Univerzita Pardubice

Fakulta elektrotechniky a informatiky

Principy bezpečnosti Smart Grid sítí

Bc. Roman Diviš

Diplomová práce

2013

Univerzita Pardubice
Fakulta elektrotechniky a informatiky
Akademický rok: **2012/2013**

ZADÁNÍ DIPLOMOVÉ PRÁCE

(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení:	**Bc. Roman Diviš**
Osobní číslo:	**I11369**
Studijní program:	**N2646 Informační technologie**
Studijní obor:	**Informační technologie**
Název tématu:	**Principy bezpečnosti Smart Grid sítí**
Zadávající katedra:	**Katedra softwarových technologií**

Zásady pro vypracování:

Cílem práce je představit principy sítí typu Smart Grid, analyzovat možná bezpečností rizika a teoreticky navrhnout jejich řešení.
Cílem teoretické diplomové práce je představit problematiku a principy Smart Grid sítí s přihlédnutím k principům "klasických" datových sítí. Na základě principů a koncepcí Smart Grid sítí analyzovat a vyhodnotit možná bezpečnostní rizika při využívání Smart Grid sítí. Na základě provedené analýzy budou navrženy modely řešení vybraných bezpečnostních rizik.

Rozsah grafických prací:

Rozsah pracovní zprávy:

Forma zpracování diplomové práce: **tištěná/elektronická**

Seznam odborné literatury:

HOSSAIN, Ekram, Zhu HAN a H POOR. Smart grid communications and networking. New York: Cambridge University Press, 2012, xxviii, 481 p. ISBN 978-110-7014-138.
SOREBO, Gilbert N, Michael C ECHOLS a H POOR. Smart Grid Security: An End-to-End View of Security in the New Electrical Grid. Boca Raton: CRC Press, 2011, xxvi, 302 s. ISBN 978-1439855874.
KNAPP, Eric, Michael C ECHOLS a H POOR. Industrial network security: securing critical infrastructure networks for Smart Grid, SCADA , and other industrial control systems. Waltham, MA: Syngress, c2011, xvii, 341 p. ISBN 15-974-9645-6.
FLICK, Tony, Justin MOREHOUSE a H POOR. Securing the smart grid: next generation power grid security. Boston: Syngress, c2011, xxv, 290 p. ISBN 15-974-9570-0.

Vedoucí diplomové práce: **Mgr. Josef Horálek**
Katedra softwarových technologií

Datum zadání diplomové práce: **31. října 2012**
Termín odevzdání diplomové práce: **17. května 2013**

Univerzita Pardubice Česká republika

L.S.

prof. Ing. Simeon Karamazov, Dr.
děkan

prof. Ing. Antonín Kavička, Ph.D.
vedoucí katedry

V Pardubicích dne 15. listopadu 2012

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., autorský zákon, 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.

Souhlasím s prezenčním zpřístupněním své práce v Univerzitní knihovně.

V Pardubicích dne 13. 5. 2013

Bc. Roman Diviš

PODĚKOVÁNÍ

Rád bych touto formou poděkoval vedoucímu mé diplomové práce panu Mgr. Josefu Horálkovi za odborné vedení a cenné rady, které mi poskytl v průběhu práce.

ANOTACE

Tato práce se zabývá problematikou sítí typu Smart Grid. Smart Grid sítě jsou analyzovány a jsou popsána možná bezpečnostní rizika při jejich používání. V závěru práce je navrženo několik řešení pro vybraná bezpečnostní rizika.

KLÍČOVÁ SLOVA

smart grid, bezpečnost, SCADA, síť

TITLE

Principles of security of Smart Grid networks

ANNOTATION

This work is dedicated to Smart Grid networks. Smart Grid networks are analyzed and then discussed possible security risks with their usage. In conclusion author proposed several solutions for selected security risks.

