkonného managementu organizace, případně představenstva společnosti. Pohled se zaměřuje na identifikování pozice organizace v rámci trhu a získávání konkurenčních výhod. Pohled se nezaměřuje na technické detaily a provozu technologií v organizaci.

- Pohled byznysu (business management perspective) – představuje pohled managementu organizace – typicky generálního ředitele. Pohled je zaměřen na byznys organizace ve vazbě na transformaci exekutivního pohledu do byznys modelu.

- Pohled architektury (architecture perspective) – pohled určený pro byznys architekty. Pohled se zaměřuje na transformaci byznys modelu do funkčních bloků (zákazníci, IT technologie apod.), které jsou klíčové pro provoz podniku a dosažení cílů byznysu.

- Pohled inženýrů (engineer perspective) – pohled zaměřený na identifikaci inženýrů, kteří budou navrhovat realizaci stavebních bloků identifikovaných pohledem architektury. Cílem pohledu je transformace identifikovaných stavebních bloků do specifikací a požadavků pro budování systémů.

- Pohled techniků (technician perspective) – pohled techniků, kteří provádí implementaci, provoz a údržbu daných systémů. Cílem pohledu je implementace specifikací a požadavků z předchozího pohledu.

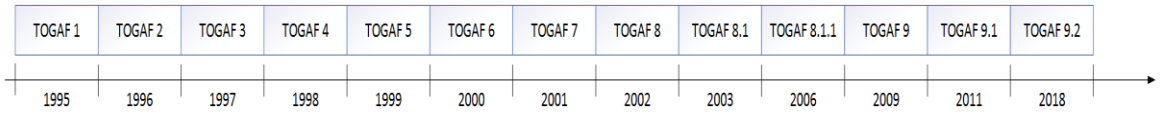
- Enterprise pohled (enterprise perspective) – pohled na organizaci z hlediska fyzického uspořádání, např. adresa budovy, identifikace počítačového sálu, identifikace HW a identifikace záloh.

5.2 TOGAF®[12]

TOGAF® (The Open Group Architecture Framework, dále TOGAF) představuje rámec pro Enterprise architekturu v oblastech jejího plánování, designu, implementace a governance. Historie TOGAF se začala psát již v roce 1995 kdy byla vydána první verze TOGAF 1.0. První verze byla založena na standardu TAFIM (Technical Architecture Framework

[12] TOGAF® je registrovaná ochranná známka konsorcia The Open Group

for Information Management), který byl vydán prostřednictvím Ministerstva obrany Spojených států amerických. V současné době jsou nové verze TOGAF vydávány prostřednictvím konsorcia The Open Group (Welcome to the TOGAF® Standard, Version 9.2, a standard of The Open Group, 2018). Jedná se o konsorcium s globálním působením, která se soustředí na dosahování obchodních cílů prostřednictvím využívání standardů a norem (About Us – What We Do, 2019). Členy konsorcia je více než 700 organizací zabývajících se výrobou, vývojem a konzultačními službami v oblasti informačních technologií. Mezi členy jsou dále zastoupeny univerzity a odborníci z různých odvětví průmyslu.



Obrázek 21 - Vývoj TOGAF. Zdroj: upraveno dle The Open Group

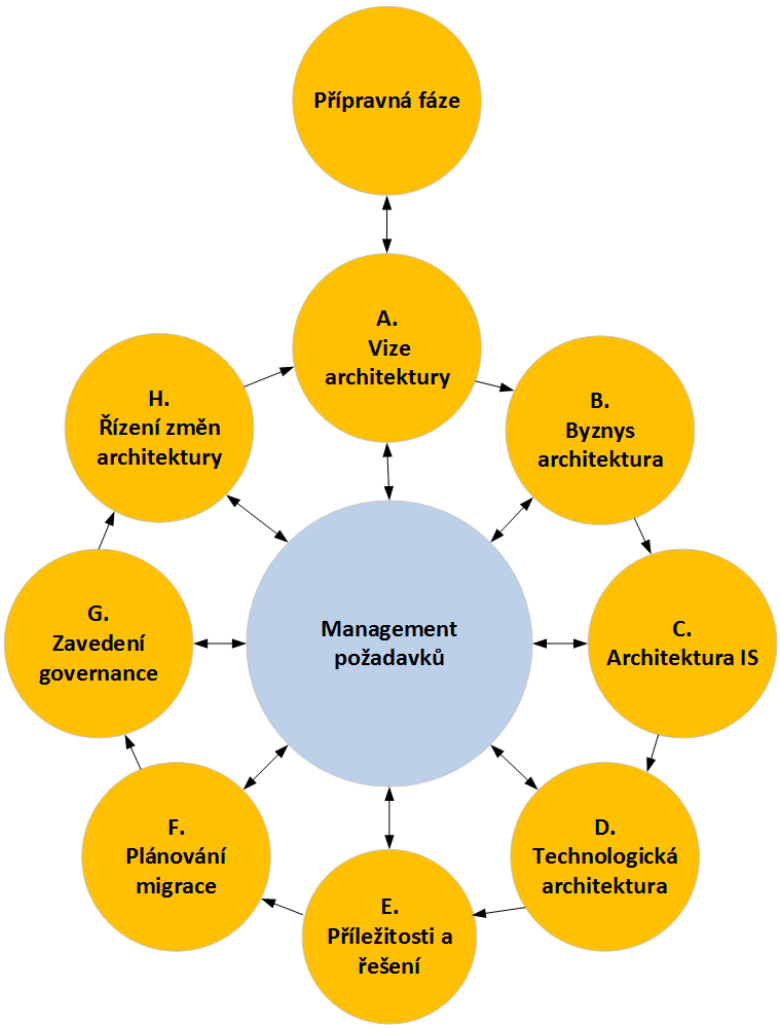
V současné době je aktuální verze TOGAF 9.2, která byla publikována konsorciem The Open Group v dubnu 2018.

Struktura dokumentace TOGAF 9.2 je rozdělena do 6-ti částí (Welcome to the TOGAF® Standard, Version 9.2, a standard of The Open Group, 2018):

- Část I (Introduction) – poskytuje úvodní informace o klíčových pohledech a přístupech pro řešení enterprise architektury v rámci TOGAFu. Součástí je i definice používaných termínů a struktura dokumentace TOGAF, která je uvedena zde.
- Část II (Architecture Development Method) – klíčová část rámce TOGAF označovaní jako ADM. Obsahem je detailní popis jednotlivých kroků pro vývoj enterprise architektury.
- Část III (ADM Guidelines & Techniques) – část obsahující soubor postupů a technik pro využití TOGAF a ADM.
- Část IV (Architecture Content Framework) – část popisující obsah TOGAF rámce, popis metamodelu pro architektonické artefakty, opětovné využití základních architektonických stavebních bloků a přehled výstupů enterprise architektury.
- Část V (Enterprise Continuum & Tools) – část obsahující klasifikaci a seznam vhodných nástrojů vhodných pro uložení výstupů enterprise architektury.

- Část VI (Architecture Capability Framework) – obsahem této části jsou informace o organizaci, zavedených procesech, dovednostech, povinnostech a rolích, které jsou zapotřebí pro implementaci, nastavení a fungování enterprise architektury v rámci podniku.

Klíčovou částí TOGAF je Architecture Development Method (ADM). Jedná se o vícefázový a iterativní přístup využití enterprise architektury pro řízení projektů v organizaci. Výsledkem je metoda, která popisuje vývoj enterprise architektury. Metoda je tvořena z celkem 10 fází, které na sebe navzájem navazují a tvoří základ pro tvorbu enterprise architektury (Čapek, 2016, s. 29–36). Obrázek 22 reprezentuje jednotlivé fáze ADM a jejich vzájemné vazby.



Obrázek 22 - TOGAF ADM. Zdroj: upraveno dle Welcome to the TOGAF® Standard, Version 9.2, a standard of The Open Group (2018)

- Přípravná fáze – fáze zahrnující a přípravné činnosti potřebné pro zajištění souladu byznys požadavků organizace a enterprise architektury (Bejšovec, 2010, s. 26). Součástí fáze je posouzení současného stavu využívání architektonických řešení v rámci organizace, definice požadavků na změnu stávajících projektů pro zajištění souladu s enterprise architekturou. V rámci přípravné fáze by mělo dojít k informování všech zúčastněných stran, které se budou podílet na enterprise architektuře, o požadavcích, které jsou na enterprise architekturu kladeny a současně vytvoření odpovídajících podmínek pro všechny zúčastněné strany (Welcome to the TOGAF® Standard, Version 9.2, a standard of The Open Group, 2018). Součástí přípravné fáze je dále vyhodnocení požadavků na finance, které jsou třeba pro zavedení enterprise architektury. Obecně lze konstatovat, že výstupem přípravné fáze je určení Kde, Co, Proč, Kdo a Jak bude vytvářet enterprise architekturu (Kearny, Gerber a Van Der Merwe, 2016, s. 004604).

- Fáze A – vize architektury – v rámci této fáze jsou identifikovány zainteresované strany a jejich zájmy, identifikace omezení požadavků na řešení a identifikace komponent a požadavků na testování architektury (Kearny, Gerber a Van Der Merwe, 2016, s. 004605). Je vypracována vize, která popisuje přidanou hodnotu pro byznys organizace při zavedení enterprise architektury. Součástí vize je deklarace priorit a dílčích úkolů a dopadů změn enterprise architektury. Je vytvořen projektový plán obsahující stanovené cíle, požadavky na lidské, finanční a technologických zdrojů, identifikaci přínosů, limitujících faktorů a rizik. Plán musí projít formálním procesem schválení, aby mohla být naplněna vize enterprise architektury (Welcome to the TOGAF® Standard, Version 9.2, a standard of The Open Group, 2018). Výstupy fáze vize architektury jsou dále postoupeny jako vstupy do fáze byznys architektury.

- Fáze B – byznys architektura – cílem fáze je rozvoj byznys architektury, která popisuje způsob práce v organizaci na operativní úrovni, který je nutný pro dosažení obchodních cílů. Současně popisuje, jakým způsobem reagovat na vize enterprise architektury definované na strategické a taktické úrovni, které jsou součástí projektového plánu (Welcome to the TOGAF® Standard, Version 9.2, a standard of The Open Group, 2018). Současně jsou modelovány byznys procesy a jejich vzájemné vazby. Za účelem rozvoje byznys architektury je třeba znát současný a cílový stav enterprise

architektury. Na základě identifikovaných rozdílů je stanoven plán pro dosažení cílového stavu (Bejšovec, 2010, s. 26).

- Fáze C – architektura IS – fáze popisující vývoj architektury informačních systémů organizace, která bude zohledňovat vstupy z byznys architektury a vize architektury prostřednictvím zainteresovaných stran. Fáze je rozdělena na dvě na sebe navazující části. První část tvoří popis datové architektury. Součástí popisu je definice datových entit a jejich vzájemných vazeb včetně popisu vytváření, distribuce, migrace, zabezpečení a archivace dat. Druhá část je tvořena aplikační architekturou, která definuje aplikace, které slouží pro správu dat. Nejedná se o stanovení konkrétních aplikačních řešení, ale o stanovení logiky nezávislé na platformě. (Welcome to the TOGAF® Standard, Version 9.2, a standard of The Open Group, 2018)

- Fáze D – technologická architektura – výstupem této fáze je zmapování aplikační architektury na HW a SW prostředky, které má organizace k dispozici nebo které je schopna zakoupit. Dochází ke stanovení požadavků na změny v oblasti informačních technologií. Výstup je tvořen zejména dokumentem obsahující seznam technologického HW a SW portfolia včetně modelů topologie počítačové sítě, definici datových uložišť, připojení serverů apod.

- Fáze E – příležitosti a řešení – na základě výstupů z fází B, C a D je sestavena architektonická roadmapa, která definuje jednotlivé změnové přírůstky v rámci časové osy, za účelem zobrazení přechodu od základní architektury k cílové architektuře (Welcome to the TOGAF® Standard, Version 9.2, a standard of The Open Group, 2018). Plán současně obsahuje přehled konkrétních řešení a nástrojů potřebných pro realizaci enterprise architektury (Štěpán, 2016, s. 28).

- Fáze F – plánování migrace – účelem této fáze je příprava implementačního a migračního plánu na základě výstupů z předchozí fáze, tedy architektonické roadmapy. V této fázi je provedena analýza nákladů a jejich porovnání s plánovaným finančním zajištěním. V případě zjištění rozdílů jsou provedeny úpravy v projektu.

- Fáze G – zavedení governance – fáze zabývající se zajištěním dohledu nad implementací. Bejšovec (2010, s. 27) uvádí, že v rámci fáze zavedení governance jsou formulována doporučení pro jednotlivé fáze projektu a současně je zajištěn

architektonický dohled projektu, jehož cílem je zajištění souladu projektu se všemi dalšími projekty v rámci organizace. (Čapek, 2016, s. 35–36)

- Fáze H – řízení změn architektury – cílem fáze řízení změn architektury je zajištění souladu architektury s požadavky byznysu organizace. Jsou stanoveny postupy pro řízení změn architektury, které mohou nastat v budoucnu (Štěpán, 2016, s. 28). Součástí fáze je proces monitorování požadavků zajištění governance, vývoj nových technologií a změn v prostředí podnikání organizace. (Welcome to the TOGAF® Standard, Version 9.2, a standard of The Open Group, 2018). V této fázi se TOGAF prolíná s oblastí IT governance, resp. dochází k mapování TOGAF na rámce, které se touto oblastí zabývají, např. ITIL, COBIT apod. Oblast enterprise architektury je tak propojena s řízením na operativní úrovni. Nezbytnou součástí této fáze je stanovení konkrétních odpovědných pracovníků, jejich zodpovědností a způsobu komunikace na operativní úrovni.

- Fáze managementu požadavků – fáze zajišťující proces a správu řízení funkčních a nefunkčních požadavků na architekturu pro všechny fáze ADM za účelem efektivního řízení enterprise architektury jako jednoho funkčního celku. Zavedení tohoto přístupu odráží reálné problémy při implementaci rozsáhlých projektů a architektonických řešení. (Welcome to the TOGAF® Standard, Version 9.2, a standard of The Open Group, 2018).

5.3 FEA

FEA (Federal Enterprise Architecture) popisuje enterprise architekturu federální vlády Spojených států amerických. První verze FEA byla publikována v únoru 2001. Cílem FEA je zavedení procesů efektivního využívání a správy informačních technologií a architektury informačních systémů využívaných v rámci federální vlády. Jak uvádí Welcome to the TOGAF® Standard, Version 9.2, a standard of The Open Group (2018), FEA popisuje komplexní proces zahrnující zahájení, implementaci a udržitelnost enterprise architektury včetně popisu rolí, které jsou v rámci procesu nezbytné a jejich zodpovědností.

Povinnost zavedení a využívání FEA v rámci federálních úřadů Spojených států amerických je dána zákonem Clinger-Cohen Act z roku 1996 (Halawi, McCarthy a Farah, 2019, s. 6). Zákon rovněž předepisuje, že instituce, které nesplní nastavené parametry výkonnosti, resp. efektivního využívání informačních technologií, nemohou investovat finanční prostředky do rozvoje informačních technologií.

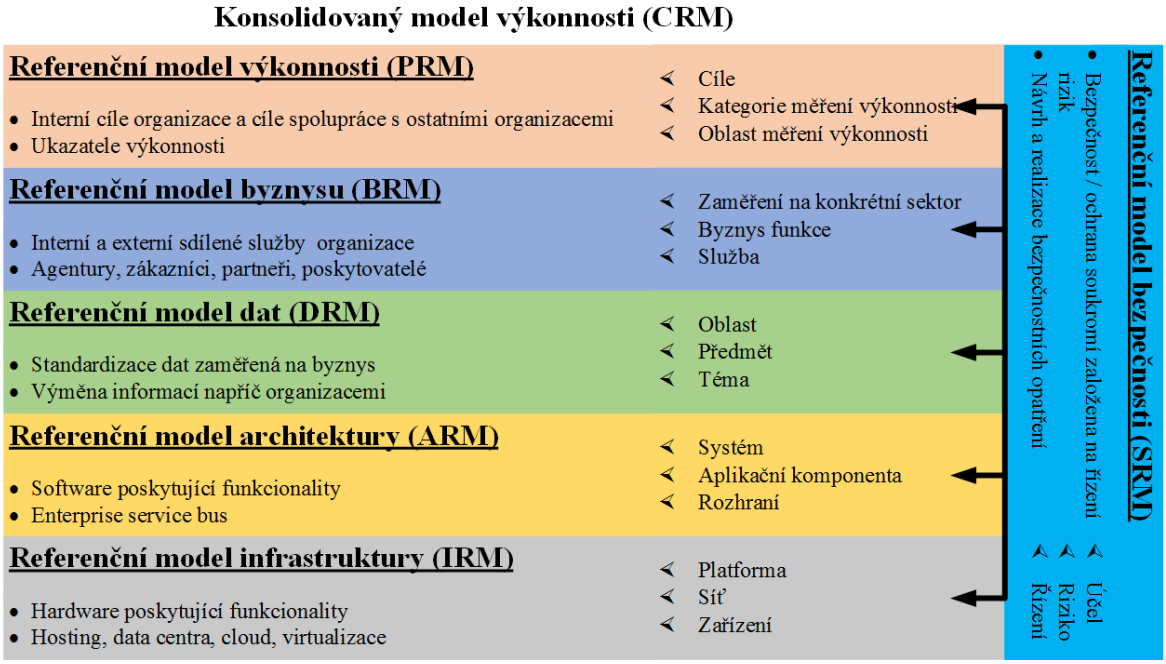
Předpokladem pro efektivní zavedení FEA je zapojení managementu organizace a vytvoření architektonického týmu (Nikpay et al, 2017, s. 934). Architektonický tým realizuje proces vytváření dílčích a cílových architektur. Zodpovědností architektonického týmu je dále příprava plánů pro přechod systémů a aplikací, aby byly v souladu s cílovou architekturou. Projekty jsou řízeny prostřednictvím procesního řízení, které reflektuje požadavky na cílovou architekturu, tj. požadavky na byznys cíle organizace, vize a využívané HW a SW vybavení. Procesy jsou úzce propojeny s jednotlivými fázemi rámce TOGAF ADM. (Welcome to the TOGAF® Standard, Version 9.2, a standard of The Open Group, 2018)

5.4 FEAF

FEAF (Federal Enterprise Architecture Framework) je rámcem pro enterprise architekturu využívanou v rámci federální vlády Spojených států amerických. První verze FEAF byla publikována v roce 1999 radou Federal CIO Council. Hlavním účelem publikace FEAF bylo sjednocení enterprise architektury v rámci jednotlivých federálních úřadů Spojených států amerických a současně sdílení informací mezi federální vládou a dalšími vládními subjekty a agenturami (Masuda, Shirasaka a Yamamoto, 2016, s. 9). Pokud není uvedeno jinak, vychází následující kapitola z oficiální dokumentace FEAF – Schiller (2013).

Součástí FEAF jsou referenční modely, které slouží k identifikaci duplicitních investic v rámci federálních úřadů a zlepšení spolupráce napříč federálními úřady formou identifikací příležitostí ke zlepšení využívání informačních technologií a přístupů ke tvorbě architektonických řešení (Bondar et al., 2017, s. 34)

Dne 22. ledna 2013 vydal Bílý dům pro federální úřady FEAF verze 2, která byla široké veřejnosti publikována o rok později. V oblasti referenčních modelů došlo v rámci FEAF k jejich přeskupení a rozšíření na celkový počet 6 modelů (Okhrimenko, 2017, s. 21).



Obrázek 23 - FEAF referenční modely verze 2. Zdroj: upraveno dle Schiller (2013, s. 20).

Referenční model výkonnosti se využívá k měření výkonnosti mezi investicemi a činnostmi, které federální agentury realizují v oblasti IT a strategickými vizemi definovanými federálními agenturami a federální vládou Spojených států. Povinnost zveřejňovat ukazatele výkonnosti jednotlivých federálních agentur přinesl v roce 2010 zákon GPRA Modernization Act. Struktura modelu je složena ze tří částí:

- Cíle – umožňují seskupovat investice a aktivity prostřednictvím rámce vytvořeného federálními agenturami, jehož výstupy poskytují detailní informace o výkonnosti federálních agentur jako celku.
- Oblast měření výkonnosti – popisuje vztah mezi investicemi a činnostmi federálních agentur ve vztahu k jejich stanoveným výkonnostním cílům.
- Kategorie měření výkonnosti upřesňuje oblast měření výkonnosti formou rozdělení oblastí měření výkonnosti do více a detailněji specifikovaných kategorií. Existuje vzájemný vztah mezi cíli a kategoriemi měření, kdy na jakýkoli cíl lze aplikovat libovolnou kategorii měření výkonnosti.

Referenční model byznysu popisuje každodenní obchodní operace realizované v rámci federálních agentur se zaměřením na využívání interních a externích služeb pro dosažení strategických cílů byznysu federálních agentur s vazbami na strategické cíle federální vlády. Struktura modelu je složena, stejně jako v případě referenčního modelu výkonnosti, ze 3 částí.

- Zaměření na konkrétní sektor – federální vláda identifikuje deset standardních oblastí týkající se společného přístupu k enterprise architektuře.

- Byznys funkce – popisuje roli federální vlády ve vztahu ke klasifikačním kódům rozpočtu, které jsou definovány v OMB Circular A-11. Účelem klasifikačních kódů v byznys modelu je jejich využití v rámci provádění analýz investic do IT.

- Služba – účelem identifikace služeb je možnost sdílení a opětovného použití aplikací a jejich komponent za účelem snižování finančních nákladů souvisejících s provozem a údržbou velkého množství aplikací, které disponují stejnými funkcionalitami.

Využívání referenčního modelu byznysu přináší federálním agenturám výhody napříč jednotlivými organizačními jednotkami.

- Management agentury – využívání referenčního modelu byznysu přináší vrcholovému managementu informace o slabých místech a duplicitně využívaných aplikací a komponent agentury. Identifikace slabých míst a duplicit vytváří příležitosti pro úsporu finančních nákladů a novým obchodním příležitostem, které napomáhají dosažení strategických cílů agentury.

- Portfolio manažeři – využití referenčního modelu byznysu jako rámce pro správu portfolia IT vytváří propojení mezi IT projekty a investicemi s obchodními potřebami agentury. Výsledkem tohoto propojení je efektivnější plánování financování vývoje aplikací a IT systémů.

- Projektoví manažeři – referenční model byznysu přináší projektovým manažerům schopnost identifikace obchodních příležitostí, vazeb konkrétního projektu na stávající architekturu, zefektivnění obchodních procesů a snižování nákladů v rámci projektů.

- Vývojáři – využití referenčního modelu byznysu zvyšuje schopnost vývojářských týmů, kteří pracují na jednotném řešení, které splňuje potřeby byznysu. Jednotné řešení přináší úsporu finančních nákladů. Nejsou vyvíjeny duplicitní aplikace a služby. Vývoj je zaměřen na vytváření sdílených služeb, které jsou využívány více aplikacemi.

Referenční model dat se zaměřuje na oblast identifikace, využití a sdílení dat a informací napříč federálními agenturami. Součástí modelu jsou standardní prostředky, pomocí kterých lze data popisovat, kategorizovat, sdílet a vyhledávat. Struktura modelu je složena ze 3 částí:

- Oblast – seskupování dat dle obecných charakteristik.
- Předmět – detailnější kategorizace dat než v případě oblastí. Specifičtější charakteristiky dat, které mohou být stále dostatečně obecné.
- Téma – detailnější kategorizace dat než v případě předmětů. Jedná se o data, která podporují obchodní procesy a byznys cíle.

Za účelem kategorizace, popisu a sdílení dat mezi federálními agenturami definuje referenční model dat tři základní metody:

- Popis dat – poskytuje jednotný prostředek pro popis dat. Popisem dat jsou podporovány procesy identifikace a sdílení dat. Jako osvědčené postupy pro procesy popisu dat v rámci využití referenčního modelu dat jsou doporučeny:
    - Integration Definition for Function Modeling (IDEF) – definice logických datových modelů v případě využití relačních databází
    - The Open Group Architecture Framework (TOGAF) – TOGAF definuje v rámci ADM čtyři domény – byznysová, aplikační, datová a technická architektura.
    - Unified Modeling Language (UML) – technologicky nezávislý modelovací jazyk pro návrh aplikací a podpory životního cyklu dat.
    - Department of Defence Architecture Framework v2.02 (DoDAF v2.02) – poskytuje rámec pro vývoj architektury.
    - ISO/IEC 11179 – standard specifikuje druhy a kvalitu metadat. Součástí standardu je definice způsobu správy metadat v registru metadat.
    - Dublin Core – standardy týkající se designu, popisu a osvědčených postupů při práci s metadaty.
- Kontext dat – kontext je tvořen informacemi, které poskytují datům další význam. Jedná se o proces také označovaný jako kategorizace či klasifikace dat. V rámci referenčního modelu dat je vládním agenturám doporučeno provést kategorizaci/klasifikaci dat. Hlavní kategorizace je založena nejen na využití oblastí, předmětů a témat, ale také na dělení témat dále na entity (přesně definované množiny dat), které jsou specifické pro vládní agenturu a podporují její byznys procesy.

Jako osvědčené postupy pro procesy kategorizace/klasifikace dat v rámci využití referenčního modelu dat jsou doporučeny:

  - Katalog datových aktiv – vytvoření datového katalogu obsahující datová aktiva a tvořící datový model přináší zejména snížení finančních nákladů potřebných pro implementaci změn v aplikacích a systémech. Využití datového katalogu zkracuje čas potřebný pro identifikaci potřebných dat, identifikaci redundantních datových aktiv a identifikaci znovupoužití datových aktiv.

  - Vyhledávání informací – mapování datových aktiv a kategorizace dat přináší zejména rychlé a snadné vyhledávání informací koncovým uživatelům na základě vyhledávacích kritérií.

- Sdílení dat – podporuje sdílení dat mezi jednotlivými vládními agenturami. V rámci referenčního modelu dat jsou doporučeny následující metody sdílení dat:

  - National Information Exchange Model (NIEM) – rámec, který umožňuje výměnu informací prostřednictvím výměny datových modelů.

  - Data.gov – účelem data.gov je zajistit přístup veřejnosti k datovým souborům federálních agentur. Součástí data.gov je popis metadat datových souborů a sada nástrojů, které pracují s datovými soubory.

Referenční model architektury podporuje kategorizaci jednotlivých aplikací a jejich součástí. Účelem kategorizace je identifikování aplikací poskytující stejné funkcionality. Výstupem kategorizace aplikací je sada doporučení pro opětovné použití již využívaných aplikací, jehož výsledkem je úspora finančních prostředků potřebných pro vývoj, instalaci, správu a udržování licenční politiky aplikací poskytujících stejné funkcionality. Struktura modelu je složena ze 3 částí:

- Systém – je tvořen IT infrastrukturou, daty a souvisejícími zdroji. Účelem systému je zejména sběr, zpracování, využívání, sdílení, údržby a nakládání s informacemi, které podporují byznys procesy.

- Aplikační komponenta – jsou tvořeny samostatným softwarovým řešením, které podporuje plnění byznys cílů. Mezi aplikační komponenty lze zařadit správu dokumentů, správu docházky apod.

- Rozhraní – jsou reprezentovány komunikačními protokoly, které zajišťují přenos informací mezi systémy.

Referenční model infrastruktury je založený na kategorizaci IT infrastruktury zahrnující zařízení a počítačové sítě potřební pro provoz aplikací. Model podporuje definici položek infrastruktury. Stejně jako v případě referenčního modelu aplikací je výsledkem referenčního modelu infrastruktury možnost sdílení a opětovného použití IT infrastruktury za účelem snižování finančních nákladů souvisejících s nákupem IT infrastruktury.

Pro využití referenčního modelu infrastruktury je zásadní, aby federální agentura disponovala registrem aktiv IT infrastruktury. Součástí registru by měly být informace o aktivech – výrobci, datum konce životnosti, datum konce podpory, mapování na referenční model zabezpečení apod. Jako osvědčené mezinárodní standardy, které využívají registry aktiv a jsou kompatibilní s referenčním modelem infrastruktury FEAF jsou:

- Control Objectives for Information and related Technology (COBIT) – je mezinárodně uznávaný rámec. Součástí rámce je komplexní pohled na správu podnikových IT. Důraz je kladen na informace a technologie, které vytváří přidanou hodnotu pro organizace. Rámec COBIT je detailněji představen v rámci kapitoly 4.2.2.

- Information Technology Infrastructure Library (ITIL) v3 – jedná se o nejrozšířenější rámec pro přístup k řízení IT služeb.

- Object Management Group (OMG) – jedná se o mezinárodní konsorcium, jehož členem jsou organizace a podniky působící v odvětví informačních technologií, vládní agentury, významné podniky využívající informační technologie a výzkumné instituce. OMG vydává mezinárodně platné normy v zaměřené na oblast informačních technologií.

- Federal Shared Services Strategy – poskytuje konzultace federálním agenturám. Podporuje úsilí federálních agentur v oblasti snížení finančních nákladů opětovné použití již využívaných aplikací, které poskytující stejné funkcionality.

- NIST Cloud Computing Reference Architecture (CCRA) and Taxonomy (Tax) – v rámci NIST SP 500-292 je definována obecná architektura, nezávislá na konkrétní implementaci.

Referenční model bezpečnosti tvoří nedílnou součást všech referenčních modelů vzhledem k faktu, že problematika bezpečnosti je nedílnou součástí všech úrovní organizace, od strategické až po operativní. Model podporuje vytváření a dodržování bezpečnostních politik, norem a standardů v rámci federálních agentur. Struktura modelu je složena ze 3 částí:

- Účel – bezpečnostní politiky a postupy musí být v souladu s legislativní předpisy a současně vést ke snižování bezpečnostních rizik identifikovaných na úrovni aplikací a IT systémů.

- Riziko – zavedením bezpečnostních politik a postupů je snižována hodnota rizika. Hodnota rizika je snížena prostřednictvím vyloučením zdroje hrozby nebo kontrolou dopadu rizika a pravděpodobnosti zneužití zranitelnosti.

- Řízení – bezpečnostní opatření zavedená v rámci systémů podléhají pravidelným kontrolám. Kontroly mohou být specificky zaměřeny na rizika, kterým daní federální agentura čelí. Výsledkem kontrol je identifikace nedostatků v nastavení bezpečnosti a doporučení pro zvýšení bezpečnostních opatření v rámci systémů federální agentury. Mezi obecné metody pro snížení rizik, využívaných rovněž i v rámci FEAF, patří (Řízení rizik projektu, 2019):

    - Mitigace (zmírnění, oslabení) rizika – jedná se o preventivní přístup k identifikovanému riziku. Cílem mitigace rizika je nalézt opatření, která snižují pravděpodobnost výskytu rizika.

    - Eliminace rizika – principem eliminace rizika je nalezení jiného řešení, které dané riziko vylučuje.

    - Přenos rizika – dopad rizika je přenesen na třetí stranu.

    - Přijmutí (akceptace) rizika – riziko je identifikováno a zaznamenáno. Přijmutí rizika je aktivní nebo pasivní. V případě pasivního přijmutí rizika je vytvořen pouze záznam o riziku, ale nejsou provedena opatření pro jeho mitigaci a rezervovány finanční prostředky potřebné pro mitigaci. Aktivní přístup přijmutí rizika je založen nejprve na vytvoření příslušné finanční rezervy, která je potřebná pro mitigaci rizika a následně provedení příslušných opatření pro snížení pravděpodobnosti jeho výskytu.

Za účelem efektivního nasazení a rozvoje enterprise architektury v rámci federální agentury, a tedy plánování přechodu od aktuálního stavu do budoucího (cílového) stavu je třeba využívat efektivní způsob přechodu mezi těmito dvěma stavy. S využitím principů enterprise architektury je agentura schopna popsat současný a cílový stav. Vhodným nástrojem, zaměřeným na proces strategie a plánu přechodu do budoucího stavu, který je využíván v rámci FEAF, je metodologie kolaborativního plánování (CPM). Metodologie kolaborativního plánování je proces zahrnující multidisciplinární analýzu. Součástí analýzy je identifikace sponzorů, zúčastněných stran, plánovačů a realizátorů změn, prostřednictvím kterých je dosaženo cílového stavu. Schiller (2013, s. 12-14).