KEYWORDS

smart grid, security, SCADA, network

OBSAH

SEZNAM ZKRATEK A ZNAČEK

ACL	Access control list
AES	Advanced encryption standard
AMI	Advanced metering infrastructure
AMR	Automated meter reading
ANSI	American National Standards Institute
ARP	Address resolution protocol
BAN	Building area network
BPDU	Bridge protocol data unit
BS	Base station
BTS	Base transceiver station
CAM	Content addressable memory
CBC-MAC	Cipher block chaining – message authentication code
CCM	Counter with CBC-MAC
CSRF	Cross site request forgery
DAU	Data aggregator unit
DES	Data encryption standard
DNP	Distributed network protocol
DNS	Domain name system
DOE	Department of energy
DoS	Denial of service
DR	Demand response
EAP	Extensible authentication protocol
EIGRP	Enhanced interior gateway routing protocol
EMS	Energy management system
ENISA	European Network and Information Security Agency
ETSI	European Telecommunications Standards Institute
FERC	Federal energy regulation commision
FTP	File transfer protocol
GEO	Geostationary Earth orbit
HAN	Home area network
HMI	Human machine interface
HTTP	Hyper text transfer protocol
IDS	Intrusion detection system
IEC	International Electrotechnical Commission
IED	Intelligent electronic device
IHD	In home display
IP	Internet protocol
IPS	Intrusion prevension system
IPSec	Internet protocol security
ISO	International Organization for Standardization
LAN	Local area network

LEO	Low Earth orbit
LTE	Long-term evolution
MAC	Media access control
MAN	Metropolitan area network
MD5	Message digest 5
MDMS	Meter data management system
MEO	Medium Earth orbit
MITM	Man in the middle
NAN	Neighbourhood area network
NERC	North American Electric Reliability Corporation
NIST	National Institute of Standards and Technology
NN	Nízké napětí
OSPF	Open shortest path first
PAN	Premise area network
PCT	Programmable communicating thermostat
PDC	Phasor data collector
PEV	Plug-in electric vehicle
PKI	Public key infrastructure
PLC	Power line communications
PLC	Programmable logic controller
PMU	Phasor measurement unit
RC4	Rivest cipher 4
RIP	Routing information protocol
RTU	Remote terminal unit
SCADA	Supervisory control and data acquisition
SHA	Secure hash algorithm
SPDC	Super phasor data collector
SQL	Structured query language
SSL	Secure sockets layer
STP	Spanning tree protocol
TCP	Transmission control protocol
TLS	Transport layer security
UDP	User datagram protocol
VN	Vysoké napětí
VPN	Virtual private network
VVN	Velmi vysoké napětí
WAMS	Wide area measurement system
WAN	Wide area network
WEP	Wired equivalent privacy
WPA	Wi-Fi protected access
WSN	Wireless sensor network
XSS	Cross site scripting

SEZNAM ILUSTRACÍ

ÚVOD

Elektrická energie a její využívání je v 21. století každodenní rutinou pro většinu vyspělého světa. Elektřina je využívána pro přepravu, osvětlení, topení i mnoho dalších činností a její nepřetržitá dodávka je dnes již standardním požadavkem. Se vzrůstajícím množstvím spotřebitelů také vzrůstá množství poptávané elektrické energie. Stávající rozvodné sítě a elektrárny jsou schopny požadovanou energii dodávat, ale síť nepracuje efektivně. Výkon elektráren dodávaný do sítě je naddimenzován a zátěž v průběhu dne je nerovnoměrně rozložena do období ranní a večerní špičky. Současné rozvodné sítě rovněž neumožňují efektivní využívání energie získané z obnovitelných zdrojů.

Koncept Smart Grid byl představen v roce 2006 a představuje evoluci elektrické rozvodné sítě. K vlastní přenosové soustavě přidává komunikační síť, která propojí zákazníky s energetickými společnostmi. Tím je umožněna obousměrná komunikace v reálném čase. Zákazníci tak mohou informovat elektrárny o své spotřebě, energetické společnosti monitorovat stav sítě a řídit přenosovou soustavu na dálku.

Cílem této diplomové práce je analyzovat komunikační architekturu Smart Grid sítí a vyhodnotit možná bezpečnostní rizika při jejich využívání. Pro vybraná bezpečnostní rizika budou navrženy modely jejich řešení.

Mezi cíle Smart Gridu patří zefektivnění činnosti rozvodné soustavy, vytvoření soustavy schopné připojovat distribuované zdroje elektrické energie (obnovitelné zdroje, elektromobily) nebo také nabídnou možnost zpoplatnění elektrické energie dle aktuální poptávky.

Smart Grid technologie jsou v současnosti realizovány v několika pilotních projektech, které testují účinnost v malém měřítku. Po úspěšné realizaci těchto projektů jsou v dnešní době připravovány plány pro realizaci národních Smart Grid sítí v USA, Číně a dalších státech. V rámci Evropské unie byla vytvořena iniciativa European Technology Platform, která připravuje podklady pro nasazení Smart Grid technologií. Dle současných plánů se uvažuje o implementaci Smart Grid technologií okolo let 2020–2030.