5.5 DoDAF

DoDAF (Department of Defense Architecture Framework) je architektonickým rámcem enterprise architektury, který je využívaný v rámci organizací a dodavatelů, kteří spolupracují s ministerstvem obrany Spojených států amerických. Pokud není uvedeno jinak, vychází následující kapitola z oficiální dokumentace DoDAF vydané prostřednictvím ministerstva obrany Spojených států amerických (Architecture Development, 2019).

DoDAF podporuje 6 klíčových procesů, které využívají definovaný architektonický popis za účelem podpory rozhodování v oblastech působnosti ministerstva obrany Spojených států amerických.

- Sdílené schopnosti a rozvoj integrace (JCIDS) – cílem procesu je zajištění potřených schopností, které potřebují vojáci k úspěšnému provádění misí. Součástí je definice procesu spolupráce, který využívá architektonické popisy a společné koncepty k identifikaci příležitostí ke zlepšení v oblastech získávání schopností, školení personálu, vedení lidí, zajištění materiálové podpory (DOTMLPF) a rozhodování o způsobu zajištění těchto oblastí (materiálové a nemateriálové). Příležitosti ke zlepšení jsou popsány v sadě dokumentů, např. plán podpory informací, plán rozvoje schopností, plán získávání kapacit apod. Tyto dokumenty tvoří společné politiky pro podporu plnění požadavků na architekturu.

- Plánování, programování, rozpočtování a provedení (PPBE) – proces je odpovědný za přidělování prostředků v rámci působnosti ministerstva obrany Spojených států amerických. Proces řídí vývoj strategie, identifikaci potřeb, plánování a získávání zdrojů a dalších rozhodovacích procesů. DoDAF podporuje proces PPBE

prostřednictvím architektonického popisu v rámci kterého identifikuje data a možnosti jejich prezentace za účelem podpory rozhodování ve výše uvedených oblastech.

- Obraný akviziční systém (DAS) – proces zajišťuje na národní úrovni řízení financí do technologií, programů a produktového portfolia, které je nezbytné pro dosažení cílů národní bezpečnostní strategie s přímou vazbou na podporu zaměstnanosti a udržitelnosti ozbrojených sil Spojených států amerických. Politiky a principy obranného akvizičního systému jsou definovány ve směrnici 5000.1 ministerstva obrany Spojených států amerických. Závazným rámcem, který určuje podmínky provozování obranného akvizičního systému je instrukce 5000.2.2 ministerstva obrany Spojených států amerických.

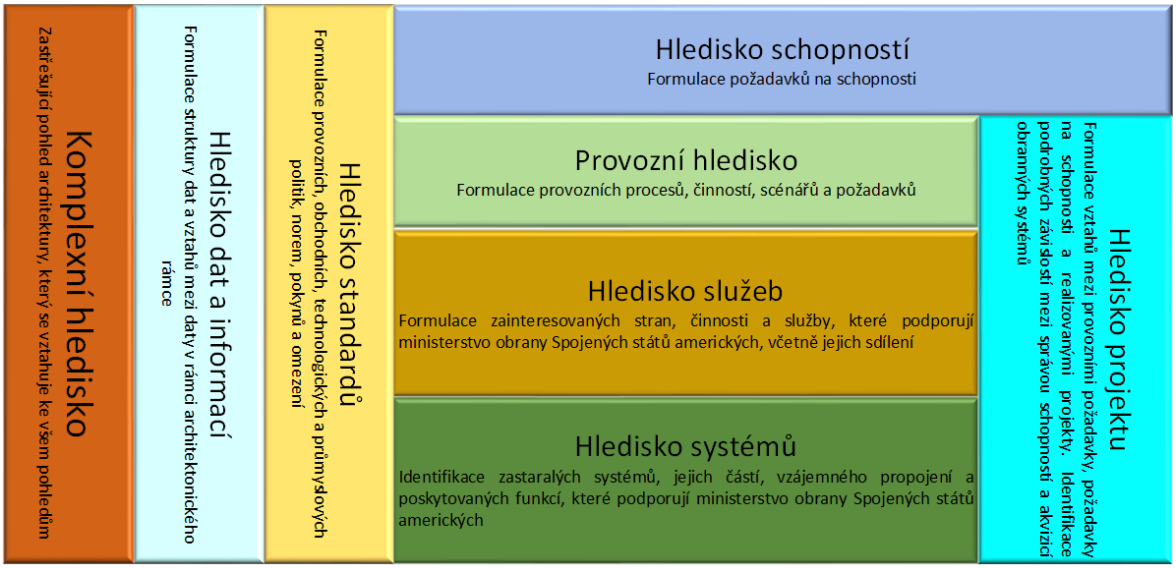
- Systémové inženýrství (SE) – směrnice 5000.1 a instrukce 5000.2.2 definují požadavky na využívání přístupu systémového inženýrství při akvizici obranných systémů. Cílem přístupu systémového inženýrství je akvizice obranných systémů s přiměřenými náklady včetně popisu činností a požadavků na zajištění zdrojů, které jsou pro úspěšnou akvizici nezbytné. DoDAF vytváří podporu pro proces systémového inženýrství prostřednictvím strukturovaného přístupu k vytváření dokumentace na základě požadavků na akvizici.

- Operační plánování (OPLAN) – operační plánování zahrnuje podporu opakovatelných činností, které nemění svoji strukturu. Jedná se zejména o plánování vojenských operací a definice projektů akvizic. Strukturu lze zahrnout do architektonického popisu prostřednictvím definice šablon dokumentů, kontrolních seznamů a jiných definovaných dokumentů, které jsou běžně používány pro podporu aktivit a akvizic v rámci ministerstva obrany.

- Správa portfolia schopností (CPM) – politiky ministerstva obrany Spojených států vyžadují, aby investice do informačních technologií byly spravovány jako portfolia. Účelem je zajištění, že investice podporují vize a cíle ministerstva obrany, tedy efektivní zajištění potřeb vojáků pro úspěšné zajištění misí a maximalizace návratnosti vynaložených investic do informačních technologií. Správa portfolia může být realizována prostřednictvím architektonických plánů, technik řízení rizik, plánování kapacit a měření výkonnosti.

První verze DoDAF byla publikována v roce 1996 pod označením Command, Control, Communications, Computers, and Intelligence Surveillance Reconnaissance Architecture Framework – C4ISR. O rok později byla vydána aktualizace s označením C4ISR v2.0. V rámci dalšího rozvoje byl rámec dále přizpůsobován potřebám ministerstva obrany. V roce 2001 byl rámec C4ISR přepracován a vydán pod názvem DoDAF 1.0. Další aktualizace byla vydána jako DoDAF v1.5 v roce 2007. O dva roky později byla vydána verze DoDAF v2.0. V současné době je aktuální verzí DoDAF v2.02. (Hurst, 2017, s. 20-21)

Klíčovou změnou v aktuální verzi DoDAF je zaměření nikoli na produkt, které bylo klíčové v předchozích verzích, ale na tzv. architektonická data. Interpretace dat je zajištěna prostřednictvím modelů (model). Mezi modely se řadí dokumenty, tabulky, dashboardy apod. Model obsahující data je nazýván pohledem (view). Sbírka pohledů je označována jako hledisko (viewpoint) (Masuda, Shirasaka a Yamamoto, 2016, s. 10). V terminologii architektonického rámce TOGAF existují rovněž hlediska, která jsou označována jako artefakty. Komplexní architektonický pohled v rámci DoDAF sestává z množiny hledisek. Obrázek 24 reflektuje celkem 8 hledisek DoDAF, která obsahují obecné informace o organizaci a zároveň detailní informace pro specifické využití. Součástí 8 hledisek je celkem 53 modelů, které slouží jako příklady pro intepretaci architektonických dat. (Ertaul a Hao, 2011, s. 1–3)



Obrázek 24 - DoDAF architektonická hlediska. Zdroj: upraveno dle Architecture Development (2019)

- Komplexní hledisko obsahuje informace o architektonickém popisu jako celku. Jedná se o popis vizí, cílů, plánů, aktivit a omezujících podmínek pro nasazení enterprise architektury a přechodu mezi současným a cílovým stavem.

Součástí komplexního hlediska je výkladový slovník všech termínů, které jsou využívány v rámci enterprise architektury.

- Hledisko dat a informací formuluje požadavky na sdílené informace a data organizace a zároveň obsahuje popis informací a dat, které jsou využívány v rámci enterprise architektury, formou definice atributů, charakteristiky dat a jejich vzájemných vztahů. Výstup ve formě hlediska dat využijí zejména obchodní manažeři organizace a zaměstnanci IT oddělení v závislosti na míře detailu, kterou hledisko obsahuje.

- Hledisko standardů tvoří sadu pravidel, která definují požadavky na uspořádání, vzájemnou interakci a závislost systémů nebo jejich částí. Účelem hlediska standardů je zejména zajištění, aby systém splňoval definované provozní požadavky. Hledisko standardů obsahuje soubor provozních, obchodních, technologických a průmyslových politik, norem, pokynů a omezení. Nepovinnými parametry souboru jsou datum platnosti, datum účinnosti a datum zrušení příslušných dokumentů spolu s informací, jakým způsobem budou již neplatné dokumenty nahrazeny. Výstup ve formě hlediska standardů využijí zejména obchodní manažeři organizace a zaměstnanci IT oddělení pro účely měření a porovnání míry plnění provozních požadavků.

- Hledisko schopností reprezentuje strategické vize a cíle organizace s vazbou na množinu potřebných schopností, které jsou nezbytné pro naplnění vizí a strategických cílů organizace. Výstup ve formě hlediska schopností je určen zejména vedení organizace za účelem nastavení procesu zajištění potřebných schopností prostřednictvím adekvátního počtu zaměstnanců s potřebnou kvalifikací a schopnostmi.

- Provozní hledisko poskytuje informace o klíčových provozních procesech, činnostech, scénářích a uživatelských požadavcích. Na základě uvedených informací lze vytvořit logický popis cílové enterprise architektury a identifikovat klíčové prvky a systémy v současné architektuře.

- Hledisko služeb popisuje služby, jejich vzájemné propojení a sdílení včetně definice SLA. Účelem popisu je podpora klíčových činností ministerstva obrany Spojených států amerických. Modely služeb zároveň vytváří asociace mezi službami a požadavky na provoz a množinu nezbytných schopností potřebných pro provozování služby.

- Hledisko systémů obsahuje popis systémů organizace. Součástí popisu je identifikace systémů, jejich vzájemného propojení, využívání zdrojů, poskytovaných funkcionalit a dostupnosti.

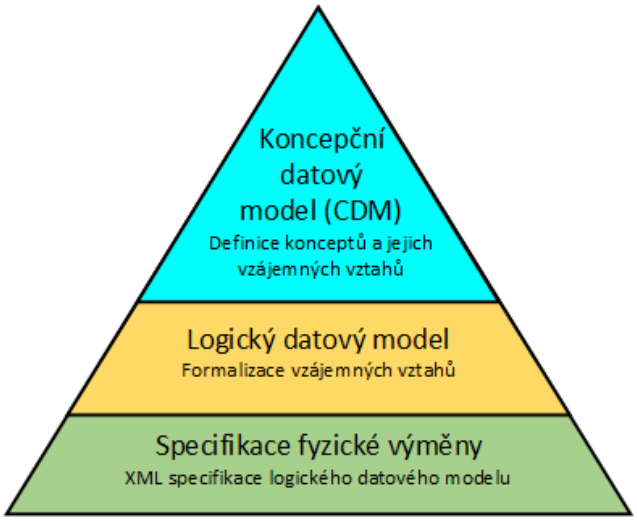
- Hledisko projektu obsahuje realizované, aktuální a rozvojové projekty. Hledisko obsahuje pohledy, které mapují organizace a jejich projekty včetně časových harmonogramů realizace projektů. Účelem popisu je, stejně jako v případě hlediska služeb, podpora klíčových činností ministerstva obrany Spojených států amerických.

Identifikace a shromažďování architektonických dat je v rámci DoDAF řešena prostřednictvím DODAF meta-modelu (DM2). Uvedený meta-model nahradil základní architektonický datový model (CADM), který byl využíván v předchozích verzích DoDAF.

Obrázek 25 zobrazuje hierarchickou strukturu DM2, která je složena celkem ze 3 vrstev. Koncepční datový model definuje architektonický popis prostřednictvím vysokoúrovňového pohledu na architektonická data. Při popisu nejsou využívány odborné technické pojmy, takže výsledný pohled umožňuje porozumět dané problematice rovněž manažerům a vedoucím pracovníkům organizace.

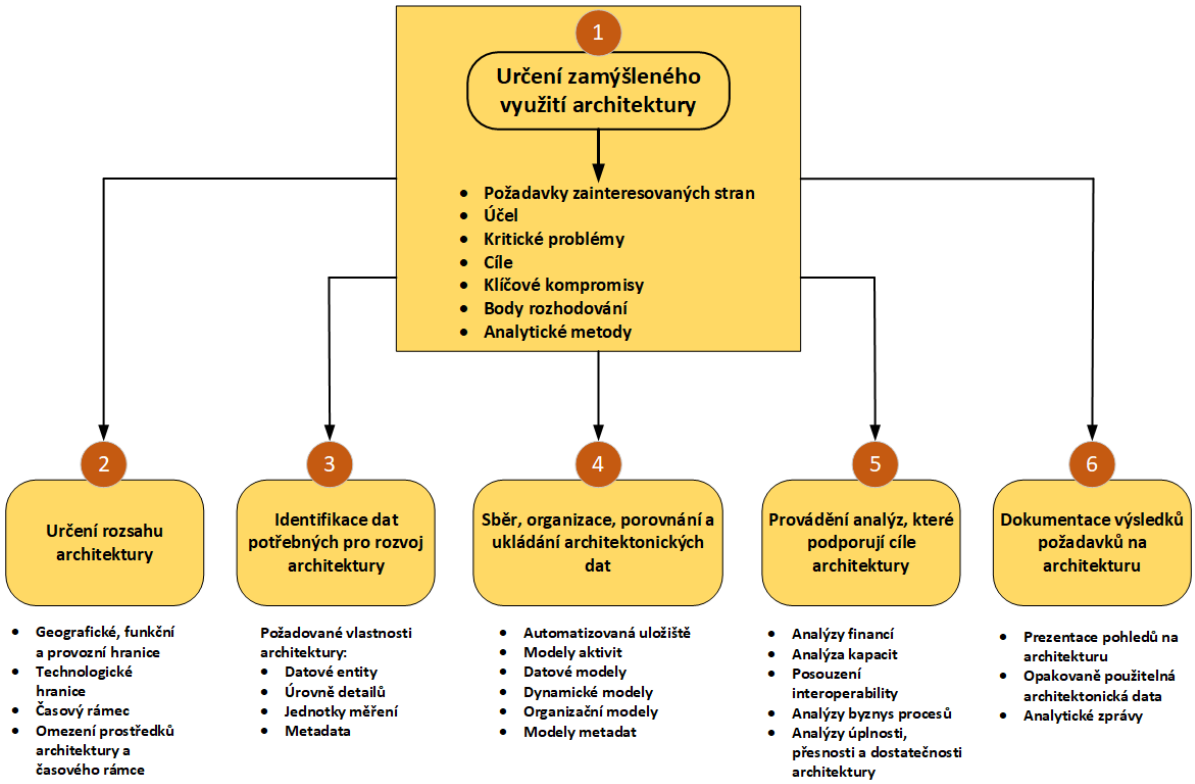
Logický datový model obohacuje architektonický popis z koncepčního datového modelu o identifikaci vzájemných vztahů mezi architektonickými daty a definici atributů dat.

Specifikace fyzické výměny obohacuje logický datový model o datové typy. Výsledkem specifikace fyzické výměny je vygenerovaný XSD soubor, který reprezentuje XML schema výměny dat.



Obrázek 25 - DM2. Zdroj: upraveno dle Architecture Development (2019)

DoDAF přistupuje k návrhu enterprise architektury s využitím iteračního 6 krokového procesu (Masuda, Shirasaka a Yamamoto, 2016, s. 10). Obrázek 26 zobrazuje těchto 6 kroků.



Obrázek 26 - Proces vývoje architektury DoDAF. Zdroj: upraveno dle Architecture Development (2019)

V prvním kroku je definován zejména účel využití enterprise architektury. Dále je prováděn sběr požadavků na enterprise architekturu od zainteresovaných stran, definovány metody pro vývoj enterprise architektury a metody kategorizace dat. Nezbytnou součástí prvního kroku je definice procesu pro měření výkonnosti enterprise architektury, které poskytuje vlastník procesu.

Druhým krokem je stanovení rozsahu architektury. Rozsah vymezuje geografické, funkční, provozní a technologické hranice, které určují hloubku a šířku architektonického popisu. Účelem vymezení rozsahu je definice pouze takového rozsahu, který umožňuje dosáhnout očekávaných výsledků. Neomezení rozsahu může vést ke zpoždění nebo neúspěchu projektu. Rozsah lze definovat prostřednictvím definice a popisu dat, která mají být využita v popisu architektury.

Třetí krokem je identifikace dat potřebných pro rozvoj architektury – architektonických dat. Jedná se zejména o datové entity, atributy a asociace. Úroveň detailu, která má být zachycena

pro každou z datových entit a atributů, je stanovena analýzou procesu, který je podroben kontrole prováděné během stanovení rozsahu v kroku 2.

Součástí čtvrtého kroku je sběr, organizace, porovnávání a ukládání architektonických dat, která byla identifikována ve třetím kroku. Odpovědnost za výše uvedené aktivity mají enterprise architekti, kteří data organizují a pro účely rozhodování je následně interpretují prostřednictvím modelů. DoDAF současně doporučuje, aby data byla uložena v komerčně dostupném nástroji.

V pátém kroku jsou prováděny analýzy za účelem podpory cílů enterprise architektury. Výstupy analýz identifikují úroveň dodržování požadavků na enterprise architekturu vlastníkem procesu. Výstupem je architektonický popis, který je následně schvalován vlastníkem procesu.

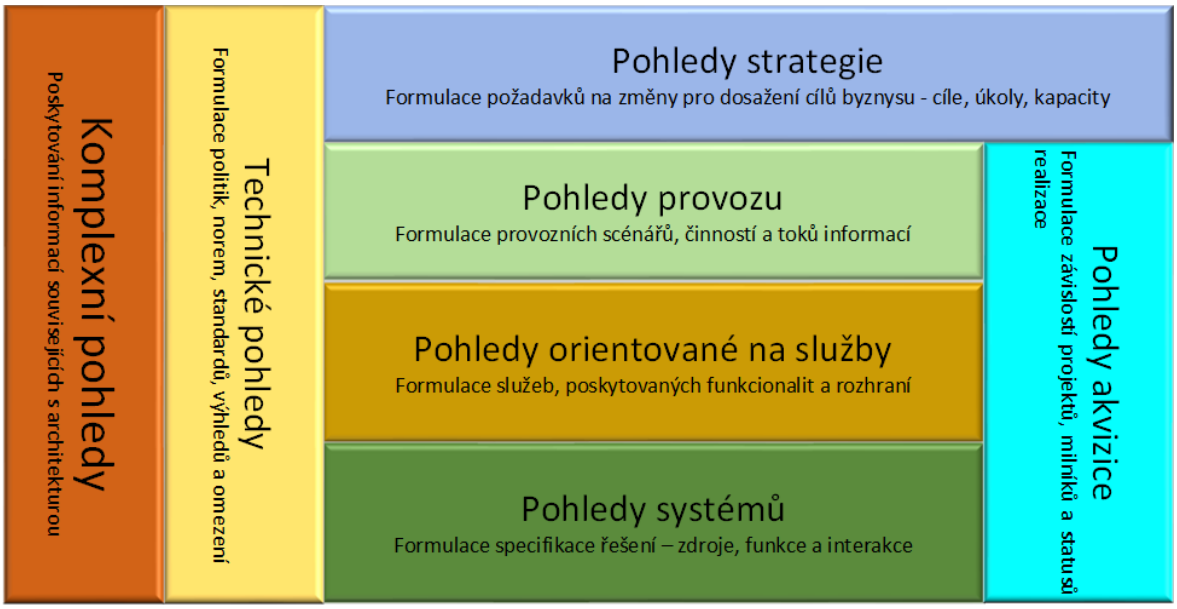
Posledním krokem je prezentace výsledků požadavků na architekturu. Výsledky jsou prezentovány formou pohledů. Pohledy byly vytvořeny již ve třetím kroku. Součástí pohledů jsou data, která byla identifikována ve druhém kroku.

5.6 MODAF

MODAF (British Ministry of Defence Architecture Framework) představuje rámec pro enterprise architekturu, který je využíván v rámci ministerstva obrany Velké Británie. Pokud není uvedeno jinak, vychází tato kapitola z oficiální dokumentace MODAF, vydané ministerstvem obrany Velké Británie (MOD Architecture Framework - GOV.UK, 2012). Historie MODAF začíná v srpnu 2005, kdy byla vydána první verze MODAF v1.0. Vzhledem k tomu, že se jedná o architektonický rámec využívaný pro ministerstvo obrany, vycházela první verze MODAF z rámce DoDAF v1.0, který byl využíván ministerstvem obrany Spojených států amerických. Zásadním rozdílem oproti DoDAF v 1.0 bylo přidání dvou pohledů – strategického a akvizičního. V dubnu 2007 byla vydána aktualizovaná verze MODAF v1.1. V září 2008 byla vydána zatím poslední verze MODAF v1.2.

Stejně jako DoDAF je MODAF zaměřena na prezentaci enterprise architektury prostřednictvím architektonických dat. Pro reprezentaci architektonických dat využívá MODAF pohledy (views). V rámci MODAF je využívaná odlišná terminologie než v případě DoDAF. Pohledy (views) v DoDAF jsou hledisky (viewpoints) v MODAF a současně produkty (products) v DoDAF jsou pohledy (views) v MODAF.

Obrázek 27 zobrazuje celkem 6 skupin pohledů MODAF, které poskytují vizualizaci enterprise architektury v grafické a textové formě stejně jako rámec DoDAF. Pohledy podporují zájmy zúčastněných stran za účelem dosažení cílů byznysu. Součástí 6 skupin pohledů je celkem 47 pohledů.



Obrázek 27 - MODAF pohledy. Zdroj: upraveno dle: (MOD Architecture Framework - GOV.UK, 2012)

Součástí každého pohledu je definice jeho využití v rámci enterprise architektury a současně definice datových objektů, které reprezentují daný pohled.

- Pohledy strategie – definují požadavky na dosahované výsledky byznysu včetně identifikace potřebných schopností, které jsou nezbytné pro dosažení definovaných výsledků.
- Pohledy provozu – definují požadavky na zajištění kapacit prostřednictvím identifikace potřebných procesů, informací a lidských zdrojů.
- Pohledy orientované na služby – popisují služby potřebné k podpoře procesů definovaných v pohledu provozu.
- Pohledy systémů – popisují implementaci pohledu provozu a pohledu orientovaného na služby. Tím je zajištěna definice řešení.
- Pohledy akvizic – popisují časové harmonogramy projektů a jejich vzájemné závislosti. Realizací projektů je zajištěno dosahování definovaných výsledků byznysu, a tedy požadavků na enterprise architekturu.

- Technické pohledy – definují standardy, které musí být implementovány v rámci projektu a musí je cílové řešení splňovat.

- Komplexní pohledy – poskytují komplexní popis a obsah enterprise architektury.

Identifikace, shromažďování a prezentace architektonických dat je v rámci MODAF řešena prostřednictvím MODAF meta-modelu (M3)[13]. Meta-model umožňuje prezentaci výměnu dat architektonických dat mezi architektonickými řešeními, která jsou modelována v odlišných softwarových aplikacích.

Základem meta-modelu MODAF je využití XMI (XML metadata Interchange) pro výměnu architektonických dat. Jedná se o standard pro výměnu metadat prostřednictvím formátu XML. Za účelem znovupoužitelnosti XMI rozhraní pro výměnu dat je současně MODAF meta-model rozšířením UML meta-modelu, který rovněž využívá XMI jako standardizovaný prostředek pro výměnu dat.

[13]MODAF meta-model je ve své specifikaci velice rozsáhlý a není primárním předmětem této práce. Detailní specifikace MODAF meta-modelu je k dispozici zde.

6 KOMPARATIVNÍ ANALÝZA RÁMCŮ ENTERPRISE ARCHITEKTURY

Za účelem vytvoření nové metodiky pro zaznamenávání činností a událostí na prvcích kritické informační infrastruktury v prostředí energetických systémů je nezbytným předpokladem zajištění efektivního návrhu a implementace systémů bezpečnostního monitoringu v rámci celého životního cyklu jejich existence. Efektivní návrh musí současně pokrývat požadavky a potřeby dané organizace.

Architektura a komponenty energetických řídicích systémů, které jsou zároveň kritickou informační infrastrukturou tvoří velice rozsáhlou a komplexní IT/OT infrastrukturu (od centrálního dispečinku energetické soustavy až po komponenty IED, RTU apod. v rámci jednotlivých rozvoden), což je detailně reflektováno zejména v kapitole 2 teoretické části této práce. Je nezbytně nutné, aby navržená metodika reflektovala tuto skutečnost a její struktura vycházela z nejlepší praxe v oblasti navrhování rozsáhlých architektonických řešení (viz kapitoly 4.3 a 5) se zohledněním požadavků na zajištění kybernetické bezpečnosti.

Navržená metodika musí současně reflektovat soulad s regulatorními (legislativními a normativními) požadavky na zajištění kybernetické bezpečnosti energetických řídicích systémů, které je organizace zavázána plnit a za které je vrcholově odpovědné vedení organizace. Bylo by mylné se domnívat, že zajištění kybernetické bezpečnosti je vztaženo pouze na implementaci technických opatření. Nezbytnou součástí zajištění kybernetické bezpečnosti jako celku je i sada organizačních opatření daných regulatorními předpisy, které musí být pro zajištění efektivity implementovány do stávajících či nových procesů společnosti. Implementace organizačních opatření do stávajících či nových procesů organizace musí zohledňovat návazností na potřeby zainteresovaných stran s přihlédnutím k zahrnutí dodavatelského řetězce. Tímto způsobem se stává implementace efektivní.

Pro vytvoření metodiky pro zaznamenávání činností a událostí na prvcích kritické informační infrastruktury v prostředí energetických systémů je tedy výchozím předpokladem nalezení vhodného rámce enterprise architektury, který bude zároveň tvořit základní rámec navržené metodiky a v rámci návrhu bude zohledňovat specifické požadavky a vlastnosti těchto systémů:

- Rozsáhlosti architektur současných energetických systémů (viz kapitola 2.5),
- Kombinace IT a OT prvků a jejich vzájemné kooperace.
- Byznys požadavků organizace.
- Regulatorních požadavků relevantních zejména pro oblast kybernetické bezpečnosti.
- Zajištění potřeb zainteresovaných stran.

Za tímto účelem je nezbytným krokem provedení srovnávací, resp. komparativní analýzy možných přístupů, tedy výše přestavených mezinárodních standardů pro enterprise architekturu, které se zabývají se uvedenou problematikou. Jak bylo uvedeno v kapitole 4.3.1, v současné době jsou nejvíce využívány rámce TOGAF, FEAF, MODAF, DoDAF a Zachman (Bejšovec, 2010, s. 21; Lapalme (2016, s. 104). S Bejšovcem a Lapalmem se v uvedené problematice shodují také Hinkelmann (2016, s. 79), Dang a Pekkola (2015, s. 141) a (Ferrugento a Rocha, 2015, s. 351).

Za účelem porovnání rámců byly zvoleny pohledy (perspektivy) a hlediska, která jsou obsažena v různých formách ve všech představených rámcích zaměřených na oblast enterprise architektury. Je nutné si uvědomit, že toto porovnání reprezentuje pohledy a hlediska jednotlivých rámců na enterprise architekturu. Aby bylo možné toto porovnání relevantním způsobem kvantifikovat a vybrat relevantní rámec, je v dalším kroku vybráno několik kritérií, která jsou relevantní pro oblast energetických systémů a reflektují výše uvedené specifické požadavky těchto systémů. Následně je provedeno ohodnocení jednotlivých rámců podle vybraných kritérií a vybrán určující rámec, který bude tvořit základ nové metodiky.

6.1 Analýza dle pohledů (perspektiv)

Analýza dle pohledů (perspektiv) vychází ze Zachmanova rámce, který je přehledně reprezentován grafickou formou. Součástí grafické formy je specifikace rolí a odpovědností v klíčových procesech organizace, v tomto případě využití specifické části příslušného rámce.

Pohled plánovače (planner) zahrnuje v obecné rovině zejména koncepty a definuje rozsahy potřebných prací (scope) na abstraktní úrovni.

Pohled vlastníka (owner) představuje zejména pohled managementu organizace ve vztahu k zajištění plnění byznys požadavků. Pohled vlastníka uvádí do kontextu koncepty a rozsahy potřebných prací definovaných plánovači s požadavky byznysu. U Zachmanova rámce je výstupem této fáze byznys model.

Pohled designera (designer) transformuje požadavky byznys modelu do funkčních architektonických bloků (IT technologie, zákazníci apod.). U Zachmanova rámce je výstupem této fáze systémový, resp. architektonický model.

Pohled architekta se zaměřuje na transformaci architektonických bloků do technických specifikací funkcionalit systémů, které mají být implementovány. U Zachmanova rámce je výstupem této fáze technologický model.

Pohled programátora zahrnuje detailní reprezentaci funkcionalit systémů a jejich realizaci, která je výstupem této fáze. Uživatelský pohled nahlíží na systém jako funkční celek s definovanými funkcionalitami.

Tabulka 8 reprezentuje analýzu dle pohledů (perspektiv) z pohledu zúčastněných stran. Podobný typ porovnání využívá např. Plojhar (2015, s. 20).

Tabulka 8 - Porovnání pohledů (perspektiv) rámců EA. Zdroj: vlastní zpracování

Rámec	Plánovač (planner)	Vlastník (Owner)	Designer (designer)	Architekt (builder)	Programátor (programmer)	Uživatel (User)
Zachman	Rozsah (scope)	Byznys model	Systémový, Architektonický model	Technologický model	Detailní reprezentace	Funkční systém
TOGAF	Přípravná fáze/vize architektury v ADM	Byznys architektura v ADM	Architektura IS/technologická architektura v ADM		Plánování migrace vADM	
FEAF	Model výkonnosti	Referenční model byznysu	Referenční model architektury	Referenční model architektury a dat	Referenční model infrastruktury	
DoDAF	Komplexní hledisko, hledisko standardů a hledisko projektu	Provozní hledisko	Hledisko systémů a služeb	Hledisko dat a informací		
MODAF	Komplexní pohledy, pohledy akvizice	Pohledy strategie	Technické pohledy	Pohledy orientované na služby, pohledy systémů		

Rámec TOGAF reflektuje pohled plánovače v ADM v rámci přípravné fáze a fáze vize architektury. Je vytvořen projektový plán (scope) a vize pro nasazení enterprise architektury v organizaci spolu s identifikací zúčastněných stran a bezpečnostních požadavků, za které je vedení organizace zodpovědné a musí být reflektovány v rámci organizace. Pohled vlastníka koresponduje se Zachmanovým rámcem – vize a projektový plán jsou uvedeny do kontextu s požadavky byznysu pro zajištění naplnění obchodních cílů organizace. Výstupem této fáze je byznys architektura. Nezbytnou součástí byznys architektury je reflektování bezpečnostních požadavků z vize architektury a identifikaci vlivu implementace bezpečnostních požadavků na byznys cíle organizace. Pohled designera koresponduje v rámci TOGAF ADM s pohledem architekta. Tyto 2 role spolu v rámci TOGAF ADM úzce spolupracují při transformaci byznys architektury do funkčních architektonických bloků a technických specifikací. V rámci TOGAF ADM jsou tyto výstupy vytvořeny zejména ve fázi architektury IS a technologické architektury. Na jejich základě je vytvořen plán migrace k cílové architektuře. Velkou přidanou hodnotou při využití TOGAF je možnost správy řízení funkčních a nefunkčních požadavků týkajících se architektury systémů, bezpečnostních požadavků, byznys požadavků, resp. požadavků všech zúčastněných stran. Správa požadavků může vstupovat do všech fází ADM prostřednictvím fáze managementu požadavků. Požadavky tak mohou být řízeny operativně a efektivně v rámci celého životního cyklu systémů a aplikací.

Rámec FEAF koresponduje s rámcem Zachman v 5 pohledech – plánovač, vlastník, designer, architekt a programátor. Oproti TOGAFu je FEAF primárně zaměřen pouze na oblast enterprise architektury v kontextu jednotného přístupu napříč spolupracujícími organizacemi ovšem bez detailnější vazby na IT architekturu rozsáhlých systémů.

Rámec DoDAF koresponduje s rámcem Zachman ve 4 pohledech – plánovač, vlastník, designer a architekt. Pohled plánovače prostřednictvím komplexního hlediska, které popisuje scope projektu včetně vizí, cílů, plánů a aktivit pro nasazení enterprise architektury. Plánovač současně může využít hledisko standardů a hledisko projektu. Z těchto hledisek lze využít vstupy týkající se souboru průmyslových politik, norem, pokynů a omezení a současně realizované projekty, které musí být zohledněny v rámci nasazení enterprise architektury jako komplexního celku. Pohled vlastníka vychází z komplexního hlediska, resp. výstupu od plánovače a je dále reflektován a rozpracován prostřednictvím provozního hlediska. Provozní hledisko zahrnuje informace o klíčových procesech, činnostech, scénářích a uživatelských požadavcích na enterprise architekturu. Pohled designera dále detailněji

specifikuje služby a systémy, které podporují klíčové procesy a činnosti organizace a byly identifikovány vlastníkem, prostřednictvím hledisek systémů a služeb. Specifikace služeb zahrnuje jejich popis, účel a vzájemné propojení. Specifikace systémů zahrnuje identifikaci systémů, jejich vzájemného propojení, využívaných zdrojů, poskytovaných funkcionalit a parametrů dostupnosti.

Rámec MODAF koresponduje s rámcem Zachman ve 4 pohledech – plánovač, vlastník, designer, architekt. Pohled plánovače je založen zejména na komplexních pohledech na enterprise architekturu, které poskytují její kompletní popis. Součástí komplexních popisů však není definice scope projektu. Pohledy plánovače tedy korespondují s rámcem Zachman pouze částečně. Pohledy vlastníka navazují a dále rozpracovávají pohledy plánovače prostřednictvím využití pohledů strategie, kde jsou reprezentovány požadavky byznysu na dosahované výsledky. Designer dále rozvíjí danou oblast o definici standardů, které musí být v rámci řešení implementovány. Pohledy architekta rozvíjí vstupy od designera prostřednictvím popisu služeb potřebných k podpoře podnikových procesů a popisují implementaci procesů a služeb.

6.2 Analýza dle hledisek

Analýza dle hledisek vychází, stejně jako analýza pohledů, ze Zachmanova rámce, který je přehledně reprezentován grafickou formou. Součástí grafické formy je specifikace oblastí, které definují 6 hledisek zúčastněných stran (Co, Jak, Kde, Kdo, Kdy a Proč), v tomto případě využití specifické části příslušného rámce.

Tabulka 9 reprezentuje výsledky porovnání hledisek jednotlivých rámců enterprise architektury.

Hledisko **Co** (what) se zaměřuje na identifikaci dat a informací, která jsou klíčová z pohledu byznysu. Hledisko **Jak** (how) se zaměřuje na identifikaci podnikových procesů. Aktuální a potencionální místa byznysu a obchodních aktivit jsou identifikována prostřednictvím hlediska **Kde** (where). Identifikace zainteresovaných osob v byznysu organizace, kteří mají odpovědnost za implementaci a dodržování požadavků enterprise architektury je předmětem hlediska **Kdo** (who). Časový harmonogram, resp. plán implementace projektů a zajištění jejich souladu s enterprise architekturou je předmětem hlediska **Kdy** (when). Poslední hledisko **Proč** (when) identifikuje motivaci k zavedení enterprise architektury ve vazbě na plnění byznys požadavků, cílů a strategii organizace.

Tabulka 9 – Porovnání hledisek rámů EA. Zdroj: vlastní zpracování

Rámec	Co (what)	Jak (how)	Kde (where)	Kdo (who)	Kdy (when)	Proč (why)
Zachman	Data	Procesy	Síť, obchodní místa	Lidé a odpovědnosti	Časový plán	Motivace
TOGAF	ADM přípravná fáze a ADM fáze C (data)	Architecture capability framework a ADM přípravná váze	Architecture capability framework a ADM přípravná váze	Architecture capability framework a ADM přípravná fáze	ADM fáze F (plánování migrace) a přípravná fáze	Architecture capability framework a ADM přípravná fáze
FEAF	Referenční model dat	Referenční model architektury	Referenční model byznysu a infrastruktury			
DoDAF	Hledisko dat a informací	Provozní hledisko	Hledisko systémů	Provozní hledisko		
MODAF	Komplexní pohledy, DODAF meta-model (M3)	Pohledy provozu	Komplexní pohledy	Pohledy provozu	Pohledy akvizic, komplexní pohledy	

V rámci TOGAFu jsou plně reflektována všechna hlediska zúčastněných stran. Hledisko **Co** reprezentováno prostřednictvím přípravné fáze, která identifikuje současný stav a fáze C – architektura IS. Výstupem fáze C je detailní popis datové architektury a aplikací pro správu dat. Hlediska **Jak, Kde, Kdo** a **Proč** reflektuje TOGAF prostřednictvím Architecture Capability Frameworku (ACF). Obsahem ACF jsou informace o organizaci, organizační struktuře, zavedených procesech, dovednostech a povinnostech a rolích osob, které jsou zainteresovány v implementaci, nastavení pravidel a správy enterprise architektury v rámci

organizace. Hledisko **Kdy** je reflektováno architektonickou roadmapou v rámci přípravy implementačních a migračních plánů.

FEAF reflektuje pouze 3 hlediska zúčastněných stran. Hledisko **Co** je reprezentováno prostřednictvím referenčního modelu dat, který identifikuje data a informace v kontextu jejich sdílení napříč federálními agenturami. V porovnání s TOGAF se FEAF zaměřuje spíše na platformu pro sdílení dat a nikoli na detailní popis entit a jejich vzájemných vazeb. Důvodem je samotné zaměření rámce FEAF na spolupráci v rámci federálních agentur Spojených států. Hledisko **Jak** je částečně reprezentováno prostřednictvím referenčního modelu architektury za využití kategorizace a možností opětovného využití aplikací ve vazbě na podnikové procesy. Hledisko **Kde** je částečně reflektováno v referenčních modelech byznysu a infrastruktury prostřednictvím identifikace federální agentury a její působnosti v rámci Spojených států. Referenční model infrastruktury je založen na registru aktiv. FEAF doporučuje, aby nedílnou součástí identifikace každého aktiva byla identifikace umístění, kde se dané aktivum fyzicky nachází. Ze seznamu umístění lze identifikovat místo působnosti federální agentury, ale nikoli potencionální místa byznysu. Hledisko **Kde** je tedy reflektováno pouze částečně.

U rámce DODAF lze na základě srovnávací analýzy identifikovat reflektování 6 hledisek – **Co, Jak, Kde a Kdo, Kdy a Proč**. Hledisko **Co** je v DoDAF reflektováno prostřednictvím hlediska dat a informací za využití DoDAF meta-modelu (DM2). Hledisko dat a informací obsahuje formulaci požadavků na informace a data organizace včetně jejich popisu, definice atributů, charakteristik a vzájemných vztahů. Formulace provozních procesů je součástí provozního hlediska, které ale neobsahuje specifikaci procesů organizace jako celku. Provozní hledisko tedy reflektuje hledisko **Jak** pouze částečně. Hledisko **Kde** je částečně reflektováno prostřednictvím hlediska projektu, které obsahuje seznam aktuálních, realizovaných a plánovaných projektů. Z informací o aktuálních a realizovaných projektech lze identifikovat aktuální místa byznysu organizace. Seznam plánovaných projektů může obsahovat i seznam potencionálních míst pro rozšiřování byznysu. Na druhou stranu informace o projektech identifikují čas provádění plánů organizace a reflektují tak hledisko **Kdy** a částečně hledisko **Proč**. Hledisko **Proč** je reflektováno prostřednictvím závazku podpory klíčových činností ministerstva obrany Spojených států. Hledisko **Kdo** je reflektováno pouze částečně prostřednictvím hlediska služeb, které identifikuje zainteresované strany a požadavky na provoz služeb. Součástí hlediska není identifikace osob, kteří jsou zainteresováni v byznysu organizace a jsou odpovědní za implementaci enterprise architektury.

MODAF reflektuje 5 hledisek rámce Zachman, ale většinu z nich pouze částečně. Hledisko **Co** je reflektováno částečně prostřednictvím komplexních pohledů, které disponují přehledem nad všemi ostatními pohledy. Primárním vstupem pro identifikaci dat a informací, která jsou pro byznys klíčová poskytuje MODAF meta-model (M3). Hledisko **Jak** je reprezentováno pohledy provozu, resp. identifikací provozních procesů. Stejně jako v případě DoDAF nejsou obsahem specifikace všechny procesy organizace jako celku a hledisko je tedy reflektováno pouze částečně. Hledisko **Kde** může být částečně reflektováno prostřednictvím komplexních pohledů, ale přesná identifikace aktuálních a potencionálních míst byznysu není explicitně v MODAF pohledech zakotvena. Částečně reflektováno je v pohledech provozu MODAF také hledisko **Kdo**, které definuje požadavky na zajištění lidských zdrojů, ale pouze v oblasti provozu, nikoli organizace jako celku. Kombinace pohledů akvizic a komplexních pohledů reflektují hledisko **Kdy**. Pohledy akvizic zahrnují časové plány projektů a jejich vzájemné závislosti.

6.3 Výběr určujícího rámce pro metodiku

Za účelem výběru rámce, který bude určující pro nově vytvořenou metodiku, je nezbytné kvantifikovat výše uvedené obecné porovnání rámců s důrazem na možnosti jejich využití v energetických systémech. Pro tento účel je využit princip multikriteriální analýzy. V 1. kroku je nutné identifikovat příslušná kritéria, která jsou určující pro oblast a problematiku návrhu bezpečnostního monitoringu tak, aby tento návrh byl v souladu s legislativními a normativními požadavky, které jsou kladeny na energetické systémy kritické informační infrastruktury. Současně musí kritéria zohledňovat specifické vlastnosti energetických systémů. Na základě výše uvedených skutečností byla vybrána následující kritéria:

- Do jaké míry je schopen rámec reflektovat budování rozsáhlých architektur současných energetických systémů?
    - Je nutné reflektovat heterogenní architekturu energetických systémů s důrazem na jejich specifika – viz kapitola 2.
- Do jaké míry je rámec využitelný při reflektování potřeb zainteresovaných stran v rámci návrhu řešení?
    - V návrhu řešení je nutné identifikovat a zohlednit požadavky všech zainteresovaných stran. Jedná se zejména o správce a dodavatele energetických systémů, byznys vlastníky a vrcholové vedení společnosti.

- Do jaké míry je rámec schopen reflektovat externí vstupy obsahující legislativní a regulatorní požadavky na dané řešení?
    - V tomto bodě je zohledněna potřeba zajištění souladu navrhovaného řešení s legislativními a regulatorními požadavky, které jsou relevantní zejména pro oblast kybernetické bezpečnosti – viz kapitola 3.2.
- Do jaké míry daný rámec reflektuje byznys požadavky společnosti na navrhované řešení?
    - Důraz je kladen na zajištění efektivity, snížení nákladů (CAPEX, OPEX) nebo přínosu ve formě zisku v oblastech řešení bezpečnostních událostí a incidentů, zvýšení efektivnosti provozu systémů prostřednictvím proaktivního přístupu k monitoringu, efektivní způsob komunikace mezi zainteresovanými osobami a odděleními ve společnosti, efektivní způsob komunikace s externími autoritami, zajištění kontinuity činností v případě výskytu bezpečnostní události nebo incidentu?
- Do jaké míry daný rámec reflektuje požadavky již provozovaných systémů, aplikací a technických prostředků energetických systémů při návrhu řešení bezpečnostního monitoringu?
    - Energetické systémy jsou specifické rozsáhlou a specifickou architekturou, která je mimo jiné ovlivněna předpokládanou dlouhou životností zařízení (viz kapitola 2). Je nezbytné aby daný rámec reflektoval soulad navrhovaného řešení bezpečnostního monitoringu s touto architekturou, resp. architekturou bezpečnostních systémů, které společnost již využívá.
- Do jaké míry je rámec schopen reflektovat rizika a omezení integrace energetických systémů do navrhovaného řešení?
- Do jaké míry je rámec schopen aplikovat rámce z oblasti procesního řízení s důrazem na zajištění oblastí řešení událostí a incidentů?
    - Tento bod reflektuje potřeby zajištění životního cyklu řešení událostí a incidentů v energetických systémech ve vazbě na životní cyklus IT a OT prvků a jejich vzájemné kooperace. Současně reflektuje legislativní požadavky v oblasti evidence a řešení událostí a incidentů – viz kapitola 3.2.

- Do jaké míry je rámec schopen aplikovat jiné rámce v oblasti procesního řízení s důrazem na zajištění oblastí operativního řízení změn?
    - Tento bod reflektuje potřeby zajištění životního cyklu řízení změn v energetických systémech ve vazbě na plnění legislativních požadavků – viz kapitola 3.2.
- Do jaké míry je rámec schopen reflektovat a využít plán migrace?
    - Plán migrace je nezbytnou součástí pro zajištění přechodu k cílové architektuře vzhledem k již uvedené rozsáhlosti energetických systémů?
- Do jaké míry je rámec schopen validovat navržené řešení s enterprise architekturou společnosti.
- Do jaké míry je rámec vhodný pro opakování iterací za účelem zvyšování vyspělosti navrženého řešení?
    - V rozsáhlém heterogenním prostředí energetických systémů a velkého množství zainteresovaných stran, které vstupují do celého procesu návrhu je velice pravděpodobné, že po první iteraci nebude dosaženo cílové architektury a bude nutné provést další iterace. Opětovný průchod iteracemi přispěje ke zvýšení vyspělosti navrženého řešení a posunu k cílové architektuře.

Ve 2. kroku je nutné ohodnotit výše uvedená kritéria na základě stupnice. Pro účely analýzy byla zvolena následující intervalová stupnice:

1. Není možné využít
2. Využitelný částečně – využitelné jen vybrané části rámce
3. Využitelný s omezeními – rámec z větší části reflektuje dané kritérium.
4. Plně využitelný – rámec plně reflektuje požadavky daného kritéria

Tabulka 10 zobrazuje hodnocení jednotlivých kritérií v jednotlivých rámcích na základě výše uvedené stupnice.

Tabulka 10 – Hodnocení kritérií na základě stupnice. Zdroj: vlastní zpracování

Kritérium	Zachman	TOGAF	FEAF	DoDAF	MODAF
Budování rozsáhlých architektur energetických systémů	2	3	2	2	2
Zajištění potřeb zainteresovaných stran v celém procesu návrhu	2	4	2	3	3
Reflektování legislativních a regulatorních požadavků	1	3	2	4	2
Reflektování byznys požadavků společnosti v procesu návrhu	2	4	3	3	2
Reflektování prostředků provozovaných energetických systémů v procesu návrhu	2	3	3	3	2
Reflektování rizik a integračních omezení v procesu návrhu	1	4	3	2	2
Aplikace rámců pro zajištění oblasti řešení událostí a incidentů	1	3	2	2	1
Aplikace rámců pro zajištění oblasti řízení změn	1	3	2	2	1
Reflektování požadavků pro zajištění plánu migrace v procesu návrhu	2	3	2	2	2
Zajištění validace navrženého řešení s enterprise architekturou společnosti	3	4	4	4	4
Zajištění opakování iterací za účelem zvyšování vyspělosti navrženého řešení	3	4	3	3	3

Jakmile jsou kritéria ohodnocena, je nutné jim přiřadit váhy tak, aby součin ohodnocení kritérií a vah odpovídal významnosti daného kritéria. Ve 3. kroku tedy byly kritériím přiřazeny váhy na stupnici 0 – 3, kde 3 reprezentuje nejvyšší váhu, 0 nejnižší váhu. Daná kritéria nejsou obecná, ale specificky vztažená a relevantní pro oblast energetických systémů, což je reflektováno váhou u každého kritéria.. Ve 4. kroku je vypočteno celkové hodnocení jednotlivých kritérií ve vazbě na jednotlivé rámce a stupnice. Tabulka 11 zobrazuje celkové výsledky hodnocení kritérií na základě zvolené stupnice a váhy.

Tabulka 11 - Celkové hodnocení rámců na základě zvolených kritérií. Zdroj: vlastní zpracování.

Kritérium	Váha	Zachman váha	TOGAF váha	FEAF váha	DoDAF váha	MODAF Váha
Budování rozsáhlých architektur energetických systémů	3	6	9	6	6	6
Zajištění potřeb zainteresovaných stran v celém procesu návrhu	3	6	12	6	9	9
Reflektování legislativních a regulatorních požadavků	3	3	9	6	12	6
Reflektování byznys požadavků společnosti v procesu návrhu	2	4	8	6	6	4
Reflektování prostředků provozovaných energetických systémů v procesu návrhu	3	6	9	9	9	6
Reflektování rizik a integračních omezení v procesu návrhu	2	2	8	6	4	4
Aplikace rámců pro zajištění oblasti řešení událostí a incidentů	3	3	9	6	6	3
Aplikace rámců pro zajištění oblasti řízení změn	3	3	9	6	6	3
Reflektování požadavků pro zajištění plánu migrace v procesu návrhu	2	4	6	4	4	4
Zajištění validace navrženého řešení s enterprise architekturou společnosti	3	9	12	12	12	12

Kritérium	Váha	Zachman váha	TOGAF váha	FEAF váha	DoDAF váha	MODAF Váha
Zajištění opakování iterací za účelem zvyšování vyspělosti navrženého řešení	3	9	12	9	9	9
Celkem		**55**	**103**	**76**	**83**	**66**

Na základě výsledků kvantifikovaného porovnání zřejmé, že TOGAF je s celkovým počtem 103 bodů vhodným rámcem pro zajištění budování řešení bezpečnostního monitoringu v kontextu enterprise architektury, se současným zohledněním specifických požadavků energetických řídicích systémů určených jako kritická informační infrastruktura.

Výsledky komparativní analýzy současně ukazují, že TOGAF reflektuje všechna hlediska a zároveň většinu pohledů, které jsou využívány klíčovými rolemi napříč celým životním cyklem enterprise architektury s vazbou na cíle byznysu. Ve vazbě na energetické systémy je dále TOGAF schopen reflektovat legislativní a regulatorní požadavky relevantní zejména pro oblast kybernetické bezpečnosti. Současně TOGAF je schopen reflektovat požadavky zainteresovaných stran v celém procesu návrhu.

Na první pohled by bylo logickým krokem využití rámce Zachman, jehož fáze představovaly určující kritéria pro obecnou komparativní analýzu (kapitoly 6.1 a 6.2). Na druhou stranu, velkou nevýhodou rámce Zachman je jeho statičnost – slouží primárně pouze pro popis současného stavu architektury a procesů a nikoli modelaci budoucího stavu architektury. Zde je možné nalézt další velkou přidanou výhodu TOGAFu, který prostřednictvím Architecture Capability Frameworku (ACF) obsahuje informace o organizaci, organizační struktuře, zavedených procesech, dovednostech, povinnostech a rolích osob, které jsou zainteresovány v procesu návrhu architektury energetických řídicích systémů a jejich vazbou na zajištění kybernetické bezpečnosti. Nedílnou součástí TOGAFu je proces managementu požadavků, resp. správa řízení funkčních a nefunkčních požadavků architektury pro všechny fáze ADM za účelem efektivního řízení enterprise architektury jako jednoho funkčního celku. Prostřednictvím ACF a procesu managementu požadavků je schopen TOGAF rychle a adekvátně reagovat na případné změny a požadavky na architekturu s využitím informací v ACF.

Částečnou nevýhodou provedené obecné komparativní analýzy je její zaměření pouze na oblast enterprise architektury, resp. budování rozsáhlých bezpečnostních řešení. Ve vztahu nejen k systémům zajišťujících zaznamenávání činností v energetických systémech,

zajišťuje ve většině případů pouze soulad navržené architektury s požadavky byznysu a high-level pohledu na architekturu rozsáhlých systémů. Pohled byznysu se soustřeďuje primárně pouze na ekonomické aspekty implementace a provozování systémů a případně na dodržení souladu se zákonnými a regulatorními požadavky týkající se zaznamenávání činností a událostí, ale nikoli na oblast provozování konkrétních řešení.

Využití principů enterprise architektury v návrhu architektury rozsáhlých bezpečnostních řešení pro zaznamenávání činnosti v prostředí energetických systémů tedy tvoří pouze jednu část. Není řešena oblast operativního provozu těchto systémů a s tím souvisejících procesů s vazbou na byznys cíle organizace. Pro tuto oblast je vhodné využít mapování TOGAF na rámce, které se zaměřují na operativní úroveň řízení a IT governance, tedy např. ITIL nebo COBIT. Jak již bylo uvedeno v předchozích kapitolách této práce, počet kybernetických útoků, které jsou cíleny na energetické systémy, resp. energetický sektor, v posledních letech neustále narůstá. Dle regulatorních a zákonných požadavků, kterým energetické společnosti podléhají je nezbytné, aby byly schopny, prostřednictvím operativního provozu bezpečnostních řešení, disponovat informacemi o aktivitách v energetických systémech prostřednictvím jejich zaznamenávání. Informace o aktivitách jsou základními stavebními kameny, které organizaci slouží k vyšetřování příčin kybernetického útoku, identifikaci napadených systémů, časové posloupnosti útoku a nasazení preventivních opatření k zamezení opakování útoku a tím minimalizaci případných škod, resp. finančních dopadů na společnost. Tyto specifické potřeby lze zajistit mapování na rámce, které se zaměřují na operativní úroveň řízení, byly reflektovány prostřednictvím určujících kritérií v provedené multikriteriální analýze.

Z výše uvedeného jasně vyplývá potřeba nejen souladu architektury navrhovaných systémů bezpečnostního monitoringu s požadavky enterprise architektury. Navržená metodika musí zohlednit i specifické potřeby související s provozem tohoto typu systémů, které budou mít pro společnost provozující energetické systémy také přidanou hodnotu ve formě rychlé a adekvátní reakce na bezpečnostní události a incidenty, včetně kontextových informací týkajících se dané události.

7 NÁVRH METODIKY SEC-MON

Na základě provedené komparativní analýzy lze konstatovat, že navrhovaná metodika SEC-MON bude tvořit podporu pro návrh komplexní bezpečnostní infrastruktury, resp. bezpečnostního monitoringu, plně reflektující požadavky pro zaznamenávání činnosti na prvcích kritické informační infrastruktury energetických systémů. Motivací pro vytvoření nové metodiky je zejména propojení specifických požadavků návrhu systémů bezpečnostního monitoringu s principy enterprise architektury. Cílem metodiky není specifikovat konkrétní kroky implementace specifických bezpečnostních technologií ve společnosti nebo organizaci. Důvodem je, že tento přístup netvoří obecný rámec pro budování komplexní bezpečnostní infrastruktury.

Metodika SEC-MON vychází z architektonického rámce TOGAF s přihlédnutím k požadavkům na specifika provozu systémů bezpečnostního monitoringu ve vztahu k plnění legislativních požadavků v působnosti zákona o kybernetické bezpečnosti. Využití rámce TOGAF určuje strukturu navrhované metodiky jako celku. Základem navržené metodiky je metoda ADM, jejíž fáze jsou uspořádány do kruhu a vzájemně se ovlivňují prostřednictvím managementu změn.

Metodika SEC-MON zároveň vysvětluje institut zajištění monitoringu činností a nastiňuje možnosti řešení plnění povinností povinných osob dle zákona o kybernetické bezpečnosti. Metodika vychází z více mezinárodních standardů zabývajících se specifickými oblastmi týkajících se efektivního využívání informačních technologií a zejména bezpečnosti informačních technologií s důrazem na návrh robustních architektonických řešení, které reflektují požadavky na zaznamenávání činností a událostí.

7.1 Pro koho je metodika určena

Metodika SEC-MON je určena primárně společnostem, jejichž oblast podnikání je zaměřena na energetický sektor a současně jsou provozovateli kritické informační infrastruktury, resp. jsou identifikovány jako povinné osoby dle zákona o kybernetické bezpečnosti včetně příslušných prováděcích vyhlášek, zejména VoKB. Povinné osoby jsou povinny implementovat požadavky zákona o kybernetické bezpečnosti a příslušných prováděcích vyhlášek ve vztahu k učeným systémům kritické informační infrastruktury.

Sekundárně může metodika sloužit jako vodítko společnostem a organizacím podnikajících v energetickém sektoru, které mají implementovaný a certifikovaný mezinárodní standard

bezpečnosti informací dle ISO 27001 nebo zvažují jeho implementaci případně certifikaci, případně očekávají, že se stanou povinnými osobami dle zákona o kybernetické bezpečnosti. V České republice je v současné době metodika relevantní zejména pro provozovatele přenosové a distribuční soustavy, kteří provozují systémy kritické informační infrastruktury - jsou povinnými osobami dle zákona o kybernetické bezpečnosti.

Vzhledem k faktu, že problematika bezpečnosti energetických řídicích systémů je aktuálním trendem v celosvětovém měřítku, což bylo výrazným způsobem reflektováno v předchozí části této práce (zejména v kapitole 3), je metodika v případě překladu do cizího jazyka univerzálním nástrojem i pro zahraniční společnosti a organizace podnikající v energetickém sektoru, které se zabývají problematikou návrhu architektury monitorovacích systémů v kontextu enterprise architektury.

V rámci budoucí vědecko-výzkumné činnosti, může být rozšířena aplikace metodiky i do jiných průmyslových odvětví, která mají svá specifika při návrhu architektury bezpečnostních systémů s vazbou na řídicí systémy využívané v daném odvětví. V každém průmyslovém odvětví, resp. v každé společnosti jsou požadavky byznysu orientovány odlišně.

Účelem metodiky není poskytnutí detailních informací pro implementaci konkrétních bezpečnostních řešení. Tento přístup je velice obtížný a netvoří obecný rámec pro návrh architektury komplexní bezpečnostní infrastruktury.

7.2 Legislativní rámec metodiky SEC-MON

Legislativní rámec, který je relevantní pro tuto metodiku byl detailně představen v kapitole 3.2 této práce. Rámec je reprezentován zejména zákonem o kybernetické bezpečnosti České republiky č. 316/2014 Sb. resp. jeho novelizace č. 205/2017 Sb. a krizovým zákonem č. 240/2000 Sb.

Detailní požadavky na implementaci bezpečnostních opatření stanovuje příslušná prováděcí vyhláška č. 316/2014 Sb. o kybernetické bezpečnosti, resp. její novelizace č. 82/2018 Sb.

Vzhledem k faktu, že energetické systémy spadají do kritické infrastruktury a kritické informační infrastruktury státu, se energetická společnost stává povinnou osobou v oblasti kybernetické bezpečnosti a ukládají se jí povinnosti v oblasti kybernetické bezpečnosti.

7.3 Struktura metodiky SEC-MON

Metodika sestává ze 9 fází, které na sebe navazují. V porovnání s rámcem TOGAF, ze kterého metodika vychází došlo k přejmenování některých fází a redukci jejich počtu. Přejmenování a redukce jednotlivých fáze koresponduje se zaměřením metodiky na oblast nasazení komplexního bezpečnostního monitoringu v souladu s principy enterprise architektury. Jednotlivé fáze již netvoří pouze obecný rámec pro implementaci enterprise architektury jako v případě TOGAF, ale jsou konkretizovány v souladu s návrhem komplexního bezpečnostního monitoringu ve společnosti. Metodika se skládá z následujících fází:

- Přípravná fáze – cílem této fáze je zejména identifikace regulatorních a legislativních požadavků týkajících se zaznamenávání činností a událostí, které je organizace zavázána plnit.

- Vize architektury bezpečnostního monitoringu – cílem této fáze je vytvoření abstraktního modelu bezpečnostní infrastruktury pro monitoring činností a událostí. Za tímto účelem je nutné identifikovat všechny lokality centrálních dispečinků, které slouží pro řízení energetické soustavy a současně všech transformoven/rozvoden, které jsou určeny dle ZoKB jako kritická informační infrastruktura. Klíčovým faktorem je identifikace zúčastněných stran a povinných bezpečnostních rolí, které participují v procesu zajištění požadavků týkajících se monitoringu činností a zaznamenávání událostí z hlediska požadavků kybernetické bezpečnosti dle regulatorních a legislativních požadavků. V této fázi je rovněž důležité identifikovat externí autority, které mají vazbu na plnění legislativních povinností organizace. Důležité vstupy do této fáze tvoří požadavky na vytvoření nebo změnu systémů bezpečnostního monitoringu, které byly identifikovány v přípravné fázi prostřednictvím legislativních požadavků. Výstupem fáze je vytvořený abstraktní model bezpečnostního monitoringu organizace.

- Vazba na byznys architekturu – Cílem této fáze je provést srovnání vytvořeného abstraktního modelu bezpečnostního monitoringu s byznys architekturou a zajištění jejich souladu na všech úrovních řízení organizace – strategické, taktické a operativní. Je nutné kvalifikovaně rozhodnout o přístupu k budování bezpečnostního monitoringu ve vazbě na zajištění kapacit (interní, externí) a s tím související finanční náklady. Toto rozhodnutí má významný dopad na byznys společnosti. Soulad s byznys architekturou je stěžejním výstupem této fáze.

- Vazba na architekturu IS – fáze koresponduje s TOGAF a je rozdělena na dvě na sebe navazující části – aplikační a datová architektura. Výstupem fáze je vytvořený architektonický pohled zajišťující soulad s datovou architekturou společnosti. Soulad s aplikační architekturou musí zohlednit provozované aplikace, technická aktiva – infrastrukturu, virtualizační nástroje a podpůrná technická aktiva potřebná pro provoz systémů (racky, UPS, baterie apod.). Identifikace výše uvedených aktiv je úzce spjata s provedením analýzy rizik, která zohledňuje dopady, hrozby a zranitelnosti pro jednotlivá aktiva.

- Návrh technologického řešení – součástí fáze je návrh integrace systémů do bezpečnostního monitoringu. Výstupy této fáze zahrnují identifikaci systémů, aplikací a aktiv, které mají být integrovány do bezpečnostního monitoringu. Dále je nutné vytvořit návrh komunikačního propojení podpůrných technických aktiv (systémů) do bezpečnostního monitoringu s důrazem na zajištění dostupnosti, důvěrnosti a integrity dat v rámci komunikační sítě a systémech bezpečnostního monitoringu. Jsou definovány komunikační protokoly pro přenos záznamů o činnostech a událostech. Součástí fáze je rovněž zajištění řešení jednotného času a vzdáleného přístupu k systémům bezpečnostního monitoringu. Výstupem této fáze je schválený návrh technologického řešení systémů bezpečnostního monitoringu, který je schválený managementem organizace.