Zavedení komunikační infrastruktury mezi zákazníky a energetické společnosti přináší mnoho bezpečnostních rizik. Ohroženi jsou zákazníci, přenosová síť, elektrárny i další aktéři v procesu distribuce elektrické energie. Zvýšení automatizace v řízení přenosové soustavy může zlepšit stabilitu sítě automatickým reagováním na problémy v síti, ale také poskytuje potenciální nebezpečí, které může hacker využít k poškození sítě a přerušení dodávek elektrické energie. Možné bezpečnostní hrozby jsou popsány v této práci a pro vybraná rizika jsou navrženy modely řešení těchto rizik.

1 REŠERŠE

Následující kapitola obsahuje přehled literární rešerše na téma bezpečnosti sítí Smart Grid.

Ze seznamu doporučené literatury, kniha od Hossaina, Hana a Poora [1] představuje konkrétní dopady útoků na systém WAMS (wide area measurement system) a možnosti rušení bezdrátových komunikací pro manipulaci s trhem. V knize jsou uvedeny konkrétní příklady topologie sítě, scénáře útoků a jejich dopad. Z obecného hlediska kniha představuje hierarchický přístup k zabezpečení sítě. Monografie od autorů Soreba a Echolse [2] popisuje Smart Grid sítě a obecné bezpečnostní problémy. *Securing the Smart Grid* od autorů Flicka a Morehouse [3] představuje praktičtější pohled na bezpečnost, v knize jsou popsány standardy a normy, které se týkají bezpečnosti Smart Grid a informačních systémů. V dalších částech jsou popsány konkrétní útoky na jednotlivé části sítě, autoři se zabývají i bezpečnostní mobilních zařízení a sociálních sítí. Ve všech zmíněných publikacích je rovněž popsán princip managementu rizik, využívaný pro vyhodnocování rizik a jejich odstraňování.

V publikaci od Kaplana a kolektivu [9] jsou podrobně popsány sítě Smart Grid, požadavky a jednotlivé funkce sítě. V knize od Knappa [7] jsou popsány bezpečnostní problémy a principy v průmyslových systémech, Smart Grid sítích a také SCADA (supervisory control and data acquisition) systémech. V novější publikaci *Applied Cyber Security and the Smart Grid* [10] se autoři zaměřují na možnosti napadení sítě Smart Grid a zejména na problematiku soukromí uživatelů. V dalších částech jsou popsány způsoby zabezpečení sítě.

Autoři článku *Security Technology for Smart Grid Networks* [11] popisují bezpečnostní problémy v bezdrátových sítích a navrhují možné řešení využitím technologie PKI (public key infrastructure). Příspěvek Davida von Oheimba [13] popisuje problémy týkající se vzdáleného odečítání smart meterů a popisuje možný komunikační protokol pro zajištění autentizace a důvěrnosti zařízení a dat. Autor také zmiňuje některé nevýhody při používání obecného PKI mechanismu. Ericsson ve svém článku [12] popisuje problematiku spojování řídících systémů SCADA s běžnými prostředky informačních technologií. Autor dále popisuje různé cesty, kudy je možné systémy SCADA napadnout.

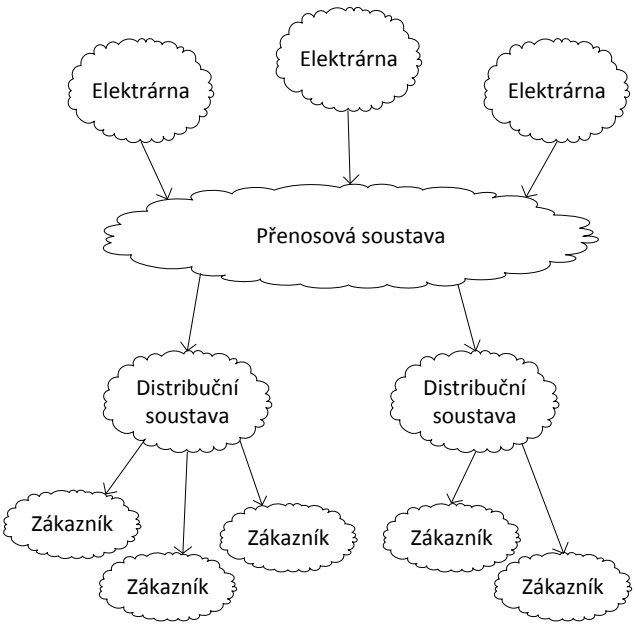
V dokumentu připraveném Isaacem Ghansahem [4] jsou popsány konkrétní bezpečnostní rizika jednotlivých komponent Smart Grid sítě. Autor zmiňuje hrozby týkající se systému AMI (advanced metering infrastructure), DR (demand response), SCADA a jednotlivých částí sítě. V závěru pak autor popisuje požadavky na bezpečnost jednotlivých komponent.