- Validace navrženého řešení – navržený model bezpečnostního monitoringu je validován s požadovaným stavem. Požadovaný stav je identifikován požadavky byznys architektury, architektury IS a technologické architektury. Jsou posuzována rizika, která souvisí s nasazením bezpečnostního monitoringu a jejich dopady do energetických systémů. Dále je na abstraktní úrovni navržen plán implementační, resp. migrační plán navrženého řešení.

- Návrh migrace a zavedení governance – Cílem fáze je navržení detailního migračního plánu ze současného stavu architektury do cílového stavu. V této fázi je abstraktní migrační plán rozpracován do dílčích fází, kroků a činností, které obsahují časový plán realizace a identifikují odpovědné osoby za realizaci. Implementace systémů bezpečnostního monitoringu je vzhledem k rozsáhlosti architektur energetických systémů komplexní záležitostí. Z tohoto důvodu je pro přechod k cílové architektuře vhodné využití metodik a principů projektového řízení a zavedení governance.

Zavedením projektového řízení je zajištěn dohled nad řízením projektu v rámci celého životního cyklu jeho implementace, a především kontrola termínů plnění dílčích činností a úkolů. Zavedením governance je zajištěn dohled a řízení rizik souvisejících s implementací navrženého řešení.

- Stanovení provozního modelu navrženého řešení – součástí fáze je definice požadavků souvisejících s provozem systémů bezpečnostního monitoringu. Je nutné zejména vytvořit/upravit pravidla obsahující pokyny a postupy včetně eskalačních postupů při vyhodnocování událostí a incidentů. Dále je nutné definovat postupy pro řízení změn a problémů navrženého řešení s vazbou na jednotné kontaktní místo zajišťující jejich evidenci. Součástí této fáze je dále návrh postupů pro ověření implementace nápravných opatření vydaných externími autoritami.

- Stanovení procesu řízení změn navrženého řešení – v této fázi je navržený model, včetně hodnocení migračního plánu a provozního modelu podroben revizi a jsou identifikovány požadavky na změny. Revize modelu je vedena formou připomínkování všech zúčastněných stran. Na základě výstupu této fáze je možné relevantním způsobem rozhodnout, zda je navržené řešení v souladu s principy enterprise architektury v dané společnosti nebo je nezbytné opakování určitých fází metodiky či provedení dalších iterací za účelem dosažení požadovaného stavu architektury.

7.4 Fáze metodiky SEC-MON

V následující části budou podrobně popsány jednotlivé fáze metodiky. Metodika SEC-MON využívá principů iterativního přístupu, na kterém je založen rovněž TOGAF. Jedná se o dynamický přístup. Tento přístup je v současné době široce využíván zejména v oblasti agilních metodik vývoje software. Využití nachází i v dalších oblastech týkajících se informačních technologií. Podstatou iterativního přístupu je opakování určitých fází za účelem dosažení očekávaného výsledku v krátkém časovém období. Na každou fázi metodiky lze tedy s využitím iterativního přístupu nahlížet jako na proces, kdy pro splnění jedné fáze a zahájení další fáze je nutné v každé fázi definovat cíle, vstupy, provedené kroky a výstupy.

7.4.1 Přípravná fáze

Cíle: cílem této fáze je zejména identifikace regulatorních a legislativních požadavků týkajících se zaznamenávání činností a událostí, které je organizace zavázána plnit.

Vstupy:

- **Legislativa –** vstupy jsou tvořeny zejména legislativními a normativními standardy, normami a zákony. V případě provozování kritické informační infrastruktury jsou relevantními vstupy, které je nezbytné zohlednit zejména Zákon o kybernetické bezpečnosti č. 181/2014 Sb. a Vyhláška o kybernetické bezpečnosti č. 314/2016.

- **Interní dokumentace –** dále je nutné zohlednit stávající vstupy, které má organizace k dispozici a tyto mají dopad do návrhu a provozování systémů bezpečnostního monitoringu a budování enterprise architektury. Jedná se zejména o stávající metodiky, směrnice, provozní předpisy, rozhodnutí o určení prvků KII, strategické dokumenty určující strategii společnosti v oblasti IT a OT, existující architektonický rámec, principy architektury apod.

Kroky:

1. krok zahrnuje analýzu legislativních požadavků. Zahrnuje současné legislativy týkající se požadavků na zaznamenávání činností a událostí v organizaci. Zcela zásadní je formalizování těchto požadavků do interního dokumentu organizace tak, aby tyto požadavky mohli být reflektovány ve všech projektech, které mají dopad na určené prvky KII a organizace s nimi byla v souladu. Pomocným krokem v rámci analýzy může být kapitola 3.2.4 této práce, která tyto požadavky představuje. V rámci analýzy je nutné reflektovat i další legislativu, která je pro danou organizaci relevantní. Jedná se zejména o následující legislativu:

- Zákon č. 458/2000 Sb. zákon o podmínkách podnikání a o výkonu státní správy v energetických odvětvích a o změně některých zákonů (energetický zákon);

- Pravidla provozování distribuční soustavy (PPDS) 2018;

- Zákon č. 240/2000 Sb. zákon o krizovém řízení a o změně některých zákonů (krizový zákon), ve znění pozdějších předpisů;

- Vyhláška MPO č. 80/2010 Sb. ze dne 18. 3. 2010 Sb. o stavu nouze v elektroenergetice a o obsahových náležitostech havarijního plánu;

- Vyhláška MPO č. 79/2010 Sb. ze dne 18. 3. 2010 Sb. o dispečerském řízení elektrizační soustavy a o předávání údajů pro dispečerské řízení energetický zákon, pravidla provozování distribuční soustavy apod.

2. krok je analýza interní dokumentace. Cílem je analyzovat stávající dokumentaci týkající se systémů bezpečnostního monitoringu a v rámci ní reflektovat legislativní požadavky na zaznamenávání činností a událostí.

Výstupy:

- **Požadavky na zaznamenávání činností a událostí** – formalizovaný a schválený dokument obsahující požadavky na zaznamenávání činností a událostí energetických systémů určených jako KII, které mají být integrovány do systémů bezpečnostního monitoringu.

- **Interní dokumentace** – stávající metodiky, směrnice, provozní předpisy, rozhodnutí o určení prvků KII, strategické dokumenty určující strategii společnosti v oblasti IT a OT, existující architektonický rámec, principy architektury apod. Nedílnou součástí interní dokumentace se stává dokument obsahující požadavky na zaznamenávání činností a událostí.

7.4.2 Vize architektury bezpečnostního monitoringu

Cíle: cílem této fáze je vytvoření abstraktního modelu bezpečnostního monitoringu zaznamenávání činností a událostí. Za tímto účelem je nutné identifikovat všechny lokality centrálních dispečinků, které slouží pro řízení energetické soustavy a současně všech transformoven/rozvoden, které jsou určeny dle ZoKB jako kritická informační infrastruktura. Důležitým vstupem jsou formalizované požadavky na systémy bezpečnostního monitoringu. Komplexní návrh bezpečnostního monitoringu se neobejde bez podpory vedení společnosti a součinnosti zainteresovaných stran, které jsou reprezentovány interními zaměstnanci společnosti a současně dodavateli energetických a bezpečnostních systémů. Pro zajištění podpory v rámci celé společnosti je tedy nezbytné identifikovat všechny zainteresované strany, stanovit jejich pravomoci a odpovědnosti v rámci návrhu a provozu systémů bezpečnostního monitoringu. Současně je nutné vytvořit komunikační plán, který definuje komunikační kanály a pravidla komunikace mezi zainteresovanými stranami. Důležité vstupy do této fáze tvoří legislativní požadavky na vytvoření nebo změnu systémů bezpečnostního monitoringu, které byly identifikovány v přípravné fázi. Výstupem fáze je vytvořený abstraktní model bezpečnostního monitoringu společnosti.

Vstupy:

- **Výstupy předcházející fáze:**
    - **Požadavky na zaznamenávání činností a událostí** – formalizovaný dokument s požadavky na zaznamenávání činností a událostí.
    - **Interní dokumentace –** aktuální dokumentace relevantní k návrhu a provozování systémů bezpečnostního monitoringu a enterprise architektury.
- **Požadavky na systémy bezpečnostního monitoringu –** potřeby a požadavky společnosti na systémy bezpečnostního monitoringu. Potřeby a požadavky musí být interpretovány v dokumentovatelné formě. Dokument by měl obsahovat v abstraktní rovině zejména legislativní, normativní, bezpečnostní a provozní požadavky včetně požadavků na integraci energetických systémů do bezpečnostního monitoringu a s tím související procesy managementu událostí, incidentů a řízení změn (pokud jsou k dispozici).
- **Organizační struktura –** stávající organizační struktura zahrnující všechny pracovní funkce ve společnosti, včetně odpovědností a rolí jednotlivých osob.
- **Seznam lokalit –** identifikace fyzického umístění prvků KII. Lokality centrálních dispečinků, transformoven/rozvoden, datových center, komunikačních uzlů apod.

Kroky:

1. krok je zahájení návrhu systémů bezpečnostního monitoringu. Pro úspěšné zahájení je třeba zajistit výše uvedené vstupní podklady. Pokud uvedené dokumenty neexistují nebo míra jejich detailu neodpovídá požadavkům, mohou být tyto doplněny nejpozději před vstupem do příslušné fáze, kde jsou využívány.

2. krok je identifikace zúčastněných stran, které participují v procesu zajištění souladu organizace s legislativními požadavky týkajících se systémů bezpečnostního monitoringu, resp. monitoringu činností a událostí. Pomocným materiálem pro identifikaci zúčastněných stran je dokumentovaná organizační struktura společnosti. Při identifikaci zúčastněných stran musí být kladen důraz na soulad s požadavky zákona o kybernetické bezpečnosti, který specifikuje povinné bezpečnostní role v dané společnosti, ve vztahu k plnění legislativních požadavků.

Jak bylo uvedeno, energetické systémy jsou tvořeny rozsáhlým portfoliem technologií, které vyžadují specifické znalosti jejich implementace a správy. Současně jsou tyto systémy typické svoji geografickou rozlehlostí, a tedy i rozsáhlou architekturou. Efektivní návrh bezpečnostního monitoringu musí zohlednit všechny výše uvedené aspekty. Ve fázi identifikace zúčastněných stran by měla organizace reflektovat zejména následující strany:

- Vrcholové vedení (zástupce vrcholového vedení) společnosti.
- Povinné role dle zákona o kybernetické bezpečnosti:
    - Manažer kybernetické bezpečnosti,
    - architekt kybernetické bezpečnosti,
    - garant primárního aktiva,
    - garant podpůrného aktiva,
    - výbor pro řízení kybernetické bezpečnosti a
    - určený administrátor systému.
- Interní administrátoři energetických systémů a pověření zaměstnanci externích dodavatelů (SCADA, RTU, HMI apod.), kteří disponují specifickými znalostmi o daných technologií a systémech.
- Interní administrátoři IT infrastruktury (datová centra, servery, síťové technologie apod.), kteří disponují informacemi o dostupné infrastruktuře včetně HW parametrů provozovaných systémů a aplikací.
- Administrátoři jednotného kontaktního místa, ve kterém jsou vedeny všechny požadavky na konfigurační úpravy, evidenci událostí a incidentů a správu systémů bezpečnostního monitoringu.
- Analytici odpovědní za vyhodnocování událostí a incidentů ze systémů bezpečnostního monitoringu a jejich eskalaci.
- Dodavatelé energetických systémů (SCADA, RTU, HMI apod.).
- Dodavatelé systémů bezpečnostního monitoringu.

3. krok zahrnuje detailní identifikaci zainteresovaných stran. Jedná se o určení konkrétních zaměstnanců v organizační struktuře, jejich rolí a odpovědností při návrhu, implementaci a provozování systémů bezpečnostního monitoringu.

Kompetentnost zainteresovaných stran a zaměstnanců lze ověřit na základě odpovídajícího vzdělání, zkušeností nebo absolvovaných odborných certifikací. Kritickým faktorem úspěchu u zainteresovaných stran je zajištění rozvoje jejich odborných zkušeností prostřednictvím odborných školení a seminářů, zaměřených na vykonávanou činnost. Seznam zainteresovaných stran včetně jejich kompetentnosti je nutné dokumentovat. Zainteresované strany si musí být vědomi své role (přínosů a důsledků nepřizpůsobení) při participaci na návrhu, implementaci a správě a servisu systémů bezpečnostního monitoringu.

Ve třetím kroku jsou stejným způsobem identifikování dodavatelé stávajících systémů bezpečnostního monitoringu, případně potenciální dodavatelé nových systémů a jejich kompetence.

4. krok zahrnuje stanovení komunikačního plánu zainteresovaných stran**.** Stanovení plánu je nezbytnou součástí návrhu systémů bezpečnostního monitoringu. Komunikační plán musí jasně specifikovat kanály a prostředky vzájemné komunikace zainteresovaných stran. Zahrnuje zejména pravidla vzájemné komunikace v případě procesu identifikace, eskalace a řešení (kybernetických) bezpečnostních událostí a incidentů. Pokud by komunikační plán neexistoval, vystavuje se společnost riziku, které souvisí s časovou prodlevou informování zainteresovaných stran v případě výskytu události či incidentu.

V 5. kroku je nutné identifikovat kapacity. Tento krok představuje kritický faktor úspěchu návrhu systémů bezpečnostního monitoringu. Nedostatečné kapacitní plánování může v extrémním případě vést k zastavení všech činností nejen při návrhu, ale také realizaci a provozování systémů bezpečnostního monitoringu. Kapacitní plánování je založeno na identifikaci a alokaci potřebných zdrojů. Identifikuje zejména kapacity lidských zdrojů a technologií. Určujícími kritérii je maximální kapacita lidských zdrojů a technologií. Na základě identifikace kapacit je vytvořen kapacitní plán, který obsahuje varianty pro různé prognózy budoucích požadavků legislativy a byznysu. Jedním z přístupů, který je možné pro kapacitní plánování využít, je kapacitní plánování dle ITSM rámce ITIL.

Metoda kapacitního plánování v ITIL je založena na dvou přístupech:

- Proaktivní – trendy, modelování změn, údržba kapacitních plánů.
- Reaktivní – monitorování, měření a reporting, reakce na kapacitní události, reakce na výkonnostní problémy.

6. krokem je identifikace IT a OT strategie. V tomto kroku je nutné stanovit na abstraktní úrovni soulad požadavků kladených na systémy bezpečnostního monitoringu se strategií v oblasti IT a OT. IT strategie definuje zásady, cíle, finanční náklady a dovednosti potřebné k využití IT prostředků, za účelem jejich efektivního využívání v rámci celé organizace. Strategie v oblasti OT se primárně zaměřuje na stejné aspekty jako oblast IT strategie s důrazem na specifika OT systémů. V oblasti energetiky se jedná primárně o pravidla a standardy pro budování transformoven/rozvoden, požadavky na provedení a architekturu řídicích systémů, standardy pro řešení LAN/WAN komunikace z transformoven/rozvoden apod. Výstupem tohoto kroku je tedy stanovení souladu navrženého řešení s IT a OT strategií organizace na abstraktní úrovni. Stanovení detailního propojení navrženého řešení se stávajícími IT a OT systémy společnosti je součástí fáze 4 – návrh technologického řešení bezpečnostního monitoringu.

7. krokem je porovnání požadavků kladených na systémy bezpečnostního monitoringu s byznys cíli organizace. V této fázi jsou požadavky porovnávány pouze na abstraktní úrovni. Cílem fáze není budování byznys architektury dané společnosti. Výstupem fáze je určení míry shody, resp. potvrzení či nepotvrzení souladu cílů organizace s požadavky na systémy bezpečnostního monitoringu. Primárním byznys cílem společností, podnikajícím v energetickém sektoru, je zejména zachování dodávek elektrické energie v požadovaném rozsahu a kvalitě. Provozování systémů bezpečnostního monitoringu podporuje včasnou identifikaci a remediaci (kybernetických) bezpečnostních událostí a incidentů, jejichž dopady mohou vést v segmentu energetiky k omezení dodávek elektrické energie, a tedy velkým finančním ztrátám, ztrátám na lidských životech a zejména ztrátě reputace. Zároveň je společnost povinna dle zákona o kybernetické bezpečnosti hlásit kybernetické bezpečnostní incidenty bez zbytečného prodlení NUKIB. Pokud společnost nenahlásí identifikovaný kybernetický bezpečnostní incident vystavuje se finančnímu postihu až do výše 1 000 000 Kč, která je udělována ve správním řízení NUKIB. Primárním požadavkem na systémy bezpečnostního monitoringu je zejména sběr a vyhodnocování informací o činnostech a událostech z integrovaných energetických systémů určených jako KII.

Pokud by se požadavky kladené na systémy bezpečnostního monitoringu významným způsobem lišily od byznys cílů organizace, je nutné provést revizi byznys strategie a cílů v souladu s požadavky kladenými na systémy bezpečnostního monitoringu.

8. krokem je prvotní abstraktní návrh systémů bezpečnostního monitoringu. Tento krok je zároveň posledním krokem fáze vize architektury bezpečnostního monitoringu. Výstup tohoto kroku zohledňuje výstupy ze všech předchozích kroků. Prvotní návrh bezpečnostního monitoringu musí zohlednit zejména identifikaci a analýzu současných bezpečnostních systémů, které společnost využívá pro bezpečnostní monitoring. Výstupem je seznam využívaných systémů. Seznam je nutné validovat a případně rozhodnout o nákupu nových bezpečnostních systémů a řešení. Součástí validace je i míra shody vlastností a funkcionalit systémů s legislativními požadavky na zaznamenávání činností a událostí. Dále je nezbytné kvalifikovaně rozhodnout o integraci energetických systémů do bezpečnostního monitoringu včetně úrovní, ze kterých budou zaznamenávány činnosti a události (technická aktiva, fyzický HW, virtualizační řešení, SCADA aplikace apod.). Identifikaci systémů a aplikací je vhodné realizovat prostřednictvím výstupů z analýzy rizik. V dalším kroku je nutné vytvořit model vzájemné komunikace a rozložení technických aktiv a aplikací energetických systémů s uvedením jejich geografického umístění. Dále je nutné rozšířit logický model o specifikaci vzájemné komunikace mezi energetickými systémy a systémy bezpečnostního monitoringu. Dále je nutné vytvořit rámcový implementační harmonogram. Legislativní požadavky týkající se hlášení kybernetických bezpečnostních incidentů musí být transformovány na operativní úroveň provozu kde ovlivňují požadavky na kapacitní plánování v oblasti personálního zajištění zaměstnanců, kteří vyhodnocují data systémů bezpečnostního monitoringu se současným zohledněním komunikačního plánu. Před ukončením tohoto kroku je nutné rovněž identifikovat možná rizika, která mají vazbu na návrh abstraktního modelu bezpečnostního monitoringu.

Výstupy:

- **Architektonická repozitoř –** za účelem centrálního umístění všech relevantních dokumentů je nutné vytvořit databázové nebo souborové uložiště, které bude využíváno po celou dobu návrhu architektury systémů bezpečnostního monitoringu. Forma a struktura architektonické repozitoře by měla reflektovat požadavky na repozitoř TOGAF.

- **Seznam zainteresovaných stran** – dokument obsahující osoby, role, povinnosti a odpovědnosti zainteresovaných stran.
- **Komunikační plán** – dokumentuje zainteresovaní strany, případně role a způsoby vzájemné komunikace.
- **Kapacitní plán** – dokumentuje požadavky na kapacity v oblasti lidských zdrojů a technologií.
- **Návrh abstraktního modelu bezpečnostního monitoringu** – návrh v dokumentovatelné formě, který obsahuje zejména:
    - Seznam současně využívaných systémů pro bezpečnostní monitoring včetně analýzy míry zajištění plnění legislativních požadavků.
    - Rozhodnutí o nutnosti nákupu nových monitorovacích systémů.
    - Abstraktní návrh integrace energetických systémů do bezpečnostního monitoringu.
    - Abstraktní komunikační model včetně návrhu vzájemné komunikace energetických a monitorovacích systémů.
    - Kapacitní a komunikační plán.
    - Rizika související s návrhem a implementací monitorovacích systémů.
    - Rámcový harmonogram implementace a rizika související s implementací na abstraktní úrovni.

7.4.3 Vazba na byznys architekturu

Cíle: Cílem této fáze je provést srovnání vytvořeného abstraktního modelu bezpečnostního monitoringu s byznys architekturou společnosti a zajištění jejich souladu. Byznys architektura definuje řízení společnosti na strategické, taktické a operativní úrovni, aby bylo dosaženo byznys cílů společnosti. Součástí strategické a taktické fáze jsou zejména byznys principy, pravidla a priority. Na operativní úrovni je byznys architektura tvořena procesy a službami, které byznys cíle podporují. Cíle musí odpovídat požadavkům na všech úrovních řízení. Soulad vize architektury bezpečnostního monitoringu s byznys architekturou je stěžejním výstupem této fáze. Stanovení souladu je nezbytné pro všechny úrovně řízení.

Požadavky byznys architektury, které se promítají do navrženého modelu bezpečnostního monitoringu jsou reprezentovány zejména finalizací požadavků kladených na bezpečnostní monitoring, identifikaci služeb, vytvoření byznys plánu apod.

Vstupy:

- **Výstupy přípravné fáze** – požadavky na zaznamenávání činností a událostí, interní dokumentace.
- **Výstupy fáze vize architektury bezpečnostního monitoringu** – architektonická repozitoř, zainteresované strany, komunikační plán, kapacitní plán, návrh abstraktního modelu bezpečnostního monitoringu.

Kroky:

Jak uvádí Soběslav (2012, s. 125), cílem je validovat vize a cíle, které mají vazbu na byznys principy, pravidla a priority na strategické a taktické úrovni a současně klíčové byznys procesy a funkce reprezentované ve formě byznys modelu architektury na operativní úrovni.

1. krokem je zajištění souladu s byznys požadavky společnosti na strategické a taktické úrovni (Desfray a Raymond, 2014, s. 155). Požadavky jsou reprezentovány prostřednictvím vizí a cílů. Soubor požadavků tvoří byznys strategii společnosti, která je reprezentovaná formalizovaným popisem. Klíčovým krokem je analýza vizí a cílů a zajištění souladu s požadavky na bezpečnostní monitoring. Byznys architektura zahrnuje zejména požadavky na zajištění efektivity při řešení bezpečnostních událostí a incidentů, zvýšení efektivnosti provozu systémů prostřednictvím proaktivního přístupu k monitoringu, efektivní způsob komunikace mezi zainteresovanými osobami a odděleními ve společnosti, efektivní způsob komunikace s externími autoritami, zajištění kontinuity činností v případě výskytu bezpečnostní události nebo incidentu. Výstupem této fáze je tedy zajištění souladu na strategické a taktické úrovni. Soulad je schválen vrcholovým vedením organizace a všemi zainteresovanými stranami.

2. krokem je zajištění souladu na operativní úrovni (Desfray a Raymond, 2014, s. 159–160). Na této úrovni je třeba zajistit soulad s byznys procesy a službami. Stejně jako v předchozím kroku, je i zde nutné mít k dispozici formalizovaný popis byznys procesů a služeb. V současné době existuje několik modelovacích jazyků, prostřednictvím kterých jsou byznys procesy vizualizovány a popsány. Mezi nejčastěji využívané patří BPM (bussiness proces

model), UML (unified modelling language), případně metoda implementovaná v rodině nástrojů ARIS.

BMP modeluje a vizualizuje procesy prostřednictvím notace BPMN (business proces model notation). Model je tvořen sítí aktivit (grafických objektů) a toků, které definují pořadí vykonávání aktivit.

UML umožňuje modelovat procesy prostřednictvím diagramů aktivit, který zobrazuje proces jako soubor aktivit a přechodů mezi aktivitami. Diagram aktivit současně zohledňuje zodpovědnosti za dané aktivity a současně prostředky, se kterými se v rámci aktivity pracuje. Metoda implementovaná v ARIS umožňuje modelovat organizační strukturu, procesy organizace a jejich vzájemné vztahy, cíle společnosti, struktury dat a aplikací. Stěžejní částí tohoto kroku je analýza a zajištění souladu pouze s procesy a službami, které jsou relevantní pro bezpečnostní monitoring.

Výstupem analýzy je seznam relevantních procesů a služeb ve formalizované podobě, které definují vazbu byznys architektury k bezpečnostnímu monitoringu. Součástí provedené analýzy je zohlednění následujících oblastí (Desfray a Raymond, 2014, s. 155–169):

- business proces flow diagram,
- business proces use-case diagram,
- business footprint diagram.

Soulad je schválen vrcholovým vedením organizace a všemi zainteresovanými stranami.

3. krokem je identifikace přístupu k budování systémů bezpečnostního monitoringu ve vztahu k byznysu. V tomto kroku je nutné zodpovědět otázku, zda společnost zajistí implementaci, správu a servis systémů bezpečnostního monitoringu prostřednictvím interních kapacit nebo využije externí dodavatele. Výběr vhodného přístupu je silně závislý na stávajících kapacitách společnosti, které jsou tvořeny kapacitním plánem vytvořeným v rámci fáze vize architektury. Nejdříve je nutné formálně popsat a analyzovat současný kapacitní plán. Výsledky analýzy slouží jako vstup pro rozhodnutí o míře zapojení externích dodavatelů. Nedílnou součástí rozhodování o zvoleném přístupu je i analýza finanční stránky při realizaci implementace, správy a zejména servisu systémů prostřednictvím interních vs. externích kapacit. Pokud se společnost rozhodne využít služby externích dodavatelů, je nezbytné zajistit vhodné nastavení metrik v obchodní rovině mezi společností a externím dodavatelem tak,

aby byla zajištěna adekvátní úroveň podpory pro dohodnuté služby, které externí dodavatel poskytuje. V obchodní rovině se v současné době nejčastěji využívají SLA. SLA popisují v obchodní rovině služby a definici kvalitativních a kvantitativních parametrů mezi společnostní a externím dodavatelem. SLA je vhodné stanovovat dle obecných pravidel a šablon, které udávají jejich obsah. Vhodným příkladem, který reflektuje pravidla a šablony je stanovení SLA dle rámce ITIL představeném v kapitole 4.2.1. Navržený přístup je schválen vrcholovým vedením organizace a všemi zainteresovanými stranami.

Výstupy:

- **Formalizovaný soulad s byznys architekturou –** schválený soulad navrženého abstraktního modelu bezpečnostního monitoringu s byznys architekturou na základě analyzované byznys strategie společnosti, byznys procesů a služeb.
- **Formalizovaný přístup k budování systémů bezpečnostního monitoringu** – stanovení přístupu k implementaci, správě a servisu systémů bezpečnostního monitoringu (interní kapacity, externí dodavatelé)

7.4.4 Vazba na architekturu IS

Cíle: cílem této fáze je stanovení souladu navrženého abstraktního modelu bezpečnostního monitoringu s datovou a aplikační architekturou společnosti. Datová architektura reflektuje zejména parametry zajištění dostupnosti, důvěrnosti a integrity dat po celou dobu jejich životního cyklu. Nezbytným krokem je také stanovení hodnoty dat z hlediska jejich důležitosti. Aplikační architektura reflektuje vzájemné vztahy mezi aplikacemi, komunikační matice a pravidla pro návrh jejich architektury, správu a servis. V tomto případě se jedná o vztah mezi aplikacemi pro řízení, správu a údržbu energetických systémů a systémy bezpečnostního monitoringu. Výstupem této fáze je schválení souladu s datovou a aplikační architekturou.

Vstupy:

- **Výstupy přípravné fáze** – požadavky na zaznamenávání činností a událostí, interní dokumentace.
- **Výstupy fáze vize architektury –** architektonická repozitoř, zainteresované strany, komunikační plán, kapacitní plán, návrh abstraktního modelu bezpečnostního monitoringu.

- **Výstupy fáze byznys architektury** – formalizovaný soulad s byznys architekturou, formalizovaný přístup k budování systémů bezpečnostního monitoringu.

- **Současná datová a aplikační architektura společnosti** – požadavky na práci s daty, životní cyklus dat, master data management, principy datové kvality a zajištění čistoty dat, požadavky na architekturu aplikací a jejich bezpečnost

Kroky:

1. krokem je stanovení souladu s datovou architekturou. Za tímto účelem je nezbytné provést analýzu současné datové architektury společnosti ve vztahu k návrhu systémů bezpečnostního monitoringu. Datová architektura se zabývá požadavky na strukturu dat na logické a fyzické úrovni včetně zdrojů pro řízení dat. Principy datové architektury jsou založeny na popisu datových sad, datových zdrojů, vazeb mezi nimi a současně vazeb na další relevantní prvky enterprise architektury (Chlapek, 2018, s. 10). Datová architektura obsahuje politiky, pravidla a normy, které definují způsoby a požadavky na shromažďování, ukládání, uspořádání, integraci, sdílení a využití dat v systémech společnosti. Aby bylo možné stanovit soulad navrženého řešení s datovou architekturou, musí být nejprve identifikována a popsána množina využívaných dat včetně jejich vzájemných vazeb. Za účelem dokumentování popisu dat a jejich vazeb je možné využít datových modelů (např. UML, DoDAF apod.) (Desfray a Raymond, 2014, s. 98). Prostřednictvím datových modelů lze zachytit datové entity a jejich vztahy, životní cyklus dat, migraci dat (datové toky) a bezpečnost dat (Desfray a Raymond, 2014, s. 188). Vstupem pro analýzu souladu jsou zejména stávající pravidla pro kategorizaci a práci s daty v rozsahu působnosti energetických systémů, resp. jejich technických aktiv, která využívají/zpracovávají a ukládají data. Kromě toho je třeba analyzovat stávající pravidla pro zajištění dostupnosti, důvěrnosti a integrity dat v kontextu pravidel datové architektury. Na základě těchto datových modelů je možné stanovit soulad navrženého řešení a datové architektury společnosti.

Požadavky datové architektury zejména v oblasti bezpečnosti dat tvoří nezbytný vstup do další fáze – návrhu technologického řešení. Bezpečnost dat je reflektována zejména při návrhu zasílání zpráv z transformovny/rozvodny/centrálního dispečinku do bezpečnostního monitoringu. Principy zajištění bezpečnosti komunikace reflektují zejména požadavky na zajištění důvěrnosti, dostupnosti, a především integrity zasílaných zpráv.

2. krokem je stanovení souladu s aplikační architekturou. Aplikační architektura je zaměřena na návrh aplikací, jejich interakcí a vazeb ve vztahu ke klíčovým byznys procesům za využití servisně orientovaného přístupu (Desfray a Raymond, 2014, s. 170). V tomto kroku je nezbytné analyzovat stávající aplikační řešení energetických systémů určených pro integraci do bezpečnostního monitoringu a na základě provedené analýzy identifikovat na abstraktní úrovni rizika a omezení jejich integrace ve vztahu k navrženému řešení. Rizika vychází zejména ze skutečnosti, že aplikace jsou specifické pro energetické systémy a jsou určeny pro OT prostředí. Velká množina aplikací jsou proprietární SCADA aplikace založené na specifických řídicích funkcích. Pro návrh bezpečnostního monitoringu je tedy nezbytné provést analýzu zaměřenou na identifikaci omezení integrace energetických systémů. Při analýze je vhodné se zaměřit na technická omezení, možnosti a požadavky jednotlivých řešení při předávání záznamů o činnostech a událostech do bezpečnostního monitoringu, která vzhledem ke své různorodosti a době poplatné jejich implementaci nemusí plnit všechny požadavky, které jsou na systémy kladeny.

Součástí provedené analýzy je zohlednění následujících oblastí (Desfray a Raymond, 2014, s. 169–186):

- diagram komunikace aplikací,
- diagram určení geografického umístění aplikací a uživatelů,
- use-case diagram systémů.

Na základě provedené analýzy je možné stanovit soulad s aplikační architekturou společnosti.

Výstupy:

- **Soulad s aplikační a datovou architekturou** – výstupem je analýza datové a aplikační architektury a jejich souladu s navrženým řešením bezpečnostního monitoringu.

7.4.5 Návrh technologického řešení bezpečnostního monitoringu

Cíle: hlavním cílem této fáze je vytvořit a formálně schválit návrh technologického řešení systémů bezpečnostního monitoringu společnosti. Vstupy této fáze jsou tvořeny výstupy všech předcházejících fází. Zde je vhodné zopakovat, že cílem fáze není stanovit přehled možných řešení systémů bezpečnostního monitoringu. Jak již bylo uvedeno v předchozí části práce, těchto systémů existuje v současné době celá řada. Navržená metodika má za cíl stanovit obecný přístup k budování systémů bezpečnostního monitoringu a není tedy závislá

na konkrétním využívaném technickém řešení. V této fázi je nutno řešit bezpečnost, resp. zaznamenávání činností a událostí na několika úrovních tak, aby byla respektována architektura energetických systémů. Jedná se o úrovně:

- Elektrická stanice/transformovna/rozvodna – ochrana lokálních řídicích systémů a aplikací a jejich integrace do bezpečnostního monitoringu.
- Komunikace z transformovny/rozvodny do bezpečnostního monitoringu – zajištění adekvátní úrovně ochrany komunikace z transformovny/rozvodny do bezpečnostního monitoringu.
- Centrální dispečink – ochrana systémů a aplikací a jejich integrace do bezpečnostního monitoringu.
- Systémy bezpečnostního monitoringu – bezpečnost ukládaných dat, zálohování, recovery plány, autentizace a autorizace uživatelů, reporting atd.

Výstupem je formální a schválený návrh technologického řešení systémů bezpečnostního monitoringu.

Vstupy:

- **Výstupy přípravné fáze** – požadavky na zaznamenávání činností a událostí, interní dokumentace.
- **Výstupy fáze vize architektury –** architektonická repozitoř, zainteresované strany, komunikační plán, kapacitní plán, návrh abstraktního modelu bezpečnostního monitoringu.
- **Výstupy fáze byznys architektury** – schválený soulad s byznys architekturou, formalizovaný přístup k budování systémů bezpečnostního monitoringu.
- **Výstupy fáze datové a aplikační architektury** – schválený soulad s datovou a aplikační architekturou společnosti.

1. krokem, který představuje kritický faktor úspěchu technologické realizace bezpečnostního monitoringu a bez kterého nelze monitoring efektivně realizovat je zajištění jednotného času v rámci energetických a bezpečnostních systémů. V důsledku nejednotnosti časových razítek se značně ztěžuje investigace při kybernetickém útoku. Nelze stanovit časovou návaznost

provedených aktivit, a tedy ani spouštěč a příčinu útoku. Prerekvizitou realizace dalších kroků je ověření jednotné časové synchronizace systémů a všech jejich aktiv. Uvedený krok není mandatorní. Vzhledem k iterativnímu přístupu metodiky může být tento krok vyžadován až v dalších krocích, případně fázích. Mandatorní se stává ve fázi realizace vzájemné integrace systémů, kdy je zajištění časové synchronizace nezbytné.

2. krokem je stanovení, resp. navržení zaznamenávání činností a událostí na úrovni každé transformovny/rozvodny a jejich integrace do systémů bezpečnostního monitoringu. Seznam systémů a aplikací je součástí analýzy rizik, která se tak stává základním zdrojem pro tento krok, protože dle ZoKB identifikuje aktiva, (SCADA, HMI, RTU, IED, komunikační prvky, prvky fyzické bezpečnosti apod.), která vyžadují určitou ochranu prostřednictvím implementace bezpečnostních opatření včetně zajištění bezpečnostního monitoringu. Pro účely metodiky SEC-MON je vhodné v tomto kroku reprezentovat výstupy z analýzy rizik prostřednictvím diagramu prostředí a geografického umístění systémů (environment and location diagram) v architektonické repozitoři.

Důležitou součástí tohoto kroku je detailní identifikace omezení zaznamenávání požadovaných činností a událostí na jednotlivých komponentách systémů a aplikací (zejména OT prvky a SCADA aplikace). Vstupem do uvedené analýzy je množina rizik, která byla identifikována při provedení analýzy souladu s aplikační architekturou. Analýza omezení musí zohlednit zejména požadovanou množinu zaznamenávaných činností a událostí systémů a aplikací ve vztahu k dokumentu požadavky na zaznamenávání činností a událostí, který byl výstupem přípravné fáze. Součástí analýzy je také identifikace komunikačních protokolů a omezení, které slouží pro předávání definované množiny dat do systémů bezpečnostního monitoringu. Pro detailní identifikaci omezení je nutné spolupracovat s interními administrátory energetických systémů, interních administrátorů IT infrastruktury nebo pověřených zaměstnanců externích dodavatelů, kteří disponují specifickými znalostmi o daných technologií a systémech. Spolupráce je realizována prostřednictvím schválených způsobů komunikace a komunikačního plánu.

Dále je nutno na základě vzájemné spolupráce identifikovat a zvolit vhodné technické řešení pro předávání zaznamenaných činností a událostí ze systémů a aplikací. Jedná se zejména o volbu řešení zasílání prostřednictvím Syslog, Syslog-ng, metalog, modular syslog nebo Rsyslog protokolu, využití SNMP trap, zaznamenávání formou Windows event logu nebo proprietárních řešení systémů/aplikací apod. Součástí navrženého řešení je také popis

a volba protokolu pro zasílání zpráv do systémů bezpečnostního monitoringu (TCP nebo UDP protokol) a dále specifikace fyzického komunikačního rozhraní, ze kterého budou zprávy odesílány.

3. krokem je zajištění bezpečnosti při zasílání zpráv z transformovny/rozvodny do bezpečnostního monitoringu. Principy zajištění bezpečnosti komunikace reflektují zejména požadavky na zajištění důvěrnosti, dostupnosti, a především integrity zasílaných zpráv. Návrh řešení musí vycházet z aktuálně využívaných/navrhovaných principů a vlastnických práv ke komunikační síti (propojení) mezi transformovnou/rozvodnou a systémy bezpečnostního monitoringu (vlastní infrastruktura, pronajímaná infrastruktura) při současném zohlednění bezpečnostních rizik, která souvisí s komunikační sítí.

Narušení integrity dat, např. prostřednictvím útoku typu man-in-the-middle, by mohlo vést k maskování kybernetického útoku cíleného na transformovnu/rozvodnu. Zprávy o provedených činnostech a událostech by mohli být modifikovány a podezřelé aktivity by nebyly dostupné v bezpečnostním monitoringu. Odhalení kybernetického útoku by v takovém případě bylo téměř nemožné. Ochrana integrity a zároveň důvěrnosti dat v rámci komunikační sítě zahrnuje řešení šifrování komunikace. Jedná se zejména o volbu využití end-to-end šifrování, případně šifrování pouze mezi výstupním komunikačním prvkem transformovny/rozvodny a vstupním komunikačním prvkem datového uzlu, ke kterému jsou připojeny systémy bezpečnostního monitoringu (IPSec tunely, šifrování prostřednictvím certifikátů apod.). End-to-end šifrování je silně závislé na technických omezeních a podpoře šifrovacích algoritmů ze strany koncových zařízení. Standardizovaným řešením pro zajištění dostupnosti je využití redundantních komunikačních prvků a záložních komunikačních linek.

4. krokem je stanovení, resp. navržení zaznamenávání činností a událostí na úrovni centrálního dispečinku a jejich integrace do systémů bezpečnostního monitoringu. Principy a realizace je totožná jako v případě druhého kroku, kdy byly tyto požadavky řešeny na úrovni transformoven/rozvoden.

5. krokem je zajištění bezpečnosti při zasílání zpráv z úrovně centrálního dispečinku do bezpečnostního monitoringu. Obecné principy a možnosti zabezpečení komunikací vychází ze stejných podmínek, které byly definovány pro úroveň transformoven/rozvoden v kroku 3.

6. krokem je stanovení kvalifikovaného odhadu na kapacitu uložiště bezpečnostního monitoringu. Tento krok představuje pravděpodobně nejtěžší část v této fázi a v praxi

je společnostmi velmi často opomíjen. Pokud se společnost nebude zabývat stanovením kvalifikovaného odhadu na kapacitu uložiště, resp. podcení požadavky na kapacitu, vystavuje se zvýšenému riziku ve formě nutnosti alokování velkých finančních prostředků v krátkém časovém období po implementaci systému. Pro efektivní stanovení odhadu je nezbytné zohlednit následující klíčové faktory:

- Legislativní požadavky – zákon o kybernetické bezpečnosti ukládá povinné osobě v oblasti energetiky ukládání záznamů o činnostech a událostech minimálně v délce 18 měsíců.
- Seznam a počet všech zařízení, resp. aktiv, která musí být integrována do systémů bezpečnostního monitoringu.
- Kvalifikovaný odhad průměrného množství záznamů, které jsou zařízeními generovány za časovou periodu. Důvodem je, že systémy bezpečnostního monitoringu jsou typicky licencovány na množství tzv. EPS (event per second), což je hodnota vyjadřující, kolik zpráv za sekundu jsou schopny přijmout a zpracovat.
- Technické řešení systémů bezpečnostního monitoringu a možnosti komprese dat a kompresních poměrů.

Kvalifikovaný odhad je vždy úzce spjatý s konkrétním technickým řešením systémů bezpečnostního monitoringu.

7. krokem je stanovení, volba a implementace bezpečnostních požadavků pro zajištění důvěrnosti, dostupnosti a integrity dat v systémech bezpečnostního monitoringu. Je nutné stanovit obecné principy a zvolit řešení pro zajištění:

- Bezpečnosti systému
    - Ochrana komunikačních sítí – je nutné definovat požadavky na segmentaci počítačové sítě ve vztahu k systémům bezpečnostního monitoringu. Segmentace sítě představuje efektivní nástroj pro řízení a kontrolu komunikací mezi systémy a aplikacemi. Řešení by mělo reflektovat obecné principy využívané v této oblasti. Typicky se jedná o nasazení síťových prvků typu firewall a řízení provozu prostřednictvím ACL.

- Návrh řešení zaznamenávání činností a událostí bezpečnostních systémů – legislativní požadavky na zaznamenávání činností a událostí je nezbytné aplikovat i na systémy zajišťující bezpečnostní monitoring. Zejména správci a dodavatelé, kteří jsou odpovědni za správu systémů a disponují administrátorskými oprávněními, představují zvýšené riziko. Rizikem je primárně možnost zavlečení úmyslné či neúmyslné chyby do systému. V extrémním případě může dojít k modifikaci nebo ztrátě dat, případně havárii systému jako celku a nutnosti jeho obnovy ze zálohy. Snížení hodnoty uvedeného rizika lze zajistit právě za využití principu zaznamenávání činností a událostí systémů bezpečnostního monitoringu a jeho uživatelů. V případě výskytu události či incidentu lze relativně snadno dohledat činnosti uživatelů a administrátorů.

- Bezpečnosti ukládaných dat

  - Návrh řešení fyzické bezpečnosti – na této úrovni je třeba definovat požadavky na fyzickou bezpečnost přístupu k datům, které musí reflektovat legislativní požadavky ZoKB.

  - Návrh ochrany před škodlivým kódem – je nutné zvolit a implementovat řešení ochrany před škodlivým kódem, které reflektuje legislativní požadavky, stejně jako v předchozím případě. Nástroj pro ochranu musí zajistit zejména ověření a kontrolu serverů a datových uložišť a pracovních stanic.

  - Návrh řešení důvěrnosti a integrity dat – je třeba implementovat mechanismy autentizace a autorizace přístupu k systémům bezpečnostního monitoringu a jejich dat s využitím principu nejnižších privilegií. Tento princip je založen na metodě přidělování autorizačních oprávnění, která jsou nejnižší možná pro zajištění správné funkcionality systému. Tímto principem je částečně eliminováno riziko úmyslné a neúmyslné chyby uživatele a správce systému, které by mohly nepříznivým způsobem ovlivnit systémy a data bezpečnostního monitoringu. Návrh je nutné formalizovat a schválit prostřednictvím zainteresovaných stran.

  - Zálohování – je nutné navrhnout řešení zálohování (systémy/data) a odpovídající frekvenci zálohování a typ (plné, rozdílové, přírůstkové zálohy).

Současně se zálohováním je třeba navrhnout plány obnovy systémů ze zálohy a disaster recovery plánů včetně jejich průběžného testování a ověřování účinnosti těchto opatření.

- Dostupnost a bezpečným přístup k systému
    - Návrh řešení vysoké dostupnosti systémů bezpečnostního monitoringu – je nutné navrhnou řešení na principu HA. Principy HA se uplatňují na aplikační úrovni, databázové úrovni, úrovni redundance síťové komunikace a úrovni redundance fyzického HW daného řešení. Vždy je nutné posoudit možnosti řešení vysoké dostupnosti nejprve na aplikační úrovni a v případě, že tato není podporována, postupovat k dalším úrovním, na kterých je možné HA využít.
    - Návrh řešení vzdáleného přístupu – pokud je zainteresovanými osobami požadováno zajištění vzdáleného přístupu k systémům bezpečnostního monitoringu je třeba navrhnout řešení vzdáleného přístupu. Řešení by mělo splňovat standardy a technologie, které jsou v současné době pro tento účel využívány. Typicky se jedná o nasazení technologie založené na VPN. Z bezpečnostního hlediska je nutno vzít na vědomí, že při realizaci VPN připojení se počítačová síť bezpečnostního monitoringu a připojeného klienta vzájemně propojí, což zvyšuje možnost kompromitace interní sítě prostřednictvím sítě klienta (stažení malware, ransomware apod.). U požadavků na vzdálené přístupy je vždy nutné zvážit bezpečnostní rizika. Pokud jsou požadavky zainteresovaných stran na vzdálený přístup opodstatněné, je vhodné realizovat tyto přístupy např. s využitím vzdálených ploch, vystavení klienta bezpečnostního monitoringu do DMZ, nahrávání session, zaznamenáváním činností a událostí dané komunikace apod.

Výstupy:

- **Návrh technologického řešení systémů bezpečnostního monitoringu** – požadavky na zajištění jednotného času integrovaných systémů, technologický návrh integrace transformoven/rozvoden, zajištění bezpečného přenosu dat do systémů bezpečnostního monitoringu, technologický návrh integrace centrálních dispečinků, stanovení požadavků na kapacitu diskových uložišť bezpečnostního monitoringu a současně

bezpečnostních požadavků pro zajištění dostupnosti, důvěrnosti a integrity dat, včetně realizace vzdáleného přístupu k systémům.

- **Schválené technologické řešení managementem** – stejně jako v předcházejících etapách je návrh technologického řešení schválen zainteresovanými stranami, ale v této fázi je klíčové i rozhodnutí managementu o realizovaném řešení.

7.4.6 Validace navrženého řešení

Cíle: navržený model bezpečnostního monitoringu je validován s požadovaným stavem. Požadovaný stav je identifikován požadavky byznys architektury, architektury IS a technologické architektury. Výstup fáze je tvořen finálním a zejména dokumentovatelným návrhem bezpečnostního monitoringu. Je nutné brát do úvahy technická omezení současně využívaných řešení (zastaralost systémů, technické omezení integrace apod.) Návrh musí být odsouhlasen vedením společnosti, které je vrcholově odpovědné za nasazení systémů bezpečnostního monitoringu, resp. zaznamenávání činností a událostí a současně vyhodnocování a hlášení bezpečnostních událostí a incidentů.

Vstupy:

- **Výstupy přípravné fáze** – požadavky na zaznamenávání činností a událostí, interní dokumentace.

- **Výstupy fáze vize architektury –** architektonická repozitoř, zainteresované strany, komunikační plán, kapacitní plán, návrh abstraktního modelu bezpečnostního monitoringu.

- **Výstupy fáze vazby na byznys architekturu** – schválený soulad s byznys architekturou, formalizovaný přístup k budování systémů bezpečnostního monitoringu.

- **Výstupy fáze vazby na datovou a aplikační architekturu** – schválený soulad s datovou a aplikační architekturou společnosti.

- **Výstupy fáze vazby na technologickou architekturu –** soulad datové a aplikační architektury společnosti s návrhem bezpečnostního monitoringu

Kroky:

1. krokem je validace stavu návrhu bezpečnostního monitoringu s požadavky byznys architektury, IS a technologické architektury. Zejména požadavky byznys a technologické architektury mohou mít rozsáhlý dopad na provoz energetických systémů. Nejprve je třeba popsat všechny rizika a dopady, které s sebou přináší jejich integrace do bezpečnostního monitoringu. Je nutné identifikovat rizika ve vztahu k zajištění normální funkce energetických systémů tak, aby jejich integrace do bezpečnostního monitoringu neovlivnila funkcionality a byla tak kontinuálně zajištěna služba dodávek elektrické energie, resp. byznys společnosti. Při určování rizik a jejich dopadů je nezbytné vytěžovat informace zejména od správců energetických systémů, kteří disponují detailní znalostí jejich fungování a jsou k jejich určení kompetentní na základě organizačního zařazení. Rizika a dopady musí být následně popsány formalizovaným způsobem. Cílem tohoto kroku je schválení rizik a dopadů všemi zainteresovanými stranami, aby bylo možné na ně adekvátním způsobem reagovat v dalších iteracích.

Validace souladu navrženého řešení s požadavky dílčích architektur reprezentovaných předcházejícími fázemi je poté řešena prostřednictvím diferenční (GAP) analýzy (Martinka, 2016, s. 21–22; Desfray a Raymond, 2014, s. 95). Podstatou diferenční analýzy je zjištění nedostatků, mezer nebo rozdílu mezi cílovým a aktuálním stavem. Výstup diferenční analýzy slouží jako podklad pro další iterace metodiky.

2. krokem je formulace strategie implementace a migrace bezpečnostního monitoringu na abstraktní úrovni. Úspěšnost implementace nového řešení, či přechod ze stávajícího na nové řešení je závislé na stanovení způsobu provedení migračního plánu. Migrační plán v detailu sestává z konkrétních kroků, které musí být provedeny spolu s uvedením zodpovědností za realizaci těchto kroků. Než bude možné přejít k definici konkrétních kroků migračního plánu a stanovení odpovědností, musí být na abstraktní úrovni identifikována rizika, časový horizont a stanoveny dílčí abstraktní cíle a milníky celého procesu migrace. Vytvoření migračního plánu na abstraktní úrovni blíže identifikuje možná rizika související s migrací, na která lze přijmout relevantní opatření a zohlednit je v návrhu bezpečnostního monitoringu.

Výstupy:

- **Identifikace rizik a dopadů navrženého řešení** – identifikace rizik a dopadů navrženého řešení a validace souladu s byznys, IS a technologické architektury.
- **Migrační plán na abstraktní úrovni** – identifikace použitých principů, milníků a rizik souvisejících s migrací.

7.4.7 Návrh migrace a zavedení governance

Cíle: Cílem fáze je rozpracování migračního plánu na abstraktní úrovni prostřednictvím detailnějšího popisu jednotlivých kroků, milníků a opatření k eliminaci identifikovaných rizik souvisejících s migrací. Implementace systémů bezpečnostního monitoringu je vzhledem k rozsáhlosti architektur energetických systémů komplexní záležitostí. Součástí fáze je popis harmonogramu napojení (integrace) energetických systémů do bezpečnostního monitoringu. Z tohoto důvodu je pro přechod k cílové architektuře vhodné využití metodik a principů, které se specializují na oblast projektového řízení a celý cyklus migrace řídit jako projekt dle zvoleného rámce procesního řízení**.**

Vstupy:

- **Výstupy přípravné fáze** – požadavky na zaznamenávání činností a událostí, interní dokumentace.
- **Výstupy fáze vize architektury –** architektonická repozitoř, zainteresované strany, komunikační plán, kapacitní plán, návrh abstraktního modelu bezpečnostního monitoringu.
- **Výstupy fáze vazby na byznys architekturu** – schválený soulad s byznys architekturou, formalizovaný přístup k budování systémů bezpečnostního monitoringu.
- **Výstupy fáze vazby na datovou a aplikační architekturu** – schválený soulad s datovou a aplikační architekturou společnosti.
- **Výstupy fáze vazby na technologickou architekturu –** soulad datové a aplikační architektury společnosti s návrhem bezpečnostního monitoringu.
- **Výstupy fáze identifikace příležitostí navrženého řešení** – Identifikace rizik a dopadů navrženého řešení, migrační plán na abstraktní úrovni.

1. krokem je stanovení míry zapojení projektového řízení do procesu implementace navrženého řešení bezpečnostního monitoringu. Důležitou předností při využití projektového řízení je dohled nad řízením projektu v rámci celého životního cyklu jeho implementace, kontrola termínů plnění dílčích úkolů a jednotlivých fází v rámci projektu. V současné praxi je zapojení projektového řízení nezbytnou součástí při implementaci rozsáhlých projektů. Nejprve je nutné analyzovat současné rámce projektového řízení, které společnost využívá. V dnešní době patří mezi nejčastěji využívané rámce projektového řízení PRINCE2 (project in controlled enviroments), CCPM (critical chain project management), EXP (extreme project management), PMBOOK (project management body of knowledge) apod. Rámce PRINCE2 a PMBOOK lze namapovat na rámec TOGAF či ITIL (Welcome to the TOGAF® Standard, Version 9.2, a standard of The Open Group (2018)). Po jejich identifikaci nastupuje krok, ve kterém jsou identifikovány a analyzovány již realizované a současné projekty, které mají vazbu na navržené řešení z hlediska časových a technických parametrů.

2. krokem je vytvoření detailního migračního plánu. Vstupem pro jeho vytvoření je zejména migrační plán na abstraktní úrovni, který byl vytvořen v předchozí fázi a obsahuje pouze obecné migrační postupy. Migrační plán zároveň zohledňuje požadavky ze všech předcházejících fází. V této fázi je nutné abstraktní migrační plán detailně rozpracovat do dílčích fází, kroků a činností spolu se stanovením detailního časového harmonogramu a konkrétní odpovědné osoby, která bude danou činnost realizovat. Provedení každé činnosti je nezbytné dokumentovat za účelem kontroly její realizace. Dílčí fáze, kroky a činnosti zahrnují zejména konfigurační úpravy v rámci HW prvků, komunikačních prvků, virtualizační řešení a aplikací energetických systémů pro integraci se systémy bezpečnostního monitoringu, tedy zasílání informací o činnostech a událostech. Dále implementace, případně úprava systémů bezpečnostního monitoringu, konfigurace autentizačních a autorizačních mechanismů uživatelů, nástrojů pro reportování, nastavení odesílání notifikací apod.

Pro stanovení harmonogramu implementace systémů bezpečnostního monitoringu a integrace energetických systémů lze využít informace z:

- Analýzy rizik – stanovení implementačního harmonogramu dle významnosti hodnoty rizik jednotlivých aktiv.
- Geografického umístění – postupná integrace systémů (celků nebo dílčích částí) v závislosti na geografickém umístění (lokalita centrálního dispečinku, transformovna/rozvodna).

- Obchodních smluv s dodavateli – postupná integrace energetických systémů jako celku v závislosti na dodavateli.

3. krok zahrnuje stanovení testovacího aparátu, požadavků a pravidel pro provádění testování navrženého řešení. Základem testovacího aparátu je výběr vhodných druhů testování – funkční/nefunkční/statické/dynamické/bezpečnostní apod.) (Felderer et al.., 2016; Oyetoyan, 201, s. 88–89). Po výběru relevantních druhů testování je nezbytné sestavit testovací plán. Jedná se o soubor informací, které reflektují zejména cíle a požadavky testování navrženého řešení, rozsah testování, typ testování, nástroje pro provádění testů, kritéria úspěšnosti testů, využití testovacího prostředí a testovacích dat, role a zodpovědnosti osob při testování apod.

Z hlediska obecných principů testování bezpečnostních systémů lze rozlišit dva relevantní druhy testování (Maraj et al., 2017; Felderer et al., 2018):

- Funkční – jedná se o testování navrženého řešení bezpečnostního monitoringu. Zahrnuje zejména oblasti testování odesílání definovaných typů činností a událostí z transformoven/rozvoden/centrálního dispečinku a ověření jejich doručení do systémů bezpečnostního monitoringu. Dále ověření nastavení korelačních pravidel, detekce false-positive a false-negative událostí a incidentů, vytváření reportů a analýza procesu eskalace detekovaných událostí/incidentů dle stanovených pravidel. Pravidla provádění testů musí reflektovat legislativní požadavky týkající se pravidel testování, oddělení produkčního, testovacího a vývojového prostředí apod. (zákon o kybernetické bezpečnosti, 2014).

- Bezpečnostní – oblasti bezpečnostního testování navržených systémů lze rozdělit na několik dílčích částí:

    - Skenování zranitelností – oblast zaměřená na identifikaci zranitelností a bezpečnostních slabin. Pro realizaci je často využíváno automatizovaných nástrojů a mezinárodně uznávaných standardů a metodik, např.:

        - OWASP (Open Web Application Security Project) – zaměření na oblast identifikace bezpečnostních hrozeb především mobilních a webových aplikací

- OSSTMM (Open Source Security Testing Methodology Manual) – metodika pro testování bezpečnosti
- CVE (Common Vulnerabilities and Exposures) – standardizovaný slovník obecných zranitelností a hrozeb, který je veřejně publikovaný
- CVSS (Common Vulnerability Scoring System) – slouží pro stanovení závažnosti dané zranitelnosti

o Penetrační testování – jedná se o formu bezpečnostního testování, které vycházejí z reálných technik, obecně používaných black-hat[14] hackery. Penetrační testování je založeno na principu reálné simulace zneužití zranitelností daných cílů z prostředí organizace (interní penetrační test) nebo za perimetrem organizace (externí penetrační test)

4. krokem je příprava zavedení dohledu nad implementací (zavedení governance). V rámci tohoto kroku jsou formulována doporučení pro pátý krok – implementace. Současně je zajištěn architektonický dohled připravované implementační fáze, jehož cílem je zajištění dohledu nad dodržováním termínů při realizaci dílčích fází, kroků a činností definovaných v migračním plánu. V rámci dohledu nad implementací musí být identifikována rizika související s realizací migračního plánu. U každého rizika musí být rozhodnuto o míře jeho závažnosti – (nevýznamné, akceptovatelné, nežádoucí, významné, nepřijatelné apod.) a u vybraných kategorií stanovit opatření pro snížení míry rizika. V oblasti zavedení dohledu nad implementací je možné využít mapování rámce TOGAF na rámce zaměřené na oblast IT Governance (např. COBIT).

5. krokem je realizace implementace navrženého řešení bezpečnostního monitoringu na základě detailního migračního plánu, který byl vytvořen ve druhém kroku. Po implementaci následuje funkční a bezpečnostní testování dle stanovených postupů definovaných ve třetím kroku.

[14] Dle výkladového slovníku kybernetické bezpečnosti je black-hat hacker (cracker) *„Jednotlivec, který se pokouší získat neoprávněný přístup k počítačovému systému. Tito jednotlivci jsou často škodliví a mají prostředky které mají k dispozici pro prolamovat se do systému.“*

Výstupy:

- **Stanovení míry zapojení projektového řízení** – identifikace a analýza rámců projektového řízení využívaného v rámci společnosti a stanovení míry jejich zapojení do fáze migrace navrženého řešení.

- **Vytvoření migračního plánu** – definice kroků a činností spolu se stanovením detailního časového harmonogramu a osob odpovědných za realizaci.

- **Stanovení testovacího aparátu –** sestavení testovacího plánu. Definice cílů a požadavků na testování navrženého řešení. Určení rozsahu a typu testování, nástrojů pro provádění testů, kritéria jejich úspěšnosti, definice rolí a zodpovědnosti osob.

- **Realizace implementace a testování** – implementace řešení dle migračního plánu. Testování implementovaného řešení na základě stanoveného testovacího aparátu.

7.4.8 Stanovení provozního modelu navrženého řešení

Cíle: součástí fáze je definice požadavků kladených na provoz systémů bezpečnostního monitoringu. Je nutné zejména vytvořit/upravit pravidla obsahující pokyny a postupy při vyhodnocování událostí, incidentů a problémů. Dále je nutné definovat pravomoci a odpovědnosti osob při správě a servisu systémů bezpečnostního monitoringu a integrovaných systémů ve vazbě na změnové řízení. Dalším cílem je vytvoření/úprava procesů týkající se eskalace událostí a incidentů na zainteresované strany a externí autority.

Vstupy:

- **Výstupy přípravné fáze** – požadavky na zaznamenávání činností a událostí, interní dokumentace

- **Výstupy fáze vize architektury –** architektonická repozitoř, zainteresované strany, komunikační plán, kapacitní plán, návrh abstraktního modelu bezpečnostního monitoringu.

- **Výstupy fáze vazby na byznys architekturu** – schválený soulad s byznys architekturou, formalizovaný přístup k budování systémů bezpečnostního monitoringu.

- **Výstupy fáze vazby na datovou a aplikační architekturu** – schválený soulad s datovou a aplikační architekturou společnosti.
- **Výstupy fáze vazby na technologickou architekturu –** soulad datové a aplikační architektury společnosti s návrhem bezpečnostního monitoringu.
- **Výstupy fáze identifikace příležitostí navrženého řešení** – identifikace rizik a dopadů navrženého řešení.
- **Výstupy fáze migrace a zavedení governance –** migrační plán, implementované řešení.

Kroky:

1. krokem je stanovení rolí a odpovědností pro vyhodnocování událostí a incidentů. V tomto kroku je nutné stanovit povinné role a jejich odpovědnosti v procesu vyhodnocování bezpečnostních událostí a incidentů. Určení povinných rolí a osob je založeno na výstupu z fáze vize architektury bezpečnostního monitoringu. Jedná se o formalizovaný dokument identifikující zainteresované strany a konkrétní osoby. V tomto kroku je nezbytné provést revizi zainteresovaných stran a stanovení jejich rolí a odpovědností v procesu managementu událostí a incidentů. Revidovaný dokument musí být formálně schválen vedením společnosti.

2. krokem je stanovení postupů monitorování a detekce bezpečnostních událostí a incidentů. Jedná se o stanovení požadavků a postupů pro detekci a sběr bezpečnostních incidentů a událostí je využití principu alarmů a korelace činností a událostí. Součástí je stanovení alarmových a korelačních pravidel, které fungují na principu analýzy činností a událostí. Návrh alarmů zahrnuje postupy a pravidla pro detekování odchylek a prahových hodnot od standardního stavu chování integrovaných systémů a formu jejich alarmování prostřednictvím systémů bezpečnostního monitoringu. Součástí návrhu je dále definice množiny pravidel a podmínek, které definují podezřelé aktivity, resp. bezpečnostní události. Principem návrhu korelací činností a událostí je vyhledávání množiny činností a událostí, které na základě společného prvku, kterým je nejčastěji společný atribut, tvoří komplexní informaci o bezpečnostní události a přispívá k výrazně lepší detekci bezpečnostních událostí.

3. krokem je stanovení postupů pro hlášení a evidenci bezpečnostních událostí a incidentů. Je nutné definovat jednotné kontaktní místo (místa), která budou sloužit jako centrální autorita pro hlášení a evidenci událostí a incidentů po celou dobu jejich životního cyklu.

Centrální evidence zajišťuje výrazné urychlení vytváření reportů, poskytování všech relevantních informací o událostech a incidentech apod. Současně je nutné definovat jednotnou formu (automatický záznam z bezpečnostních systémů, záznam zadaný uživatelem) a náležitosti hlášení tak, aby byly k dispozici relevantní informace související s hlášenou událostí nebo incidentem. Pro tento účel je vhodné využít rámců, které se specializují na operativní řízení IT služeb s důrazem na centrální evidenci prostřednictvím jednotného kontaktního místa. Vhodným rámcem je ITIL, resp. principy zajištění procesu incident managementu a využití service desku.