Podobný soupis zranitelností, útočníků a možných řešení je uveden v článku *Smart Grid Security: Threats, Vulnerabilities and Solutions* [14]. Autor zde uvádí i několik obecných řešení pro zmiňované zranitelnosti.

Bezpečností sítí Smart Grid se také věnují dokumenty vydané různými bezpečnostními společnostmi a agenturami. Dokument *Smart Grid Security* [15] od agentury ENISA popisuje potenciální cíle útoků a rizika, která se jich týkají. Dokument také obsahuje kategorizaci možných hrozeb. Dokument organizace NIST [8] popisuje množství konkrétních požadavků na bezpečnost, v další části jsou popsány možné zdroje bezpečnostních hrozeb.

2 ROZVODNÁ ELEKTRICKÁ SÍŤ

Stávající distribuční sítě byly budovány s primárním cílem přenést elektrickou energii od elektrárny k zákazníkům. Topologie sítě počítá pouze s jednosměrným tokem elektrické energie. Proces začíná výrobou el. energie v elektrárnách, dále pokračuje přes přenosovou a distribuční soustavu ke koncovým zákazníkům. Klasický model soustavy je znázorněn na obrázku 1.



Obrázek 1 – Klasický model přenosové soustavy [5]

Připojování dalších zdrojů elektřiny do sítě na straně zákazníka přináší síti problémy v podobě ztrát při transformaci nn (nízké napětí) na vn (vysoké napětí), snížené kvality dodávky elektrické energie (vliv vyšších harmonických) a nemožnost efektivně řídit tyto zdroje [5, 6].

2.1 SCADA

Systémy SCADA (supervisory control and data acquisition) představují stávající model dohledových a řídících systémů. V řídících centrech, elektrárnách se může nacházet i několik samostatných SCADA systémů [2].

Model SCADA se obvykle skládá z následujících komponent:

- rozhraní HMI (human machine interface) – rozhraní pro obsluhu systémy lidmi,

- SCADA server – uchovává data a řídí ostatní činnosti,
- jednotky RTU (remote terminal unit) – vzdálené terminály, předávají data od lokálních senzorů a přeposílají je do SCADA serveru,
- jednotky PLC (programmable logic controller), IED (intelligent electronic device) – senzorické a akční prvky,
- komunikační infrastruktura – slouží k propojení jednotlivých částí.

Rozhraní HMI v hlavním řídícím místě informuje o stavu celého systému, obnovovací frekvence dat je okolo dvou až deseti sekund.

Pokud se systém nachází ve stabilním stavu a systémy SCADA slouží především pro informaci o stavu systému, je několikasekundová latence přijatelná. Při haváriích na elektrické síti však může být taková latence příliš vysoká pro včasné reagování a předcházení výpadků. Stávající SCADA systémy z velké části ponechávají rozhodovací proces na lidech a nevykonávají rozhodovací proces samostatně.

SCADA systémy využívají různé komunikační protokoly. Mezi zastaralé protokoly využívané v SCADA systémech patří Modbus RTU, RP-570, Profibus nebo Conitel. V novějších systémech se využívají standardizované protokoly IEC 60870-5-101/104, IEC 61850 a DNP3. Většina novějších protokolů již podporuje komunikaci přes TCP/IP.

Propojování SCADA systémů s počítačovými sítěmi vede také k možnostem útoku na tyto systémy a způsobení rozsáhlých škod.

3 SMART GRID

Stávající rozvodné sítě pomalu již nevyhovují dnešním nárokům na kvalitu, efektivitu a spolehlivost zásobování elektrickou energií. Přestože fungují spolehlivě, pro další rozvoj je nutná celková modernizace. Sítě Smart Grid představují evoluci el. rozvodné sítě a přinášejí několik základních součástí [1, 37]:

- integrovaná obousměrná komunikace;
- pokročilé komponenty a metody řízení;
- senzorické a měřící technologie;
- vylepšená rozhodovací podpora.

3.1 Komponenty

3.1.1 Integrovaná obousměrná komunikace

Obousměrná komunikace umožní operátorům monitorovat a spravovat jednotlivé součásti sítě v reálném čase. V každém okamžiku bude dostupná informace o stavu sítě a jejích jednotlivých částí.