4. krokem je stanovení eskalačních mechanismů a postupů. Eskalační mechanismy jsou stanoveny za účelem rychlé a adekvátní reakce na bezpečnostní událost nebo incident. V této části je nutné zodpovědět otázku, zda-li společnost zajistí reakci na bezpečnostní incidenty pouze prostřednictvím interních kapacit nebo využije externí dodavatele. Pro stanovení kvalifikovaného rozhodnutí je nutné revidovat kapacitní a komunikační plán s důrazem na zajištění tohoto procesu. Využívání externích zdrojů souvisí zejména s poskytováním specifických služeb v oblasti incident response těmito organizacemi. Jedná se především o služby v rámci zajištění důkazních materiálů pro případné soudní spory, specifické služby v oblasti provádění forenzní analýzy apod. Nedílnou součástí stanovení eskalačních mechanismů je stanovení procesu hlášení kybernetických bezpečnostních incidentů na externí autority (NUKIB, CERT apod.)

5. krokem je stanovení postupů pro hlášení kybernetických bezpečnostních incidentů NUKIB. V tomto kroku je nutné identifikovat a jmenovat zainteresované strany, resp. konkrétní osoby, které mohou předávat hlášení o identifikovaném kybernetickém bezpečnostním incidentu prostřednictvím standardních komunikačních kanálů (elektronického formuláře zveřejněného na internetových stránkách NUKIB, emailu na adresu elektronické pošty NUKIB určené pro příjem hlášení kybernetických bezpečnostních incidentů, datové zprávy do datové schránky NUKIB, prostřednictvím určeného datového rozhraní, jehož popis je zveřejněn na internetových stránkách NUKIB, v listinné podobě na adresu Národního centra kybernetické bezpečnosti)

6. krokem je stanovení postupů pro zajištění reaktivních a ochranných opatření vydaných NUKIB. V tomto kroku je, stejně jako v předchozím, nutné identifikovat a jmenovat zainteresované strany, resp. konkrétní osoby, které jsou odpovědné za přijetí rozhodnutí NUKIB o vydaném varování a provedení reaktivních a ochranných opatření a současně

přezkoumání efektivnosti opatření. Odpovědné osoby musí být informovány o právech a povinnostech, které souvisí s přijetím, provedením a oznámením výsledku o provedení NUKIB. Práva a povinnosti jsou definovány v §4 a §33 VoKB.

7. krokem je stanovení postupů pro zajišťování důkazů. Pro zajištění nezpochybnitelnosti důkazů o průběhu události nebo incidentu musí být definovány náležitosti jejich evidence. Problematika zajištění důkazů pro trestní řízení týkající se vyšetřování událostí a incidentů je v současné sobě velice rozsáhlá a v právním řádu České republiky není k dispozici zcela jednoznačný právní výklad týkající se této problematiky. Obecná doporučení zahrnují poznatky z nejlepší praxe. Jedná se primárně o zajištění centrální evidence, kde jsou po celou dobu životního cyklu evidovány zejména následující informace o události nebo incidentu:

- datum a čas vzniku události/incidentu,
- subjekt, který zjistil, zaznamenal a nahlásil událost nebo incident,
- popis události nebo incidentu,
- identifikaci systémů, služeb, zainteresovaných stran apod.,
- identifikaci osoby, která provedla kategorizaci a klasifikaci události nebo incidentu,
- stav řešení události nebo incidentu, změny stavu řešení a odpovědných řešitelů.

8. krokem je stanovení postupů pro vyhodnocování událostí a incidentů. Jedná se o stanovení požadavků a postupů pro vyhodnocení (kybernetických) bezpečnostních událostí a incidentů. Návrh by měl zejména reflektovat oblasti:

- Kategorizace události nebo incidentu – pro určení významnosti je nutné stanovit postupy a definovat kategorie událostí a incidentů, které budou určovat míru jejich závažnosti. Definování kategorií musí zohlednit legislativní požadavky ZoKB, které definují kybernetickou bezpečnostní událost a kybernetický bezpečnostní incident. Kategorizace událostí a incidentů by měla zohlednit zejména kategorie: provozní události, bezpečnostní události, kybernetické bezpečnostní události, bezpečnostní incidenty a kybernetické bezpečnostní incidenty.

- Stanovení míry závažnosti (klasifikace) události nebo incidentu – je nutné stanovit míru závažnosti události a incidentu. V případě kybernetického bezpečnostního incidentu musí být stanovena míra závažnosti v souladu s platnou legislativou – §31 VoKB.

- Eskalace události nebo incidentu – řídí se eskalačními mechanismy definovanými v kroku 4.

- Řešení bezpečnostních událostí a incidentů a posuzování slabých míst v oblasti bezpečnosti informací – je nutné definovat postupy pro přiřazení události nebo incidentu řešiteli na základě jejich kategorizace a klasifikace. Řešitel disponuje pravomoc vzniklou situaci analyzovat a v případě potřeby eskalovat s cílem zajištění obnovy systému/aplikace/služby, jehož funkčnost byla vznikem události či incidentu omezena nebo narušena. V oblasti řešení bezpečnostních událostí a incidentů je možné využít standardizované rámce, které se specializují na operativní řízení IT služeb s důrazem na procesy řešení událostí a incidentů. Vhodným rámcem je ITIL, resp. principy zajištění procesů správy událostí, incidentů a správy aktiv. Tyto principy byly detailně představeny v kapitole 4.2.1 a proto zde nebudou opětovně popisovány.

- Hlášení kybernetických bezpečnostních incidentů NUKIB – řídí se postupy definovanými v kroku 5.

9. krokem je stanovení postupů pro operativní řízení změn v provozování systémů bezpečnostního monitoringu. Provoz bezpečnostního monitoringu s sebou přináší nutnost zajištění operativních konfiguračních změn. Změny se týkají zejména vytváření, úprav, případně rušení alarmových a korelačních pravidel, pravidel pro detekci bezpečnostních událostí, pravidel reportingu apod. Každá provedená úprava musí být zaznamenána a přezkoumávána. Požadavky na řízení změn musí být plně v souladu s §11 Řízení změn VoKB. Pro zajištění souladu společnosti při plnění §11 VoKB v oblasti řízení změn je nezbytné disponovat procesy a postupy pro zaznamenávání, prioritizaci, plánování, otestování, implementaci a dokumentaci požadavků na změny. Všechny požadavky na změny musí být evidovány prostřednictvím formálního návrhu provedení změny. Formální návrh obsahuje detailní popis navrhované změny a je zaznamenán papírovou nebo elektronickou formou. Stejně jako v oblasti řešení událostí a incidentů, je pro oblast řízení změn vhodné využít standardizované rámce, které se specializují na operativní řízení IT služeb s důrazem na proces řízení změn a jsou kompatibilní s TOGAF. Vhodným rámcem je ITIL, resp. principy zajištění procesů správy změn a s tím související proces správy aktiv.

10. krokem je stanovení návrhu postupů pro řešení problémů. Jedná se o stanovení procesu, který zodpovídá za správu problémů v rámci jejich životního cyklu. Problém vzniká jako příčina výskytu jednoho nebo kombinací více incidentů, kdy není v čase vytvoření problému známé řešení. V případě potřeby se v průběhu řešení problému vystavuje požadavek na změnu v rámci managementu změn. Spouštěčem procesu je jeden nebo kombinace více incidentů, kdy není známá příčina jejich výskytu. Pro zajištění procesu managementu problémů je vhodné využít rámců, které se specializují na operativní řízení IT služeb s důrazem na řešení problémů a jejich vazeb na řešení incidentů a změn. Vhodným rámcem je ITIL, resp. principy zajištění procesu managementu problémů, incidentů a změn.

Výstupy:

- **Stanovení rolí a odpovědností pro vyhodnocování událostí a incidentů** – identifikace povinných rolí a jejich odpovědnosti v procesu vyhodnocování bezpečnostních událostí a incidentů

- **Stanovení postupů v oblastech –** monitorování a detekce bezpečnostních událostí a incidentů, hlášení a evidenci bezpečnostních událostí a incidentů, eskalačních mechanismů, hlášení kybernetických bezpečnostních incidentů NUKIB, zajištění reaktivních a ochranných opatření vydaných NUKIB, zajišťování důkazů

7.4.9 Revize požadavků a řízení změn navrženého řešení

Hlavním cílem této fáze je revize souladu navrženého a implementovaného řešení s podnikovou architekturou organizace. Pomocí diferenční analýzy je stanoven soulad navržené architektury s byznys, aplikační, datovou a technologickou architekturou společnosti. Výstupem je hodnocení „zralosti“ architektury. Výstupem této fáze je zhodnocení současného stavu architektury monitorovacích systémů a vytvoření požadavků na optimalizaci a změny architektury.

1. krokem je validace stavu navržené architektury s enterprise architekturou společnosti v oblastech byznys architektury, datové a aplikační architektury. Vstupy jsou tvořeny popisem původní a současné byznys, aplikační a datové architektury. Pomocí diferenční analýzy je stanovena míra jejich souladu. Pro stanovení souladu jsou analyzovány požadavky na:

- výstupy ze systémů bezpečnostního monitoringu (počty, klasifikace, kategorizace událostí nebo incidentů),

- dokumentaci řešení událostí a incidentů,
- dokumentaci časů řešení událostí a incidentů,
- eskalační postupy,
- hlášení kybernetických bezpečnostních incidentů externím autoritám (NUKIB),
- metody zajišťování důkazů.

Výstup tohoto kroku je tvořen dokumentem, který stanovuje míru souladu výše uvedených oblastí s požadavky enterprise architektury v jednotlivých úrovních.

2. krokem je stanovení míry zralosti navrženého řešení bezpečnostního monitoringu. Je nutné určit vyspělost navrženého řešení a případně určit další fáze, které budou realizovány opětovnými iteracemi metodiky SEC-MON a jejich realizace zvýší vyspělost navrženého řešení. Určení vyspělosti bezpečnostního monitoringu lze realizovat prostřednictvím rámce SOC-CMM (security operation centre – capability & maturity model), který se zaměřuje na zhodnocení zajištění bezpečnostního monitoringu v následujících oblastech:

- Byznys – součásti byznysu (business drivers), soukromí (privacy) , governance.
- Lidé – zaměstnanci, role, hierarchie, školení, vzdělávání, znalosti.
- Procesy – security operation centre management, reporting, use-case management, provoz a řízení.
- Technologie – bezpečnostní analýza, automatizace a orchestrace, SIEM, IPS, IDS apod.
- Služby – bezpečnostní monitoring, bezpečnostní analýza, management činností a událostí, management zranitelností, management bezpečnostních událostí a incidentů, vyhledávání hrozeb.

Nejprve jsou ohodnoceny jednotlivé oblasti. Na základě jejich ohodnocení je možné stanovit celkovou míru vyspělosti bezpečnostního monitoringu, který tvoří stěžejní výstup tohoto kroku. Na základě stanovené míry vyspělosti lze určit relevantní fáze pro další iteraci metodiky k dosažení cílové vyspělosti navrženého řešení.

3. krokem je stanovení procesu řízení změn architektury bezpečnostního monitoringu. Pokud jsou v předchozích krocích identifikovány požadavky na změny architektury,

je nezbytné transformovat tyto požadavky do konkrétních změn a tyto změny realizovat prostřednictvím opětovného průchodu metodiky SEC-MON, resp. provedení další iterace ve fázích, které jsou touto změnou dotčeny. V případě, že je potvrzen soulad navrženého řešení s cílovou enterprise architekturou společnosti, není zapotřebí realizovat další iterace. Pokud navrhované změny výrazným způsobem zasahují do stávající architektury je možné rozhodnout o opětovném zahájení návrhu architektury bezpečnostního monitoringu. Důsledkem tohoto rozhodnutí je opětovné zahájení tvorby architektury dle metodiky SEC-MON prostřednictvím opětovného průchodu všemi fázemi metodiky. U každé požadované změny je nutné posoudit její dopady do všech úrovní enterprise architektury a současně stanovit režim její implementace.

Výstupy:

- **Stanovení souladu navržené architektury bezpečnostního monitoringu s enterprise architekturou společnosti** – identifikace souladu v oblastech byznys architektury, datové a aplikační architektury.
- **Stanovení zralosti navrženého řešení** – propojení s hodnotícím rámcem a stanovení vyspělosti navrženého řešení.
- **Stanovení procesu řízení změn** – stanovení mechanismu řízení a realizace změn navržené architektury.

8 OVĚŘENÍ A HODNOCENÍ METODIKY SEC-MON

Jak bylo řečeno v úvodu, autor této disertační práce aktuálně působí ve společnosti, která zajišťuje provozování distribuční soustavy na svěřeném území České republiky a je současně provozovatelem prvků kritické informační infrastruktury státu. Hlavní pracovní náplní autora je zajištění bezpečnostního dohledu těchto prvků včetně procesu návrhu a implementace bezpečnostních systémů. Hlavním faktorem a motivací pro vytvoření metodiky SEC-MON byla zejména absence metodiky v oblasti návrhu řešení bezpečnostního monitoringu. Vzhledem k aktuálnosti tématu a nutnosti řešení uvedené problematiky (viz kapitola 3).

Ověření a hodnocení navržené metodiky SEC-MON vychází tedy zejména z její existence. Metodika vychází z mezinárodně platného rámce TOGAF, jehož smyslem existence je systematická podpora pro řízení enterprise architektury v rámci společnosti nebo organizace. Stejně tak, i smyslem navržené metodiky SEC-MON je poskytnutí systematické podpory pro řízení zavádění bezpečnostních monitorovacích systémů v energetickém sektoru, které jsou specializovány na oblast zaznamenávání činností a událostí. Za tímto účelem využívá metodika v relevantní části propojení s projektovým managementem. Prostřednictvím projektového managementu lze zajistit soulad navrženého řešení a promítnutí požadavků do souvisejících projektů společnosti.

Velkou přidanou hodnotou navržené metodiky je rovněž zahrnutí provozního modelu vyhodnocování činností a událostí a tím zajištění adekvátní rychlé reakce na bezpečnostní události a incidenty. Za tímto účelem je metodika propojena v relevantních oblastech s rámci, které se specializují na operativní úroveň provozu navržených řešení, zejména rámcem ITIL.

Pro účely ověření a možnosti zhodnocení metodiky SEC-MON lze využít obecné principy ověřování metodik a hypotéz. Jedná se o ověření přímé a nepřímé. Nepřímé ověření je založeno na hodnocení vlastností a přístupů, které metodika přináší a současně hodnocení jejích přínosů. Přímé ověření je založeno na využití a míry implementace metodiky v projektech společností a organizací, které ji využívají.

8.1 Nepřímé ověření

Pokud se podíváme na základní vlastnosti a přístupy uplatněné v rámci metodiky SEC-MON, lze nepřímé ověření provést za pomoci následující množiny vlastností a přístupů.

8.1.1 Existence metodiky

Jak již bylo částečně řečeno v úvodu této kapitoly, stěžejním výstupem této disertační práce je vytvoření nové metodiky, která poskytuje systematickou podporu pro řízení návrhu a implementace monitorovacích systémů společnostem podnikajícím v energetickém sektoru, které provozují kritickou informační infrastrukturu. Implementace technických řešení bez zajištění systematického přístupu a propojení na úrovni celé společnosti není zárukou pro zajištění maximální efektivity a přínosů pro společnost. Metodika SEC-MON integruje proces návrhu a implementace technických řešení, které zajišťují bezpečnostní monitoring, s principy enterprise architektury. Tato integrace je založena na principu holistického přístupu k uvedené problematice jako celku. Využití uvedeného přístupu tvoří významný přínos metodiky SEC-MON. Je zajištěna integrace požadavků zainteresovaných strana požadavků na architektonické, byznys, datové a aplikační úrovni v celém procesu návrhu bezpečnostního monitoringu – viz kapitola 7. Stěžejním přínosem je tedy už samotné vytvoření a existence metodiky SEC-MON.

8.1.2 Založení na standardizovaném rámci

Přínosem metodiky SEC-MON je její založení na mezinárodně využívaném standardu TOGAF, který je zaměřen na oblast enterprise architektury. TOGAF patří v současné době mezi hojně využívaný koncept pro budování rozsáhlých podnikových architektur, jak bylo uvedeno v kapitole 5. Metodika SEC-MON využívá technik a nástrojů, které poskytuje TOGAF. V oblasti vize architektury se jedná zejména o využití principů Architecture Capability Frameworku (ACF), který obsahuje informace o organizaci, organizační struktuře, zavedených procesech, dovednostech, povinnostech a rolích osob, které jsou zainteresovány v procesu návrhu architektury energetických řídicích systémů a jejich vazbou na zajištění kybernetické bezpečnosti.

Metodika SEC-MON se dále výrazným způsobem soustředí na reflektování požadavků zainteresovaných stran v celém procesu návrhu architektury – viz kapitola 7.4.2. Tato vlastnost je plně kompatibilní s principy řízení požadavků v TOGAF a tvoří zásadní přínos navržené metodiky. Řízení požadavků v rámci celého životního cyklu návrhu architektury tvoří výraznou přidanou hodnotu metodiky SEC-MON, kdy je zajištěna rychlá a adekvátní reakce na změny a požadavky na architekturu.

Dalším důležitým přínosem navržené metodiky SEC-MON je její kompatibilita s modelovacími nástroji, které využívá TOGAF – viz kapitola 4.3.2.

8.1.3 Orientace na soulad s legislativními požadavky

Metodika SEC-MON je silně orientována na zajištění plnění legislativních požadavků daných ZoKB, které se týkají povinných osob, a to v celém procesu návrhu. Metodika reflektuje zajištění požadavků zejména v oblastech:

- Zapojení povinných rolí dle ZoKB – povinné role participují na celém procesu návrhu bezpečnostního monitoringu – viz kapitola 7.4.2.
- Zaznamenávání činností a událostí – metodika obsahuje souhrn doporučení pro zajištění jednotné evidence a všech náležitostí souvisejících s evidencí událostí a incidentů – viz kapitola 7.4.8
- Vyhodnocování událostí a incidentů – metodika obsahuje souhrn doporučení pro zajištění efektivního vyhodnocování událostí a incidentů. Pro účely vyhodnocování a eliminaci rizika nebezpečí z prodlení je využíváno konceptu eskalačních mechanismů – viz kapitola 7.4.8.
- Řízení změn a řízení aktiv – metodika reflektuje v procesu návrhu architektury a provozování daného řešení požadavky na řízení změn a řízení aktiv daného řešení, které jsou dány legislativními požadavky – viz kapitoly 7.4.8 a 7.4.9.
- Hlášení kybernetických bezpečnostních incidentů – metodika obsahuje souhrn doporučení pro zajištění hlášení kybernetických bezpečnostních incidentů na NUKIB. Tento přístup plně reflektuje v rámci návrhu řešení. Je tedy plně v souladu s plněním legislativních požadavků v této oblasti – viz kapitola 7.4.8.
- Reaktivní a ochranná opatření NUKIB – metodika obsahuje souhrn doporučení pro zajištění plnění reaktivních a ochranných opatření vydaných NUKIB. Tento přístup plně reflektuje v rámci návrhu řešení. Je tedy plně v souladu s plněním legislativních požadavků v této oblasti – viz kapitola 7.4.8.

V případě provedení legislativních změn požadavcích týkajících se zaznamenávání činností a událostí, jsou tyto požadavky jednoduše přenositelné do navrženého řešení prostřednictvím opětovné iterace metodiky SEC-MON (pokud dochází ke změně návrhu řešení jako celku) nebo průchodu pouze určitých fází metodiky. Totožný postup lze uplatnit v případě, že společnost bude reflektovat i další legislativní či normativní požadavky.

8.1.4 Nezávislost na konkrétním technickém řešení a výrobci

Metodika SEC-MON je zaměřena na systematickou podporu při návrhu řešení bezpečnostního monitoringu. Přínosem dané metodiky je rovněž její nezávislost na konkrétním řešení, výrobci nebo dodavateli bezpečnostních a monitorovacích systémů.

8.1.5 Orientace na procesní řízení a iterativní přístup

Metodika SEC-MON je založena na iterativním přístupu, který je uplatněn i v rámci TOGAF – viz kapitola 5.2. Iterativní přístup nachází využití i v dalších oblastech týkajících se informačních technologií, zejména v oblasti vývoji SW. Podstatou iterativního přístupu je opakování určitých fází za účelem dosažení očekávaného výsledku v krátkém časovém období. Přínosem využití iterativního přístupu v metodice SEC-MON je zejména zajištění kontinuálního přístupu k architektuře monitorovacích systémů.

Metodika jako celek, stejně jako každá fáze metodiky, je koncipována jako proces. Cílem tohoto přístupu je zajistit srozumitelnost a konkretizaci uvedených postupů. Každá fáze metodiky je charakterizována nezbytnou množinou vstupů, cíli, kroky a výstupy. Cíle definují v abstraktní rovině jednotlivé kroky, které jsou nezbytné pro úspěšný průchod dané fáze. Kroky představují množinu konkrétních činností, které je třeba provést, aby bylo dosaženo požadovaných cílů dané fáze. Výstupy jednotlivých fází tvoří ve většině případů nezbytné vstupy do dalších fází metodiky.

8.1.6 Nezávislost na konkrétním odvětví

Primárním zaměřením a přínosem metodiky SEC-MON je její orientace oblast návrhu bezpečnostního monitoringu v oblasti energetických systémů, které jsou určeny jako kritická informační infrastruktura. Sekundárně je metodika zaměřena na plnění souladu s legislativními požadavky v oblasti zaznamenávání činností a událostí. Vzhledem k faktu, že metodika vychází z obecného rámce pro řízení enterprise architektury TOGAF, je možné ji využít i v jiných průmyslových odvětvích, které se zabývají návrhem bezpečnostního monitoringu v kontextu enterprise architektury a mají povinnost plnit zejména legislativní požadavky dle ZoKB. Metodika je plně využitelná i v případě společností, které podléhají jiným legislativním požadavkům, než je ZoKB a VoKB. Legislativní a normativní požadavky lze v rámci metodiky SEC-MON jednoduše zohlednit v příslušných fázích, které se těmito požadavky zabývají. Metodika je tedy do jisté míry univerzální pro použití.

8.2 Přímé ověření

Přímé ověření metodiky je založeno na posouzení jejího využití a míry implementace v projektech společností nebo organizací. V současné době je metodika ověřována v rámci implementace projektů týkajících se nasazení monitorovacích systémů v energetické společnosti, která zajišťuje distribuci elektřiny na svěřeném území České republiky a je regulovaným subjektem dle ZoKB. Jedná se zejména o projekty „*Jednotný inteligentní bezpečnostní dohled systémů určených pro řízení distribuční soustavy*“ a „*Technologický SIEM*“. Na základě realizace těchto projektů dle metodiky SEC-MON bude možné relevantně vyhodnotit přínosy metodiky, případně navrhnout její dílčí úpravy.

Současně probíhá zahájení spolupráce na sdílení metodiky SEC-MON v rámci platformy ČSRES. Jedná se o platformu, která sdružuje regulované elektroenergetické společnosti v rámci České republiky (ČEPS, a. s.; ČEZ Distribuce, a. s.; E.ON Distribuce, a. s.; PRE Distribuce, a. s.). Metodika bude sdílena napříč všemi společnostmi, které jsou členy ČSRES. Výrazným přínosem sdílení metodiky je získání zpětné vazby z jejího používání v projektech jednotlivých společností týkajících se budování systémů bezpečnostního monitoringu v kontextu enterprise architektury. Cílem je získání větší množiny relevantních výstupů na základě kterých bude možné realizovat přímé zhodnocení metodiky SEC-MON.

Závěr

V současné době je spolehlivost dodávek elektrické energie klíčovým faktorem pro zajištění nejen sociálního, ale také ekonomického rozvoje jednotlivých národů. Spotřeba elektrické energie a ekonomický růst jsou dva faktory, které se v přímé úměře ovlivňují. Kritickým faktorem pro zajištění spolehlivosti je možnost řízení elektrizační soustavy prostřednictvím energetických řídicích systémů. Tyto systémy byly historicky koncipovány jako uzavřené systémy s důrazem na zajištění požadovaných funkcionalit řízení elektrizační soustavy. Nárůst kybernetických útoků, které byly v posledních několika letech zaměřeny právě na energetický sektor, vedl k nutnosti legislativní regulace subjektů v energetickém sektoru se zaměřením na zajištění bezpečnosti energetických řídicích systémů.

Legislativní regulace subjektů v energetickém sektoru s sebou přinesla mnoho výzev. Limitujícím faktorem je zejména zastaralost energetických systémů, které velice často nejsou schopny plně zajistit implementaci bezpečnostních požadavků na ně kladených a tedy být v souladu s požadavky platné legislativy.

Narušení bezpečnosti energetických systémů prostřednictvím kybernetických útoků má dopady zejména v ekonomické oblasti a představuje významné reputační riziko pro energetické subjekty. Za účelem plnění legislativních požadavků, snížení hrozby provedení kybernetického útoku a zajištění rychlé a adekvátní reakce na bezpečnostní incidenty, resp. kybernetické útoky, je nezbytné monitorovat činnosti a události v energetických systémech, které představují velmi významný zdroj informací.

Současné přístupy k zajištění monitorování činností a událostí zahrnují zejména technologický pohled na danou problematiku. Jedná se zejména o implementaci bezpečnostních systémů a řešení, které slouží jako datová platforma pro sběr činností a událostí. Samotné technologické řešení bez vazby na byznys, aplikační a datovou architekturu společnosti ale nezaručuje přidanou hodnotu pro společnost.

Hlavním cílem disertační práce bylo vytvoření nové metodiky, která by vytvořila průnik mezi specifickou oblastí problematiky bezpečnostních monitorovacích systémů sloužících pro zaznamenávání činností a událostí v energetických systémech a oblastmi návrhu a implementace rozsáhlých architektonických řešení, kterými se zabývá oblast enterprise architektury. Za účelem naplnění cíle práce bylo nutné představit a analyzovat oblast energetických systémů a možných přístupů k zajištění monitoringu činností a události

ve vztahu k plnění legislativních požadavků a možností propojení s principy a standardizovanými rámci enterprise architektury.

Stěžejním výstupem této práce je nově vytvořená metodika SEC-MON. Metodika SEC-MON je založena na rámci TOGAF, který v současné době tvoří jeden z nejpoužívanějších rámců pro oblast enterprise architektury. Rámec TOGAF byl vybrán na základě komparativní analýzy vybraných rámců enterprise architektury s přihlédnutím ke specifickým požadavkům energetických systémů.

V porovnání s jinými metodikami a obecnými rámci enterprise architektury aplikuje metodika SEC-MON holistický přístup k uvedené problematice. Metodika SEC-MON je současně silně orientována na zajištění plnění legislativních požadavků daných zákonem o kybernetické bezpečnosti v celém procesu návrhu. Metodika je založena na iterativním přístupu, který je uplatněn i v rámci TOGAFu. Podstatou iterativního přístupu v metodice SEC-MON je opakování určitých fází za účelem dosažení očekávaného výsledku v krátkém časovém období. Metodika jako celek, stejně jako každá fáze metodiky, je koncipována jako proces. Cílem tohoto přístupu je zajistit srozumitelnost a konkretizaci uvedených postupů. Každá fáze metodiky je charakterizována nezbytnou množinou vstupů, cíli, kroky a výstupy. Cíle definují v abstraktní rovině jednotlivé kroky, které jsou nezbytné pro úspěšný průchod dané fáze. Kroky představují množinu konkrétních činností, které je třeba provést, aby bylo dosaženo požadovaných cílů dané fáze. Výstupy jednotlivých fází tvoří ve většině případů nezbytné vstupy do dalších fází metodiky.

Motivací k vytvoření nové metodiky byly zejména praktické zkušenosti autora s implementací a správou systémů bezpečnostního monitoringu v rámci společnosti, která zajišťuje provozování distribuční soustavy na svěřeném území České republiky a je současně provozovatelem prvků kritické informační infrastruktury státu. Praktické zkušenosti autora potvrzují, že při implementaci těchto systémů je velmi často soustředěna pozornost pouze na technické řešení bez vazby na byznys, aplikační a datovou architekturu společnosti, která vytváří přidanou hodnotu pro společnost. Metodika SEC-MON pokrývá všechny uvedené oblasti a tím i standardizuje proces návrhu systémů bezpečnostního monitoringu. V současné době je metodika ověřována v projektech „*Jednotný inteligentní bezpečnostní dohled systémů určených pro řízení distribuční soustavy*“ a „*Technologický SIEM*“ společnosti ČEZ Distribuce, a. s. Současně probíhá zahájení spolupráce na sdílení metodiky SEC-MON v rámci platformy ČSRES. Jedná se o platformu, která sdružuje regulované elektroenergetické

společnosti v rámci České republiky (ČEPS, a. s.; ČEZ Distribuce, a. s.; E.ON Distribuce, a. s.; PRE Distribuce, a. s.). Metodika bude sdílena napříč všemi společnostmi, které jsou členy ČSRES. Výrazným přínosem sdílení metodiky je získání zpětné vazby z jejího používání v projektech jednotlivých společností týkajících se budování systémů bezpečnostního monitoringu v kontextu enterprise architektury. Cílem je získání větší množiny relevantních výstupů pro ověření metodiky SEC-MON.

Literatura

About Us - What We Do, 2019. *The Open Group* [online]. San Francisco: © 1995-2019 The Open Group. [cit. 2019-07-20]. Dostupné z: https://www.opengroup.org/about-us/what-we-do

A DNP3 Protocol Primer. DNP.org - Distributed Network Protocol [online]. California, 2005 [cit. 2018-02-07]. Dostupné z: https://www.dnp.org/AboutUs/DNP3%20Primer%20Rev%20A.pdf

ADEPU, S., MISHRA, G., MATHUR, A., 2017. Access control in water distribution networks: A case study, Proceedings - 2017 IEEE International Conference on Software Quality, Reliability and Security, QRS 2017, art. no. 8009922, pp. 184-191.

ALI, Ikbal a S.M. Suhail HUSSAIN, 2017. Control and management of distribution system with integrated DERs via IEC 61850 based communication. *Engineering Science and Technology, an International Journal* [online] 20(3), 956-964 [cit. 2018-02-17]. DOI: 10.1016/j.jestch.2016.11.017. ISSN 22150986. Dostupné z: http://linkinghub.elsevier.com/retrieve/pii/S2215098616307753

ALKHALDI, Firas M, Samir Marwan HAMMAMI a Mohammed AHMAR UDDIN, 2017. Understanding value characteristics toward a robust IT governance application in private organizations using COBIT framework. *International Journal of Engineering Business Management* [online]. **9** [cit. 2019-07-18]. DOI: 10.1177/1847979017703779. ISSN 1847-9790. Dostupné z: http://journals.sagepub.com/doi/10.1177/1847979017703779

ALVAREZ DE SOTOMAYOR, A., D. DELLA GIUSTINA, G. MASSA, A. DEDÈ, F. RAMOS a A. BARBATO, 2017. IEC 61850-based adaptive protection system for the MV distribution smart grid. *Sustainable Energy, Grids and Networks* [online]. [cit. 2018-01-28]. DOI: 10.1016/j.segan.2017.09.003. ISSN 23524677.

ANASTOPOULOS, Vasileios a Sokratis KATSIKAS, 2017. A structured methodology for deploying log management in WANs. *Journal of Information Security and Applications* [online]. 34, 120-132 [cit. 2018-05-02]. DOI: 10.1016/j.jisa.2017.02.004. ISSN 22142126.

ANCILLOTTI, Emilio, Raffaele BRUNO a Marco CONTI, 2013. The role of communication systems in smart grids: Architectures, technical solutions and research challenges. *Computer Communications*[online]. 2013, 36(17-18), 1665-1697 [cit. 2017-11-04]. DOI: 10.1016/j.comcom.2013.09.004. ISSN 01403664.

Architecture Development, 2019. *Chief Information Officer: U.S. Department of Defense* [online]. [cit. 2019-08-09]. Dostupné z: https://dodcio.defense.gov/Library/DoD-Architecture-Framework/dodaf20_arch_development/

BALDWIN, Sam, et al., 2015. Quadrennial Technology Review 2015: Chapter 3: Enabling Modernization of the Electric Power System. In: *Department of Energy* [online]. Washington, 2018, 2015 [cit. 2018-04-08]. Dostupné z: https://www.energy.gov/sites/prod/files/2015/09/f26/QTR2015-3A-Cyber-and-Physical-Security_0_0.pdf

BARAFORT, Béatrix, Antoni-Lluís MESQUIDA a Antonia MAS. Integrating risk management in IT settings from ISO standards and management systems perspectives [online]. 2017, 54, 176-185 [cit. 2020-07-01]. DOI: 10.1016/j.csi.2016.11.010. ISSN 09205489. Dostupné z: https://linkinghub.elsevier.com/retrieve/pii/S0920548916301866

BAYAT, Kamjoo. SCADA PROTOCOLS INTRODUCTION [online]. In: . 2017 [cit. 2018-03-29].

BEJŠOVEC, Lubomír. Tvorba a řízení změn architektury informačního systému [online]. 2010 [cit. 2020-07-01]. Dostupné z: <https://is.ambis.cz/th/vzib0/>. Diplomová práce. Vysoká škola regionálního rozvoje a Bankovní institut – AMBIS. Vedoucí práce Vlasta Svatá.

BENNET, Corry, 2015. Iranian hackers take credit for breaching New York dam. *The Hill* [online]. Washington D.C: Capitol hill publishing [cit. 2017-11-05]. Dostupné z: http://thehill.com/policy/national-security/264106-iranian-hackers-take-credit-for-cracking-new-york-dam

BERMUDEZ, Ignacio, Alok TONGAONKAR, Marios ILIOFOTOU, Marco MELLIA a Maurizio M. MUNAFÒ, 2016. Towards automatic protocol field inference. *Computer Communications* [online]. 84, 40-51 [cit. 2018-02-07]. DOI: 10.1016/j.comcom.2016.02.015. ISSN 01403664.

BITHAS, Kostas a Panos KALIMERIS, 2016. A Brief History of Energy Use in Human Societies. BITHAS, Kostas a Panos KALIMERIS. *Revisiting the Energy-Development Link* [online]. Cham: Springer International Publishing, s. 5-10 [cit. 2018-01-06]. SpringerBriefs in Economics. DOI: 10.1007/978-3-319-20732-2_2. ISBN 978-3-319-20731-5.

BONDAR, Sergej, John C. HSU, Alain PFOUGA a Josip STJEPANDIĆ, 2017. Agile digital transformation of System-of-Systems architecture models using Zachman framework. *Journal of Industrial Information Integration* [online]. **7**, 33-43 [cit. 2019-08-02]. DOI: 10.1016/j.jii.2017.03.001. ISSN 2452414X. Dostupné z: https://linkinghub.elsevier.com/retrieve/pii/S2452414X16301121

BOUŠKA, Jan, 2016. Historie výroby elektřiny. *Svaz podnikatelů pro využití energetických zdrojů, z.s*[online]. Praha. [cit. 2017-11-27]. Dostupné z: http://www.spvez.cz/pages/history/history_01.htm

BOYER, Stephen. Examining the cybersecurity landscape of utilities and control systems. *TechCrunch* [online]. New York City: Oath Tech Network, 2016 [cit. 2017-12-29]. Dostupné z: https://techcrunch.com/2016/06/17/examining-the-cybersecurity-landscape-of-utilities-and-control-systems/

BROAD, William J., John MARKOFF a David E. SANGER. Israeli Test on Worm Called Crucial in Iran Nuclear Delay [online]. In: . New York: New York Times, 2011 [cit. 2020-07-01]. Dostupné z: https://www.nytimes.com/2011/01/16/world/middleeast/16stuxnet.html

BRUNNER, CH. 2009, IEC 61850 – Introduction. 67s. Dostupné z WWW: < http://www.ieee.ch/assets/Uploads/pes/downloads/0904/09043iec61850.pdf >

BRYANT, Blake D. a Hossein SAIEDIAN, 2017. A novel kill-chain framework for remote security log analysis with SIEM software. *Computers & Security* [online]. 67, 198-210 [cit. 2019-06-20]. DOI: 10.1016/j.cose.2017.03.003. ISSN 01674048. Dostupné z: https://linkinghub.elsevier.com/retrieve/pii/S0167404817300561

CANTO, Carlos J. Del, Miguel A. PRADA, Juan J. FUERTES, Serafín ALONSO a Manuel DOMÍNGUEZ, 2015. Remote Laboratory for Cybersecurity of Industrial Control Systems. *IFAC-PapersOnLine* [online]. 48(29), 13-18 [cit. 2018-01-07]. DOI: 10.1016/j.ifacol.2015.11.206. ISSN 24058963.

CIP Standards, 2016. *NERC* [online]. Atlanta: North American Electric Reliability Corporation [cit. 2018-01-17]. Dostupné z: http://www.nerc.com/pa/Stand/Pages/CIPStandards.aspx

CONRAD, Eric; MISENAR, Seth; FELDMAN, Joshua. CISSP study guide. Newnes, 2012. ISBN 978-1-59749-961-3

CONTRIBUTORS, Previous, 2016. Industrial Control Systems: Next Frontier for Cyber Attacks? Https://www.tripwire.com [online]. Portland [cit. 2018-01-07]. Dostupné z: https://www.tripwire.com/state-of-security/featured/ics-next-frontier-for-cyber-attacks/

COOK, Allan, Helge JANICKE, Richard SMITH a Leandros MAGLARAS, 2017. The industrial control system cyber defence triage process. *Computers & Security* [online]. 70, 467-481 [cit. 2017-11-04]. DOI: 10.1016/j.cose.2017.07.009. ISSN 01674048.

CRATER, Kenneth C., a Craig E. GOLDMAN, 1998, "Distributed interface architecture for programmable industrial control systems." U.S. Patent No. 5,805,442.

CLEVELAND, Cutler J. a Christopher MORRIS, 2014. Electricity. *Handbook of Energy* [online]. Elsevier, s. 169-195 [cit. 2017-11-04]. DOI: 10.1016/B978-0-12-417013-1.00010-8. ISBN 9780124170131.

Cyber security solutions for critical infrastructure and industrial control systems, 2017. FireEye [online]. Milpitas: FireEye. [cit. 2018-01-07]. Dostupné z: https://www.fireeye.com/content/dam/fireeye-www/solutions/pdfs/pf/ms/sb-critical-infrastructure.pdf

ČAPEK, Jan, 2016. *Vytvoření modelu Enterprise Architektury podle rámce TOGAF*. Praha. Bakalářská práce. Vysoká škola ekonomická v Praze, Fakulta informatiky a statistiky. Vedoucí práce Prof. Ing. Petr Doucek, CSc.

ČEPS a.s. - O společnosti [online]. Praha: ČEPS a.s, 2017 [cit. 2017-11-04]. Dostupné z: https://www.ceps.cz/CZE/O-spolecnosti/Stranky/Default.aspx

Česko v datech, ©2016, Kybernetické útoky v energetice. *Česko v datech* [online]. Praha: Česko v datech [cit. 2017-11-05]. Dostupné z: http://www.ceskovdatech.cz/clanek/46-kyberneticke-utoky-v-energetice/

ČTK, 2020. Hlavní systémy OKD jsou už po hackerském útoku plně funkční. In: *ITBiz.cz* [online]. Praha: Nitemedia s.r.o. [cit. 2020-03-23]. Dostupné z: https://www.itbiz.cz/zpravicky/hlavni-systemy-okd-jsou-uz-po-hackerskem-utoku-plne-funkcni

DA SILVA, Lázaro Eduardo a Denis Vinicius COURY, 2016. *A new methodology for real-time detection of attacks in IEC 61850-based systems* [online]. [cit. 2018-02-17]. DOI: 10.1016/j.epsr.2016.08.022. ISBN 10.1016/j.epsr.2016.08.022. Dostupné z: http://linkinghub.elsevier.com/retrieve/pii/S0378779616303236

DAIRINRAM, Pavarit, Damras WONGSAWANG a Pagaporn PENGSART, 2016. SIEM with LSA technique for Threat identification. *In: 2013 19th IEEE International Conference on Networks (ICON)* [online]. IEEE, s. 1-6 [cit. 2019-06-25]. DOI: 10.1109/ICON.2013.6781951. ISBN 978-1-4799-2084-6. Dostupné z: http://ieeexplore.ieee.org/document/6781951/

DANG, D and PEKKOLA, S., 2017. "Systematic Literature Review on Enterprise Architecture in the Public Sector" In: *The Electronic Journal of e-Government*, Volume 15, Issue 2, (pp132-

154), Dostupné z: https://pdfs.semanticscholar.org/58b9/7d4e9d23e85826ab542b2405f4a43d962120.pdf

DE HAES, Steven, et al., 2013. *COBIT® 5: Enabling Information*. 1. Rolling Meadows, IL 60008 USA: © 2013 ISACA. ISBN 978-1-60420-350-9

DESFRAY, Philippe a Gilbert RAYMOND, 2014. *Modeling Enterprise Architecture with TOGAF®: A Practical Guide Using UML and BPMN*. Waltham: Elsevier. ISBN 978-0-12-419984-2

DETKEN, Kai-Oliver, Thomas RIX, Carsten KLEINER, Bastian HELLMANN a Leonard RENNERS, 2015. SIEM approach for a higher level of IT security in enterprise networks. *In: 2015 IEEE 8th International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS)* [online]. IEEE, s. 322-327 [cit. 2019-06-25]. DOI: 10.1109/IDAACS.2015.7340752. ISBN 978-1-4673-8359-2. Dostupné z: http://ieeexplore.ieee.org/document/7340752/

DEY, Arin, 2017. Enterprise Architecture & Frameworks -TOGAF, ITIL, COBIT, PMBOK. *Medium*[online]. San Francisco: Medium. [cit. 2019-07-20]. Dostupné z: https://medium.com/@arindey/enterprise-architecture-frameworks-togaf-itil-cobit-pmbok-88a3e4dca82c

DING, Derui, Qing-Long HAN, Yang XIANG, Xiaohua GE a Xian-Ming ZHANG, 2018. A survey on security control and attack detection for industrial cyber-physical systems. *Neurocomputing* [online]. 275, 1674-1683 [cit. 2018-03-04]. DOI: 10.1016/j.neucom.2017.10.009. ISSN 09252312.

DI SARNO, Cesario, Alessia GAROFALO, Ilaria MATTEUCCI a Marco VALLINI, 2016. A novel security information and event management system for enhancing cyber security in a hydroelectric dam. *International Journal of Critical Infrastructure Protection* [online]. 13, 39-51 [cit. 2018-03-04]. DOI: 10.1016/j.ijcip.2016.03.002. ISSN 18745482.

EDER-NEUHAUSER, Peter, Tanja ZSEBY, Joachim FABINI a Gernot VORMAYR, 2017. Cyber attack models for smart grid environments. Sustainable Energy*, Grids and Networks* [online]. 12, 10-29 [cit. 2018-01-07]. DOI: 10.1016/j.segan.2017.08.002. ISSN 23524677.

EJESH, Rejepova a Zhang ZHONGLIN, 2017. Safety of the SCADA Systems in Power Systems by Using Industry Protocols Data Communication. In: *2017 4th International Conference on Information Science and Control Engineering (ICISCE)* [online]. IEEE, s. 1705-1708 [cit. 2017-11-27]. DOI: 10.1109/ICISCE.2017.356. ISBN 978-1-5386-3013-6. Dostupné z: http://ieeexplore.ieee.org/document/8110583/

E.ON Česká republika, s.r.o, Přenosová a distribuční soustava 1. část - vedení velmi vysokého napětí (VVN), 2017. E.ON Distribuce[online]. České Budějovice: E.ON, [cit. 2017-10-22]. Dostupné z: https://www.eon-distribuce.cz/o-nas/novinky/media/prenosova-a-distribucni-soustava-elektricke-energie

ERTAUL, L. a HAO, J, 2011. Enterprise security planning with department of defense architecture framework (DODAF). In: *Proceedings of the International Conference on Security and Management (SAM)*. The Steering Committee of The World Congress in Computer Science, Computer Engineering and Applied Computing (WorldComp),

FAZLIDA, M.R. a Jamaliah SAID, 2015. Information Security: Risk, Governance and Implementation Setback. *Procedia Economics and Finance* [online]. **28**, 243-248 [cit. 2019-07-18]. DOI: 10.1016/S2212-5671(15)01106-5. ISSN 22125671. Dostupné z: https://linkinghub.elsevier.com/retrieve/pii/S2212567115011065

FELDERER, Michael, Matthias BÜCHLER, Martin JOHNS, Achim D. BRUCKER, Ruth BREU a Alexander PRETSCHNER., 2016. Security Testing. Elsevier, 2016. 1-51. Advances in Computers. DOI: 10.1016/bs.adcom.2015.11.003. ISBN 9780128051580. Dostupné také z: https://linkinghub.elsevier.com/retrieve/pii/S0065245815000649

FERNANDES, Fábio Alves, Guilherme Serpa SESTITO, André Luís DIAS, Dennis BRANDÃO a Paolo FERRARI, 2016. Influence of network parameters on the recovery time of a ring topology PROFINET network. *IFAC-PapersOnLine* [online]. 49(30), 278-283 [cit. 2018-02-17]. DOI: 10.1016/j.ifacol.2016.11.141. ISSN 24058963.

FERRUGENTO, Adriana a Álvaro ROCHA, 2015. Evolution of Methodological Proposals for the Development of Enterprise Architecture. *New Contributions in Information Systems and Technologies* [online]. Cham: Springer International Publishing, 2015, 2015, , 351-359 [cit. 2019-08-02]. Advances in Intelligent Systems and Computing. DOI: 10.1007/978-3-319-16486-1_35. ISBN 978-3-319-16485-4. Dostupné z: http://link.springer.com/10.1007/978-3-319-16486-1_35

FORGUE, Bruno a Pavel VLADYKA, 2010. IEC 61850: soubor norem pro komunikaci v energetice s velkým potenciálem výhod. *Automa* [online]. 8(3) [cit. 2018-01-28]. Dostupné z: http://automa.cz/Aton/FileRepository/pdf_articles/40771.pdf

GOLDMAN, Jeff. North Korea Blamed for Nuclear Power Plant Data Breach. In: *eSecurity Planet*[online]. Foster City: Quinstreet, 2015 [cit. 2017-11-04]. Dostupné z: https://www.esecurityplanet.com/network-security/north-korea-blamed-for-nuclear-power-plant-data-breach.html

GOVINDARASU, Manimaran, Adam HAHN a Peter SAUER, 2012, Cyber-Physical Systems Security for Smart Grid, Power Systems Engineering Research Center, February 2012.

HALAWI, Leila., MCCARTHY, Richard. a FARAH, James, 2019. Where We Are With Enterprise Architecture. Journal of Information Systems Applied Research, 12(3). Dostupné z: https://commons.erau.edu/publication/1234

HAMPTON, Robert, 2019. *About ISACA* [online]. s. 1-2 [cit. 2019-07-18]. Dostupné z: http://www.isaca.org/About-ISACA/Press-room/Documents/ISACA_Fact-Sheet_0119.pdf

HAN, Guozheng, Bingyin XU, Kaijun FAN a Guangxian LV, 2014. An open communication architecture for distribution automation based on IEC 61850. *International Journal of Electrical Power & Energy Systems [*online]. 54, 315-324 [cit. 2018-01-28]. DOI: 10.1016/j.ijepes.2013.07.013. ISSN 01420615.

HEATH, Robert L, 2013. *Encyclopedia of public relations*. 2nd edition. Thousand Oaks, California: SAGE Publications, 2013. ISBN 978-1-4522-4079-4.

HAVELKA, T, 2014. *Návrh komunikační struktury terminálu chránění a rozšiřujících periferii v řídicím systému*. Brno: Vysoké učení technické v Brně, Fakulta elektrotechniky a komunikačních technologií. Ústav mikroelektroniky. 47 s., 20 s. příloh. Bakalářská práce. Vedoucí práce: doc. Ing. Jiří Háze, Ph.D.

HÉGR, Tomáš, 2012. *Implementace a porovnání průmyslových protokolů v simulačním prostředí Omnet++* [online]. Praha. [cit. 2018-02-17]. Dostupné z: https://dip.felk.cvut.cz/browse/pdfcache/hegrtom1_2012dipl.pdf. Diplomová práce. České vysoké učení technické v Praze. Vedoucí práce Ing. Zbyněk Kocur.

HENNING, Carl, February 2nd, 2016. THE DIFFERENCE BETWEEN PROFIBUS AND PROFINET. *The worlds leading Industrial Ethernet Fieldbus* [online]. Scottsdale, ©2006-2018, [cit. 2018-02-17]. Dostupné z: http://us.profinet.com/the-difference-between-profibus-and-profinet/

HINKELMANN, Knut, Aurona GERBER, Dimitris KARAGIANNIS, Barbara THOENSSEN, Alta VAN DER MERWE a Robert WOITSCH, 2016. A new paradigm for the continuous alignment of business and IT: Combining enterprise architecture modelling and enterprise ontology. *Computers in Industry* [online]. **79**, 77-86 [cit. 2019-07-20]. DOI: 10.1016/j.compind.2015.07.009. ISSN 01663615. Dostupné z: https://linkinghub.elsevier.com/retrieve/pii/S0166361515300270

HIRSH, Richard F. a Christopher F. JONES, 2014. History's contributions to energy research and policy. *Energy Research & Social Science* [online]. 1, 106-111 [cit. 2018-01-06]. DOI: 10.1016/j.erss.2014.02.010. ISSN 22146296.

Historie českého elektrárenství, 2018. O společnosti | Skupina ČEZ [online]. Praha: ČEZ, [cit. 2018-01-06]. Dostupné z: https://www.cez.cz/cs/vyzkum-a-vzdelavani/pro-zajemce-o-informace/historie-a-soucasnost/historie-ceskeho-elektrarenstvi.html

Historie elektrifikace a vývoj elektrizační soustavy v čr, 2017. E.ON Distribuce [online]. České Budějovice, [cit. 2017-11-27]. Dostupné z: https://www.eon-distribuce.cz/o-nas/novinky/media/prenosova-a-distribucni-soustava-elektricke-energie

HOLLA, Abhiram, 2016. *Cyber Risk for Energy/Power Industry* [online]. In: . Aon Risk Solutions. [cit. 2017-12-29]. Dostupné z: http://www.aon.com/attachments/risk-services/cyber/Energy.pdf

HOLLOWAY, Michael, 2015. *Stuxnet Worm Attack on Iranian Nuclear* Facilities [online]. [cit. 2017-11-04]. Dostupné z: http://large.stanford.edu/courses/2015/ph241/holloway1/

HOLMES, J.F., G. RUSSELL a J.K. ALLEN, 2013. Supervisory Control and Data Acquisition (SCADA) and related systems for automated process control in the food industry: an introduction. *Robotics and Automation in the Food Industry* [online]. Elsevier, 2013, s. 130-142 [cit. 2018-05-02]. DOI: 10.1533/9780857095763.1.130. ISBN 9781845698010.

HONG, Junho a Chen-Ching LIU, 2017. Intelligent Electronic Devices with Collaborative Intrusion Detection Systems. *IEEE Transactions on Smart Grid* [online]. [cit. 2017-11-04]. DOI: 10.1109/TSG.2017.2737826. ISSN 1949-3053

HORÁLEK, Josef a Vladimír SOBĚSLAV, 2012. Technologie a požadavky na inteligentní sítě pro Smart Grid. *Elektrorevue* [online]. 13(6), 65-1 - 65-6 [cit. 2018-05-02]. ISSN 1213-1539. Dostupné z: http://elektrorevue.cz/cz/clanky/energetika--vykonova-elektronika--elektrotechnologie/25/technologie-a-pozadavky-na-inteligentni-site-pro-smart-grid/

HORYCH, V, 2009. *Analýza řídících protokolů využívaných v průmyslových aplikacích*.Brno: Vysoké učení technické v Brně, Fakulta elektrotechniky a komunikačních technologií. 49 s. Vedoucí diplomové práce Ing. Martin Koutný.

HOSSEINBEIG, S., D. KARIMZADGAN MOGHADAM, D. VAHDAT a R. ASKARI MOGHADAM, 2011. Combination of IT strategic alignment and IT governance to evaluate strategic alignment maturity. *2011 5th International Conference on Application of Information and Communication Technologies (AICT)* [online]. IEEE, 2011, 1-10 [cit. 2019-07-18]. DOI: 10.1109/ICAICT.2011.6110901. ISBN 978-1-61284-832-7. Dostupné z: http://ieeexplore.ieee.org/document/6110901/

HURST, Kyle B, 2017. *Applying the engineering systems multiple-domain matrix framework to nanosatellite space systems*. Massachusett. Disertační práce. Massachusetts Institute of Technology. Vedoucí práce Dr. Donna H. Rhodes.

CHERIFI, Tarek a Latifa HAMAMI, 2017. A practical implementation of unconditional security for the IEC 60780-5-101 SCADA protocol. *International Journal of Critical Infrastructure Protection* [online]. [cit. 2018-01-28]. DOI: 10.1016/j.ijcip.2017.12.001. ISSN 18745482.

CHLAPEK, Dušan, 2018. Přístupy ke správě dat v prostředí velké organizace. In: *Data a znalosti & WIKT 2018* [online]. Brno: Brno. [cit. 2020-03-20]. Dostupné z: http://daz2018.fit.vutbr.cz/data/08_01_chlapek_vse.pdf

IEC 61850 Substation Overview. *Moxa Inc.* [online]. California: Moxa, ©2018, 2018 [cit. 2018-02-17]. Dostupné z: https://www.moxa.com/doc/guidebooks/IEC_61850_Substation_Overview.pdf

IEC 60870-5-104 telegram structure. Beckhoff Information Systém, 2018 [online]. Verl. [cit. 2018-03-29]. Dostupné z: https://infosys.beckhoff.com/english.php?content=../content/1033/tf6500_tc3_iec60870_5_10x/984444939.html&id=

INNS, Jon. The evolution and application of SIEM systems, 2014. *Network Security* [online]. 2014(5), 16-17 [cit. 2019-06-20]. DOI: 10.1016/S1353-4858(14)70051-0. ISSN 13534858. Dostupné z: https://linkinghub.elsevier.com/retrieve/pii/S1353485814700510

JARMAKIEWICZ, Jacek, Krzysztof PAROBCZAK a Krzysztof MAŚLANKA, 2017. Cybersecurity protection for power grid control infrastructures. *International Journal of Critical Infrastructure Protection* [online]. 2017, 20-33 [cit. 2018-04-25]. DOI: 10.1016/j.ijcip.2017.07.002. ISSN 18745482.

JIRÁSEK, Petr, Luděk NOVÁK a Josef POŽÁR, 2013. *Výkladový slovník kybernetické bezpečnosti: Cyber security glossary.* 2., aktualiz. vyd. Praha: Policejní akademie ČR v Praze. ISBN 978-80-7251-397-0.

KABOVIC, Anka V., Milenko M. KABOVIC a Vladimir V. CELEBIC, 2014. Software realization for the communication according to the IEC61850 standard on the nanoRISC MSC hardware platform. In: *2014 22nd Telecommunications Forum Telfor (TELFOR)* [online]. IEEE, 2014, s. 423-426 [cit. 2018-02-17]. DOI: 10.1109/TELFOR.2014.7034438. ISBN 978-1-4799-6191-7. Dostupné z: http://ieeexplore.ieee.org/document/7034438/

KANG, D.J., J.J. LEE, B.H. KIM a D. HUR, 2009. Proposal strategies of key management for data encryption in SCADA network of electric power systems. *International Journal of Electrical Power & Energy Systems*[online]. [cit. 2017-11-04]. DOI: 10.1016/j.ijepes.2009.03.004. ISSN 01420615.

KNAPP, Eric a James BROAD. 2011 *Industrial Network Security Securing Critical Infrastructure Networks for Smart Grid, SCADA, and Other Industrial Control Systems*. Burlington: Elsevier Science. ISBN 9781597496469.

KNAPP, Eric D. a Joel Thomas LANGILL, 2015. Standards and Regulations. *Industrial Network Security* [online]. Elsevier, 2015, s. 387-407 [cit. 2018-01-17]. DOI: 10.1016/B978-0-12-420114-9.00013-7. ISBN 9780124201149.

KANG, D.J., J.J. LEE, B.H. KIM a D. HUR, 2009. Proposal strategies of key management for data encryption in SCADA network of electric power systems. *International Journal of Electrical Power & Energy Systems*[online]. [cit. 2017-11-04]. DOI: 10.1016/j.ijepes.2009.03.004. ISSN 01420615.

KEARNY, Carike, Aurona GERBER a Alta VAN DER MERWE, 2016. Data-driven enterprise architecture and the TOGAF ADM phases. *2016 IEEE International Conference on Systems, Man, and Cybernetics (SMC)* [online]. IEEE, 2016, 004603-004608 [cit. 2019-07-21]. DOI: 10.1109/SMC.2016.7844957. ISBN 978-1-5090-1897-0. Dostupné z: http://ieeexplore.ieee.org/document/7844957/

KEZUNOVIC, M, 2011. Integration of Substation Data. *IFAC Proceedings Volumes* [online].44(1), 12861-12866 [cit. 2017-10-08]. DOI: 10.3182/20110828-6-IT-1002.02654. ISSN 14746670.

KOTÁL, Tomáš. *Moderní komunikace protokolem IEC61850* [online]. Paha, 2009 [cit. 2018-03-15]. Dostupné z: https://dip.felk.cvut.cz/browse/pdfcache/kotalt1_2009dipl.pdf. Diplomová práce. České vysoké učení technické v Praze. Vedoucí práce Ing. David Řehoř.

KOVANIČOVÁ, Eva, 2019. Benešovská nemocnice po kyberútoku obnovila provoz Zdroj: https://benesovsky.denik.cz/zpravy_region/benesovska-nemocnice-jiz-pracuje-v-normalnim-rezimu-20191230.html. In: *Benešovský deník* [online]. Benešov u Prahy: ©VLTAVA LABE MEDIA a.s [cit. 2020-03-23]. Dostupné z: https://benesovsky.denik.cz/zpravy_region/benesovska-nemocnice-jiz-pracuje-v-normalnim-rezimu-20191230.html

KRYŠTŮFEK, Jan, 2001. Profibus - Technický popis - Přehled. ČVUT Fakulta strojní [online]. Praha, ©2014-2018 [cit. 2018-02-17]. Dostupné z: http://www1.fs.cvut.cz/cz/u12110/site/profibus/

LAINHART, John W, et al, 2012. *COBIT® 5: Enabling Processes*. 1. Rolling Meadows, IL 60008 USA: © 2012 ISACA. ISBN 978-1-60420-241-0.

LAPALME, James, Aurona GERBER, Alta VAN DER MERWE, John ZACHMAN, Marne De VRIES a Knut HINKELMANN, 2016. Exploring the future of enterprise architecture: A Zachman perspective. *Computers in Industry* [online].**79**, 103-113 [cit. 2019-07-20]. DOI: 10.1016/j.compind.2015.06.010. ISSN 01663615. Dostupné z: https://linkinghub.elsevier.com/retrieve/pii/S0166361515300166

LEE, Robert M., Michael J. ASSANTE a Tim CONWAY. Analysis of the Cyber Attack on the Ukrainian Power Grid. *NERC* [online]. 2016 [cit. 2017-11-05]. Dostupné z: http://www.nerc.com/pa/ci/esisac/documents/e-isac_sans_ukraine_duc_18mar2016.pdf

LIM, Il-Hyung a Tarlochan S. SIDHU, 2016. A new local backup scheme considering simultaneous faults of protection IEDs in an IEC 61850-based substation. *International Journal of Electrical Power & Energy Systems* [online].77, 151-157 [cit. 2017-11-04]. DOI: 10.1016/j.ijepes.2015.11.024. ISSN 01420615.

LESZCZYNA, Rafał, 2018. Cybersecurity and privacy in standards for smart grids – A comprehensive survey. *Computer Standards & Interfaces* [online]. 56, 62-73 [cit. 2018-04-25]. DOI: 10.1016/j.csi.2017.09.005. ISSN 09205489.

MADANI, Afsaneh, Saed REZAYI a Hossein GHARAEE, 2011. Log management comprehensive architecture in Security Operation Center (SOC*). In: 2011 International Conference on Computational Aspects of Social Networks (CASoN)* [online]. IEEE, 2011, s. 284-289 [cit. 2019-06-20]. DOI: 10.1109/CASON.2011.6085959. ISBN 978-1-4577-1133-6. Dostupné z: http://ieeexplore.ieee.org/document/6085959/

MACKIEWICZ, R.E, 2006. Overview of IEC 61850 and Benefits. In: *2006 IEEE PES Power Systems Conference and Exposition* [online]. IEEE, 2006, s. 623-630 [cit. 2018-02-24]. DOI: 10.1109/PSCE.2006.296392. ISBN 1-4244-0177-1

MACAULAY, Tyson a Bryan L. SINGER. Cybersecurity for Industrial Control Systems [online]. 2016-4-19 [cit. 2020-07-01]. DOI: 10.1201/b11352.

MAGDOŇOVÁ, Jana, 2020. Na nemocnici v Benešově útočil ruský virus Ryuk. Jermanová odmítá, že by někdo požadoval výkupné. In: *IRozhlas* [online]. Praha: ©1997-2020 Český rozhlas. [cit. 2020-03-23]. Dostupné z: https://www.irozhlas.cz/zpravy-domov/nemocnice-benesov-kyberneticky-utok-ransomware-vykupne-ochrana-osobnich-udaju_2001140615_cha

Magic Quadrant for Enterprise Architecture Tools, 2019. Gartner, Inc. *Gartner* [online]. [cit. 2020-03-20]. Dostupné z: https://www.gartner.com/en/documents/3970555/magic-quadrant-for-enterprise-architecture-tools

Magic Quadrant for Security Information and Event Management, 2018. Gartner, Inc. *Gartner* [online]. [cit. 2019-10-20]. Dostupné z: https://www.gartner.com/en/documents/3894573/magic-quadrant-for-security-information-and-event-manage

MAGLARAS, Leandros A., Ki-Hyung KIM, Helge JANICKE, Mohamed Amine FERRAG, Stylianos RALLIS, Pavlina FRAGKOU, Athanasios MAGLARAS a Tiago J. CRUZ, 2018. Cyber security of critical infrastructures. *ICT Express* [online].[cit. 2018-03-04]. DOI: 10.1016/j.icte.2018.02.001. ISSN 24059595.

MARAJ, Arianit, Genc JAKUPI, Ermir ROGOVA a Xheladin GRAJQEVCI, 2017. Testing of network security systems through DoS attacks. 6th Mediterranean Conference on Embedded Computing (MECO). IEEE, 2017, 2017, , 1-6. DOI: 10.1109/MECO.2017.7977239. ISBN 978-1-5090-6742-8. Dostupné z: http://ieeexplore.ieee.org/document/7977239/

MASUDA, Yoshimasa; SHIRASAKA, Seiko a YAMAMOTO, Shuichiro, 2016. Integrating Mobile IT/Cloud into Enterprise Architecture: a Comparative Analysis. In: *PACIS*..

MATOUŠEK Petr. Description and analysis of IEC 104 Protocol. FIT-TR-2017-12, Brno: Fakulta informačních technologií VUT v Brně, 2017.

MENGES, F., BÖHM, F., VIELBERTH, M., PUCHTA, A., TAUBMANN, B., RAKOTONDRAVONY, N., a LATZO, T, 2018. Introducing DINGfest: An architecture for next generation SIEM systems.[online],[cit. 2017-11-04]

MISSION SUPPORT CENTER, 2016. *Cyber Threat and Vulnerability Analysis of the U.S. Electric Sector* [online]. [cit. 2017-12-28]. Dostupné z: https://energy.gov/sites/prod/files/2017/01/f34/Cyber%20Threat%20and%20Vulnerability%20Analysis%20of%20the%20U.S.%20Electric%20Sector.pdf

MOD Architecture Framework - GOV.UK, 2012 [online]. Londýn: Ministry of Defence, [cit. 2019-09-09]. Dostupné z: https://www.gov.uk/guidance/mod-architecture-framework

MODBUS APPLICATION PROTOCOL SPECIFICATION V1.1b, 2006. *The Modbus Organization* [online]. Hopkinton: Modbus Organization [cit. 2018-02-17]. Dostupné z: http://www.modbus.org/docs/Modbus_Application_Protocol_V1_1b.pdf

Modbus TCP/IP, 2017. *Simply Modbus: Data Communication Test Software* [online]. Simply Modbus [cit. 2018-02-17]. Dostupné z: http://www.simplymodbus.ca/TCP.htm

MODBUS TUTORIAL FOR ARDUINO, RASPBERRY PI AND INTEL GALILEO. *Cooking Hacks - Electronic and IoT Kits, tutorials and guides for Makers and Education, 2016* [online]. Libelium Comunicaciones Distribuidas S.L [cit. 2018-02-17]. Dostupné z: https://www.cooking-hacks.com/documentation/tutorials/modbus-module-shield-tutorial-for-arduino-raspberry-pi-intel-galileo/

MOLNÁR, Zdeněk, 2012. *Pokročilé metody vědecké práce* [online]. Zeleneč: Profess Consulting, [cit. 2020-01-30]. Věda pro praxi (Profess Consulting). ISBN 978-80-7259-064-3.

MOOSDIJK, Jarno a Daan WAGENAAR, 2015. *Addressing SIEM* [online]. [cit. 2019-05-21]. Dostupné z: http://www.vurore.nl/images/vurore/downloads/scripties/2030-Def-scriptie-Jarno-van-de-Moosdijk---daan-Wagenaar.pdf

MOREIRA, Naiara, Elías MOLINA, Jesús LÁZARO, Eduardo JACOB a Armando ASTARLOA, 2016. Cyber-security in substation automation systems. *Renewable and Sustainable Energy Reviews* [online]., 54, 1552-1562 [cit. 2017-11-04]. DOI: 10.1016/j.rser.2015.10.124. ISSN 13640321.

NAZIR, Sajid, Shushma PATEL a Dilip PATEL, 2017. Assessing and augmenting SCADA cyber security: A survey of techniques. *Computers & Security* [online]. 70, 436-454 [cit. 2018-01-28]. DOI: 10.1016/j.cose.2017.06.010. ISSN 01674048.

NEERAJA T.P., SIVRAJ P. a SASI K.K, 2015. Sensor Based Communication Network for WACS with DNP3. *Procedia Technology* [online]. 21, 76-81 [cit. 2018-02-23]. DOI: 10.1016/j.protcy.2015.10.012. ISSN 22120173.

NEITZEL, Lee a Bob HUBA, 2014. Top ten differences between ICS and IT cybersecurity. *InTech Magazine* [online]. 15(3) [cit. 2018-01-07]. Dostupné z: https://www.isa.org/standards-and-publications/isa-publications/intech-magazine/2014/may-jun/features/cover-story-top-ten-differences-between-ics-and-it-cybersecurity/

NERC, 2016 [online]. Atlanta: North American Electric Reliability Corporation, 2016 [cit. 2018-01-17]. Dostupné z: http://www.nerc.com/Pages/default.aspx

NETWRIX CORPORATION, 2017. *2016 SIEM Efficiency Surwey* [online]. Irwine. [cit. 2019-05-21]. Dostupné z: https://www.netwrix.com/2016_siem_efficiency_survey_report.html

NEZAMODDINI, Nasim, Seyedamirabbas MOUSAVIAN a Melike EROL-KANTARCI, 2017. A risk optimization model for enhanced power grid resilience against physical attacks. *Electric Power Systems Research* [online]. 143, 329-338 [cit. 2017-12-29]. DOI: 10.1016/j.epsr.2016.08.046. ISSN 03787796. Dostupné z: http://linkinghub.elsevier.com/retrieve/pii/S0378779616303546

NIKPAY, Fatemeh, Rodina Binti AHMAD, Babak Darvish ROUHANI, Mohd Naz'ri MAHRIN a Shahaboddin SHAMSHIRBAND, 2017. An effective Enterprise Architecture Implementation Methodology. *Information Systems and e-Business Management* [online]. **15**(4), 927-962 [cit. 2019-08-02]. DOI: 10.1007/s10257-016-0336-5. ISSN 1617-9846. Dostupné z: http://link.springer.com/10.1007/s10257-016-0336-5

OCHRANA, František, 2019. *Metodologie, metody a metodika vědeckého výzkumu*. Praha: Univerzita Karlova, nakladatelství Karolinum. ISBN 978-80-246-4200-0.

OKHRIMENKO, Anastasiia 2017. *Comparing Enterprise Architecture Frameworks – A Case Study at the Estonian Rescue Board*. Tartu. Diplomová práce. Institute of Computer Science Software Engineering Curriculum. Vedoucí práce Fredrik Payman Milani a Henrik Veenpere. Dostupné z: https://pdfs.semanticscholar.org/8edc/438a42ce7f6502d79e263bc96d402d7c823a.pdf?_ga=2.227796125.1449854370.1564680349-2102907078.1564680349

OSBORNE, M., 2013. *Cyber attack, cyber crime, cyber warfare: Cyber complacency*. North Charleston, SC: Create Space Independent Publishing Platform. ISBN 1493581287.

OSOUCH, Marek a Petr ŠKARDA, 2020. Brněnská nemocnice čelí kybernetickému útoku, neoperuje a převáží pacienty. *IDNES.cz* [online]. Praha: © 1999–2020 MAFRA. [cit. 2020-03-23]. Dostupné z: https://www.idnes.cz/brno/zpravy/brno-nemocnice-fakultni-nemocnice-kyberneticky-utok.A200313_071531_brno-zpravy_bur

OTUOZE, Abdulrahaman Okino, Mohd Wazir MUSTAFA a Raja Masood LARIK, 2018. Smart grids security challenges: Classification by sources of threats. *Journal of Electrical Systems and Information Technology* [online]. [cit. 2018-03-04]. DOI: 10.1016/j.jesit.2018.01.001. ISSN 23147172.

Overview of the DNP3 Protocol. *DNP.org - Distributed Network Protocol* [online]. California, 2011 [cit. 2018-02-07]. Dostupné z: https://www.dnp.org/pages/aboutdefault.aspx

OYETOYAN, Tosin Daniel, Bisera MILOSHESKA, Mari GRINI a Daniela SOARES CRUZES, 2018. Myths and Facts About Static Application Security Testing Tools: An Action Research at Telenor Digital. Agile Processes in Software Engineering and Extreme Programming. Cham: Springer International Publishing, 2018-05-17, , 86-103. Lecture Notes in Business Information Processing. DOI: 10.1007/978-3-319-91602-6_6. ISBN 978-3-319-91601-9. Dostupné také z: http://link.springer.com/10.1007/978-3-319-91602-6_6

QINGRONG JASON WU, Wu, Xuan ZHU SHERRY ZHU, Kuei-Chi KUO ERIC GUO a Cong LU MAX LU, 2017. Light SIEM for semiconductor industry. *In: 2017 IEEE International Conference on Industrial Engineering and Engineering Management (IEEM)* [online]. IEEE, 2017, s. 2331-2335 [cit. 2019-06-20]. DOI: 10.1109/IEEM.2017.8290308. ISBN 978-1-5386-0948-4. Dostupné z: http://ieeexplore.ieee.org/document/8290308

PAI, Shreenivas, Neha BANSAL, Kama DESAI, Archana DOSHI, Devendra MOHARKAR a Mihir PATHARE. *Intelligent PLC based transformer cooling control system* [online]. [cit. 2017-11-27]. DOI: 10.1109/ICNTE.2017.7947926. ISBN 10.1109/ICNTE.2017.7947926. Dostupné z: http://ieeexplore.ieee.org/document/7947926/

PAL, Aurabind a Roma DASH, 2015. A Paradigm Shift in Substation Engineering: IEC 61850 Approach. *Procedia Technology* [online]. 21, 8-14 [cit. 2017-10-08]. DOI: 10.1016/j.protcy.2015.10.003. ISSN 22120173.

PARMAR, Bimal, 2012. Protecting against spear-phishing. *Computer Fraud & Security* [online]. 2012(1), 8-11 [cit. 2017-12-29]. DOI: 10.1016/S1361-3723(12)70007-6. ISSN 13613723. Dostupné z: http://linkinghub.elsevier.com/retrieve/pii/S1361372312700076

PAL, Aurabind a Roma DASH, 2015. A Paradigm Shift in Substation Engineering: IEC 61850 Approach. *Procedia Technology* [online]. 21, 8-14 [cit. 2017-11-04]. DOI: 10.1016/j.protcy.2015.10.003. ISSN 22120173.

PASSERI, Paolo. 2016 Cyber Attacks Statistics. PASSERI, Paolo. *Hackmageddon* [online]. 2017 [cit. 2017-11-04]. Dostupné z: http://www.hackmageddon.com/2017/01/19/2016-cyber-attacks-statistics/

PATÓN-ROMERO, J. David, Maria Teresa BALDASSARRE, Moisés RODRÍGUEZ a Mario PIATTINI, 2018. *Green IT Governance and Management based on ISO/IEC 15504* [online]. **60**, 26-36 [cit. 2019-10-22]. DOI: 10.1016/j.csi.2018.04.005. ISSN 09205489. Dostupné z: https://linkinghub.elsevier.com/retrieve/pii/S0920548918300126

PEKÁREK, D. Popis a testování komunikačních protokolů normy IEC 60870-5-103 a 60870-5-104. 2017. Diplomová práce. Brno: Ústav elektroenergetiky FEKT VUT v Brně, 72 stran.

PEREZ, Evan a Shimon PROKUPECZ, 2016. *First on CNN: U.S. plans to publicly blame Iran for dam cyber breach* [online]. Atlanta, Georgia: Turner Broadcasting Systém [cit. 2017-11-05]. Dostupné z: http://edition.cnn.com/2016/03/10/politics/iran-us-dam-cyber-attack/index.html

PIGNY, G., et al., 2017. A new PROFIBUS interface for vacuum sector gate valve controllers." *Journal of Instrumentation* 12.02: C02066.

PLOJHAR, Jan. Analýza a návrh na zlepšení IS [online]. Praha, 2015 [cit. 2020-06-22]. Dostupné z: https://vskp.vse.cz/45649_analyza_anavrh_na_zlepseni_is. Bakalářská práce. Vysoká škola ekonomická v Praze, Fakulta informatiky a statistiky, Katedra informačních technologií. Vedoucí práce Ing. Filip Vencovský.

Ponemon institute, 2016. *2016 Cost of Cyber Crime Study & the Risk of Business Innovation* [online]. Ponemon Institute LLC., 1-36 [cit. 2017-11-05]. Dostupné z: http://go.cyphort.com/Ponemon-SIEM-Report-2017-Page.html

Ponemon institute, 2017. *2016 Ponemon Report: Challenges to Achieving SIEM Optimization* [online]. Ponemon Institute LLC., 1-30 [cit. 2019-21-05]. Dostupné z: https://www.ponemon.org/local/upload/file/2016%20HPE%20CCC%20GLOBAL%20REPORT%20FINAL%203.pdf

POUDEL, Shiva, Zhen NI a Naresh MALLA, 2017. Real-time cyber physical system testbed for power system security and control. *International Journal of Electrical Power & Energy*

Systems [online]. 90, 124-133 [cit. 2017-11-04]. DOI: 10.1016/j.ijepes.2017.01.016. ISSN 01420615.

POWELL, James. PROFIBUS AND MODBUS: A COMPARISON, 2013. *Siemens* [online]. Mnichov. [cit. 2018-02-17]. Dostupné z: https://www.industry.siemens.com/datapool/industry/automation/Tech-Art/2013/FAV-105-2013-IA-SC/FAV-105-2013-IA-SC-V01_EN.pdf

PROFIBUS Protocol Overview, 2014. *Real Time Automation: Saving the World from Inaccessible Data* [online]. Colorado Springs, ©2018 [cit. 2018-02-17]. Dostupné z: https://www.rtaautomation.com/technologies/profibus/

PROVOZOVATELÉ DISTRIBUČNÍCH SOUSTAV. *Pravidla provozování distribuční soustavy*. 2014. Dostupné také z: https://www.cezdistribuce.cz/edee/content/file-other/distribuce/energeticka-legislativa/ppds/2014/ppds-2014-hc.pdf

PŘENOSOVÁ A DISTRIBUČNÍ SOUSTAVA 1. ČÁST - VEDENÍ VELMI VYSOKÉHO NAPĚTÍ (VVN), 2017. E.ON Distribuce[online]. České Budějovice, [cit. 2017-11-27]. Dostupné z: https://www.eon-distribuce.cz/o-nas/novinky/media/prenosova-a-distribucni-soustava-elektricke-energie

PUTRI, Rahmi Eka a Kridanto SURENDRO, 2015. A process capability assessment model of IT governance based on ISO 38500. *2015 International Conference on Information Technology Systems and Innovation (ICITSI)* [online]. IEEE, 1-6 [cit. 2019-10-22]. DOI: 10.1109/ICITSI.2015.7437673. ISBN 978-1-4673-6663-2. Dostupné z: http://ieeexplore.ieee.org/document/7437673/

RADVANOVSKY, Robert a Jacob BRODSKY, 2016. *Handbook of SCADA/control systems security*. Second edition. Boca Raton: CRC Press, Taylor & Francis Group. ISBN 9781498717076.

RAYDEL Montesino, Stefan FENZ a Walter BALUJA, 2012. SIEM-based framework for security controls automation", *Information Management & Computer Security*, Vol. 20 Issue: 4, pp.248-263, [cit. 2019-06-20]. Dostupné z: https://doi.org/10.1108/09685221211267639

RAUS, Petr. ELEKTROENERGETIKA V ČESKÉ REPUBLICE (1997 AŽ 2006), 2009. [online]. Jihlava. [cit. 2017-11-04]. Dostupné z: https://is.vspj.cz/bp/get-bp/student/10315/thema/415. Bakalářská práce. Vysoká škola polytechnická Jihlava. Vedoucí práce Prof. Ing. Bohumil Minařík, Csc.

RAZI KAZEMI, A.A. a P. DEHGHANIAN, 2012. A practical approach on optimal RTU placement in power distribution systems incorporating fuzzy sets theory. *International Journal of Electrical Power & Energy Systems*[online]. 37(1), 31-42 [cit. 2017-11-04]. DOI: 10.1016/j.ijepes.2011.12.001. ISSN 01420615.

Reporting, 2019. *LogRhythm* [online]. Boulder: ©LogRhythm, [cit. 2019-06-20]. Dostupné z: https://logrhythm.com/products/features/reporting/

REZAI, Abdalhossein, Parviz KESHAVARZI a Zahra MORAVEJ, 2013. Secure SCADA communication by using a modified key management scheme. *ISA Transactions* [online]. 52(4), 517-524 [cit. 2017-11-04]. DOI: 10.1016/j.isatra.2013.02.005. ISSN 00190578.

REXHEPI, Vezir, 2017. An Analysis of Power Transformer Outages and Reliability Monitoring. *Energy Procedia* [online]. 141, 418-422 [cit. 2017-12-29]. DOI: 10.1016/j.egypro.2017.11.053. ISSN 18766102. Dostupné z: http://linkinghub.elsevier.com/retrieve/pii/S1876610217354590

ROBERTS, Paul F, Duben 2010. What is NERC CIP, and IT's role in critical infrastructure protection? TechTarget [online]. TechTarget, ©2009-2018, [cit. 2018-01-17]. Dostupné z: http://searchcompliance.techtarget.com/feature/What-is-NERC-CIP-and-ITs-role-in-critical-infrastructure-protection

RONEŠOVÁ, Andrea, 2005. Přehled protokolu MODBUS. *Západočeská univerzita v Plzni* [online]. Plzeň, květen 2005 [cit. 2018-02-17]. Dostupné z: http://home.zcu.cz/~ronesova/bastl/files/modbus.pdf

RP 570 Protocol Description: Technical Description Manual, 1997. *ABB Group - Leading digital technologies for industry* [online]. Curych [cit. 2018-02-17]. Dostupné z: https://library.e.abb.com/public/9a5c1896695487e6c2256a7200361578/REC501RP570_EN_A.pdf

RUBIO, Juan E., Cristina ALCARAZ a Javier LOPEZ, 2017. Recommender system for privacy-preserving solutions in smart metering. *Pervasive and Mobile Computing* [online]. 41, 205-218 [cit. 2018-01-28]. DOI: 10.1016/j.pmcj.2017.03.008. ISSN 15741192.

RUDZINSKI, Yvan a Pavel VLADYKA, 2010. Komunikační protokoly pro dálkové ovládání IEC/ISO 60870-5. *Automa* [online]. 8(2), 21-22 [cit. 2018-01-28]. Dostupné z: http://automa.cz/Aton/FileRepository/pdf_articles/40552.pdf

RYCHLÝ, Marek, 2015. Úvod do COBIT. In: *Fakulta informačních technologií VUT v Brně* [online]. Brno: Fakulta informačních technologií. [cit. 2019-07-18]. Dostupné z: http://www.fit.vutbr.cz/~rychly/public/docs/slides-intr_COBIT_framework/slides-intr_COBIT_framework.print.pdf

Řízení rizik projektu, 2019. *PM Consulting* [online]. Praha. [cit. 2019-08-02]. Dostupné z: https://www.pmconsulting.cz/pm-wiki/rizeni-rizik-projektu/

SEBERA, Martin, 2012. *Vybrané kapitoly z metodologie*. Brno: Masarykova univerzita. ISBN 978-80-210-5963-4

SEDLÁK, Jan, 2019. OKD přerušila těžbu ve všech dolech, síť a servery napadli hackeři. In: *Lupa.cz*[online]. Praha: © 1998 – 2020 Internet Info. [cit. 2020-03-23]. Dostupné z: https://www.lupa.cz/aktuality/okd-prerusila-tezbu-ve-vsech-dolech-sit-a-servery-napadli-hackeri/

SEDLÁK, Jan, 2019. *Vládní CERT vydal varování před ransomwarem a botnetem, ohrožuje ČR* [online]. In: . Praha: © 1998 – 2020 Internet Info. [cit. 2020-03-23]. Dostupné z: https://www.lupa.cz/aktuality/vladni-cert-vydal-varovani-pred-ransomwarem-a-botnetem-ohrozuje-cr/

SENNEWALD, Charles a Curtis BAILLIE. Effective Security Management. 6th edition. Oxford: Butterworth-Heinemann, 2015. ISBN 9780128027745.

SCHILLER, Susannah, 2013. *Federal Enterprise Architecture Framework: Version 2* [online]. Washington, D.C. [cit. 2019-08-02]. Dostupné z: https://obamawhitehouse.archives.gov/sites/default/files/omb/assets/egov_docs/fea_v2.pdf

SCHLEGEL, Roman, Sebastian OBERMEIER a Johannes SCHNEIDER, 2017. A security evaluation of IEC 62351. Journal of Information Security and Applications [online]. 34, 197-204 [cit. 2018-04-02]. DOI: 10.1016/j.jisa.2016.05.007. ISSN 22142126. Dostupné z: http://linkinghub.elsevier.com/retrieve/pii/S2214212616300771

SENTHIVEL, Saranyan, Irfan AHMED a Vassil ROUSSEV. SCADA network forensics of the PCCC protocol. *Digital Investigation* [online]. 2017, 22, S57-S65 [cit. 2018-02-07]. DOI: 10.1016/j.diin.2017.06.012. ISSN 17422876.

SHABU, Martin, 2020. Hackeři v minulých dnech napadli i distribuční síť ČEZ, která obsluhuje miliony domácností Zdroj: https://www.lidovky.cz/byznys/firmy-a-trhy/distribucni-sit-cez-distribuce-celila-v-minulych-dnech-kybernetickemu-utoku.A200421_073109_firmy-trhy_ele. Lidovky.cz [online]. Praha: © 2020 MAFRA, a.s, [cit. 2020-05-19]. Dostupné z: https://www.lidovky.cz/byznys/firmy-a-trhy/distribucni-sit-cez-distribuce-celila-v-minulych-dnech-kybernetickemu-utoku.A200421_073109_firmy-trhy_ele

SIEMENS, 2016, Energeticky úsporná stanice vzdáleného ovládání (RTU) společnosti Siemens umožní dálkový monitoring pomocí sítí mobilních operátorů. *Tiskové centrum SIEMENS Česká republika* [online]. Česká republika, 2016 [cit. 2017-10-08]. Dostupné z: http://www.siemens.cz/press/energeticky-usporna-stanice-vzdaleneho-ovladani-rtu-spolecnosti-siemens-umozni-dalkovy-monitoring-pomoci-siti-mobilnich-operatoru

SIMA, Jiri, Ondrej SIKULA, Katarina KOSUTOVA a Josef PLASEK, 2014. Theoretical Evaluation of Night Sky Cooling in the Czech Republic. *Energy Procedia* [online]. 48, 645-653 [cit. 2018-01-06]. DOI: 10.1016/j.egypro.2014.02.075. ISSN 18766102.

Security Orchestration, Automation and Response, 2019. Logrhythm [online]. Boulder: ©LogRhythm, [cit. 2019-06-25]. Dostupné z: https://logrhythm.com/solutions/security/security-automation-and-orchestration/

SOBĚSLAV, Vladimír, 2012. *Architektury počítačových sítí v podnikové informatice*. Hradec Králové. Disertační práce. Univerzita Hradec Králové. Vedoucí práce Prof. RNDr. Peter Mikulecký, PhD.

SON, Kwang Seop, Dong Hoon KIM, Gee Yong PARK a Hyun Gook KANG, 2018. Availability analysis of safety grade multiple redundant controller used in advanced nuclear safety systems. *Annals of Nuclear Energy* [online]. 111, 73-81 [cit. 2017-11-04]. DOI: 10.1016/j.anucene.2017.08.065. ISSN 03064549.

SRIDHAR, Siddharth, Adam HAHN a Manimaran GOVINDARASU, 2012. Cyber–Physical System Security for the Electric Power Grid. *Proceedings of the IEEE* [online]. 100(1), 210-224 [cit. 2017-12-29]. DOI: 10.1109/JPROC.2011.2165269. ISSN 0018-9219. Dostupné z: http://ieeexplore.ieee.org/document/6032699/

STAGGS, Jason, David FERLEMANN a Sujeet SHENOI, 2017. Wind farm security: attack surface, targets, scenarios and mitigation. *International Journal of Critical Infrastructure Protection* [online]. 17, 3-14 [cit. 2018-03-04]. DOI: 10.1016/j.ijcip.2017.03.001. ISSN 18745482.

STODŮLKA, I, 2012. *Model elektrické stanice s komunikačním protokolem IEC 61850*. Brno: Vysoké učení technické v Brně, Fakulta elektrotechniky a komunikačních technologií. 97s. Vedoucí diplomové práce doc. Ing. Jaroslava Orságová, Ph.D.

STOUFFER, K., FALCO J., and SCARFONE, K., 2015, "Guide to industrial control systems (ICS) security." *NIST special publication,*800.82: 16-16.

SUN, Chih-Che, Adam HAHN a Chen-Ching LIU, 2018. Cyber security of a power grid: State-of-the-art. *International Journal of Electrical Power & Energy Systems* [online]. 99, 45-56 [cit. 2018-03-04]. DOI: 10.1016/j.ijepes.2017.12.020. ISSN 01420615.

SYSTÉMY CHRÁNĚNÍ, 2017. E.ON Distribuce[online]. České Budějovice: E.ON, [cit. 2017-10-27]. Dostupné z: https://www.eon-distribuce.cz/o-nas/novinky/media/prenosova-a-distribucni-soustava-3-cast-dispecersky-ridici-system-systemy-chraneni-komunikace-a-hdo

ŠIKULA, J. Převod standardu IEC 61850 na komunikační protokol MODBUS, 2016. BRNO: Vysoké Učení Technické v Brně, Fakulta Elektrotechniky a Komunikačních Technologií, 2016. 37 S. Vedoucí Bakalářské práce ing. Helena Polsterová, Csc.

ŠKEŘÍK, Ondřej, 2016. *Systém řízení bezpečnosti informací prostřednictvím normy ČSN/EN ISO/IEC 27001* [online]. Pardubice, 2016 [cit. 2018-04-02]. Dostupné z: https://theses.cz/id/3lkxvo/STAG64882.pdf. Diplomová práce. Univerzita Hradec Králové, Fakulta informatiky a managementu. Vedoucí práce Mgr. Josef Horálek, Ph. D.

ŠTEPÁN, Jakub, 2016. *Outsourcing a jeho dopady na organizaci optikou podnikové architektury*. Praha. Diplomová práce. Vysoká škola ekonomická v Praze, Fakulta informatiky a statistiky. Vedoucí práce Ing. Michal Šebesta.

TAKALA, Rudy, 2015. Iranian group claims credit for hacking NY dam. *Washington Examiner* [online]. Washington D. C: Turner Broadcasting System [cit. 2017-11-05]. Dostupné z: http://www.washingtonexaminer.com/iranian-group-claims-credit-for-hacking-ny-dam/article/2579008

TESAŘÍK, J, 2014. *Systémy ochran a vzdáleného řízení vn rozvodny s použitím ochran s komunikací Profibus a IEC61850*. Brno: Vysoké učení technické v Brně, Fakulta elektrotechniky a komunikačních technologií. 75 s. Vedoucí diplomové práce Ing. Rostislav Huzlík

TETI, R., K. JEMIELNIAK, G. O'DONNELL a D. DORNFELD, 2010. Advanced monitoring of machining operations. *CIRP Annals* [online]. 2010, 59(2), 717-739 [cit. 2017-11-04]. DOI: 10.1016/j.cirp.2010.05.010. ISSN 00078506.

The 62443 series of standards, 2016. *ISA* [online]. Durham [cit. 2018-04-02]. Dostupné z: https://cdn2.hubspot.net/hubfs/3415072/Resources/The%2062443%20Series%20of%20Standards.pdf

The State of Industrial Cybersecurity 2017, 2017. In: Kaspersky [online]. Moskva. [cit. 2018-01-07]. Dostupné z: https://go.kaspersky.com/rs/802-IJN-240/images/ICS%20WHITE%20PAPER.pdf

THOMAS, Brinda A., Inês L. AZEVEDO a Granger MORGAN, 2012. Edison Revisited: Should we use DC circuits for lighting in commercial buildings? *Energy Policy* [online]. 2012, 45, 399-411 [cit. 2017-11-04]. DOI: 10.1016/j.enpol.2012.02.048. ISSN 03014215.

VAN DEN BERG, Martin, Raymond SLOT, Marlies VAN STEENBERGEN, Peter FAASSE a Hans VAN VLIET, 2019. How enterprise architecture improves the quality of IT investment decisions. *Journal of Systems and Software* [online]. 152, 134-150 [cit. 2019-07-20]. DOI:

10.1016/j.jss.2019.02.053. ISSN 01641212. Dostupné z: https://linkinghub.elsevier.com/retrieve/pii/S0164121219300433

VAIDYA, B., D. MAKRAKIS a H. T. MOUFTAH, 2013. Authentication and authorization mechanisms for substation automation in smart grid network. *IEEE Network* [online]. 27(1), 5-11 [cit. 2018-03-04]. DOI: 10.1109/MNET.2013.6423185. ISSN 0890-8044.

VAN DEN BERG, Martin, Raymond SLOT, Marlies VAN STEENBERGEN, Peter FAASSE a Hans VAN VLIET. How enterprise architecture improves the quality of IT investment decisions. Journal of Systems and Software[online]. 2019, 152, 134-150 [cit. 2020-07-01]. DOI: 10.1016/j.jss.2019.02.053. ISSN 01641212. Dostupné z: https://linkinghub.elsevier.com/retrieve/pii/S0164121219300433

VAVRECZKY, G, 2012. *Otestovaní komunikace po IEC61850 s využitím GOOSE mezi ABB a Siemens ochranou.* Brno: Vysoké učení technické v Brně, Fakulta elektrotechniky a komunikačních technologií, 69 s. Vedoucí diplomové práce doc. Ing. Jaroslava Orságová, Ph.D.

VLČEK, Tomáš a Filip ČERNOCH. Energetický sektor České republiky. Brno: Masarykova univerzita, 2012. ISBN 978-80-210-5982-5.

VOZDECKÝ, M, 2013. *Implementace procesní metodiky ITIL.* Brno: Vysoké učení technické v Brně, Fakulta podnikatelská, 74 s. Vedoucí diplomové práce doc. Ing. Miloš Koch, CSc.

Vyhláška č. 82/2018 Sb. o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních a o stanovení náležitostí podání v oblasti kybernetické bezpečnosti a likvidaci dat (vyhláška o kybernetické bezpečnosti), *In: Sbírka zákonů České republiky*. Česká republika, ročník 2018, částka 43

Vyhláška č. 80/2010 Sb. o stavu nouze v elektroenergetice a o obsahových náležitostech havarijního plánu, In: Sbírka zákonů České republiky. Česká republika, ročník 2010, částka 28

Vyhláška č. 79/2010 Sb. Vyhláška o dispečerském řízení elektrizační soustavy a o předávání údajů pro dispečerské řízení, In: Sbírka zákonů České republiky. Česká republika, ročník 2010, částka 28

What is Zachman Framework?, 2019 *Visual Paradigm* [online]. Hong Kong: Visual Paradigm International. [cit. 2019-09-05]. Dostupné z: https://www.visual-paradigm.com/guide/enterprise-architecture/what-is-zachman-framework/

WU, Longfei, Xiaojiang DU a Jie WU, 2016. Effective Defense Schemes for Phishing Attacks on Mobile Computing Platforms. *IEEE Transactions on Vehicular Technology* [online].65(8), 6678-6691 [cit. 2017-11-04]. DOI: 10.1109/TVT.2015.2472993. ISSN 0018-9545.

YAKIMOV, Peter I. a IOVEV, Atanas N. Application of PLC as a Gateway in a Network of Smart Power Transducers. IFAC-PapersOnLine [online]. 2015, 48(24), 95-98 [cit. 2020-07-01]. DOI: 10.1016/j.ifacol.2015.12.063. ISSN 24058963. Dostupné z: https://linkinghub.elsevier.com/retrieve/pii/S2405896315026877

YOUNG, Carl S, 2015. Electronic Terrorism Threats, Risk, and Risk Mitigation. *The Science and Technology of Counterterrorism* [online]. Elsevier, 2015, s. 221-281 [cit. 2018-04-08]. DOI: 10.1016/B978-0-12-420056-2.00008-7. ISBN 9780124200562. Dostupné z: http://linkinghub.elsevier.com/retrieve/pii/B9780124200562000087

ZACHMAN, John, 2008. The Concise Definition of The Zachman Framework by: John A. Zachman. *Zachman international enteprise architecture* [online]. Monument, Colorado: Zachman International, 2008 [cit. 2019-09-09]. Dostupné z: https://www.zachman.com/about-the-zachman-framework

ZHU, Bonnie, Anthony JOSEPH a Shankar SASTRY, 2011. A Taxonomy of Cyber Attacks on SCADA Systems. In: *2011 International Conference on Internet of Things and 4th International Conference on Cyber, Physical and Social Computing* [online]. IEEE, s. 380-388 [cit. 2017-11-04]. DOI: 10.1109/iThings/CPSCom.2011.34. ISBN 978-1-4577-1976-9.

Zákon o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti). In: *Sbírka zákonů České republiky*. Česká republika, ročník 2014, částka 95.

Zákon č. 458/2000 Sb.: Zákon o podmínkách podnikání a o výkonu státní správy v energetických odvětvích a o změně některých zákonů (energetický zákon). In: *Sbírka zákonů České republiky*, ročník 2000, částka 95.

ŽÁČEK, Jaroslav, 2019. ITIL základy. In: WWW server uživatelů na Ostravské univerzitě [online]. Ostrava [cit. 2019-07-02]. Dostupné z: http://www1.osu.cz/~zacek/sweng/10.pdf

PŘÍLOHA A – proces určování kritické informační infrastruktury