Obousměrná komunikace také umožní automatické odečítání stavu elektroměrů u zákazníků a okamžitou reakci na aktuální spotřebu v síti (technologie AMI). Tato funkčnost umožní optimalizovat vyráběné množství elektrické energie a snížit tak její cenu v době mimo špičku.

Pro lepší rozložení zatížení sítě je možné připojit distribuované energetické zdroje (elektrárny z obnovitelných zdrojů, elektromobily). Pomocí komunikační infrastruktury je možné je využít v době špičky či při výpadku některých bodů distribuční soustavy k dodávce el. proudu.

3.1.2 Senzorické a měřící technologie

Zavedení technologie AMI (advanced metering infrastructure) a AMR (automated meter reading) vyžaduje u zákazníků tzv. chytrý elektroměr („smart meter“). Ten umožňuje vzdálené odečítání stavu a další pokročilé funkce. Namísto každoročního odečtu stavu pracovníkem firmy budou informace o aktuální spotřebě zákazníka odesílány skrze

komunikační síť v téměř reálném čase (s periodou vzorkování maximálně několika desítek minut).

3.1.3 Pokročilé komponenty a metody řízení

Mezi pokročilé komponenty patří senzory, akční prvky (relé, aj.), které je možné řídit na dálku, el. banky pro shromáždění nadbytečné el. energie (generované například z obnovitelných zdrojů).

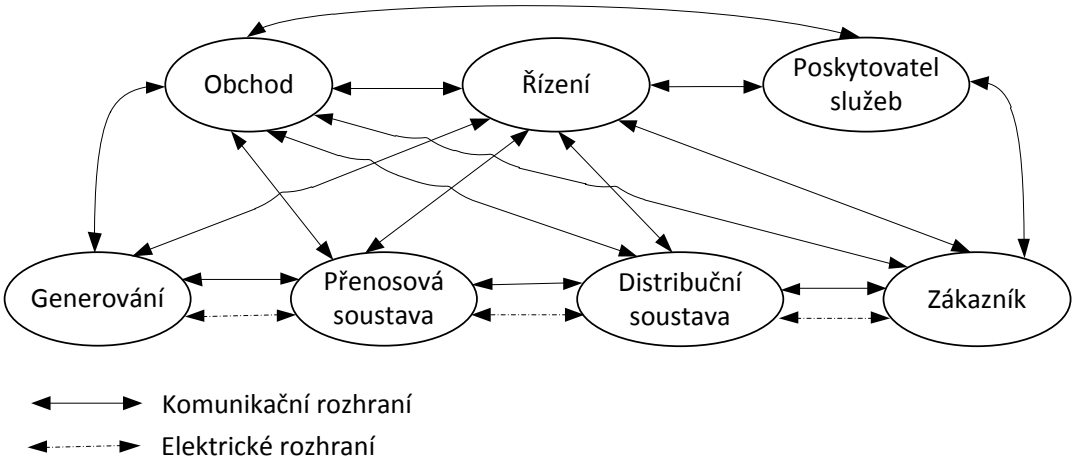
Řízení Smart Gridu může být více automatizované. Dostupnost obousměrné komunikace a senzorů na síti umožní automatická a rychlá rozhodnutí pro udržení stabilní sítě. Topologii distribuční soustavy je tak možné upravovat v reálném čase dle potřeby a výskytu poruch. Distribuované energetické zdroje mohou poskytovat elektrickou energii v místech, která budou zcela odpojena od distribuční soustavy. V případě výskytu poruch ohrožujících celou síť je možné danou část sítě zcela izolovat (tzv. ostrovní režim).

Technologie DR (demand response) umožňuje optimalizovat zatížení sítě. Energetické společnosti mohou na dálku ovládat energeticky náročné spotřebiče (ohřev vody, klimatizace aj.) a v případě vysokého zatížení sítě je vypnout nebo snížit jejich spotřebu, jejich činnost tak může být odložena do období s nižším zatížením sítě [31, 32].

3.2 Konceptuální model

Pro potřeby definování Smart Grid byl vytvořen konceptuální model, který následně přijala organizace NIST, další organizace (IEC, ECR, aj.) a standardy využívají tento model.

Architektura Smart Grid je rozdělena do sedmi základních domén, mezi nimiž existuje komunikační anebo elektrické propojení. Model vychází ze současné topologie elektrických sítí a rozšiřuje jej o domény obchodu, řízení a poskytovatelů služeb. Model je zobrazen na obrázku 2.

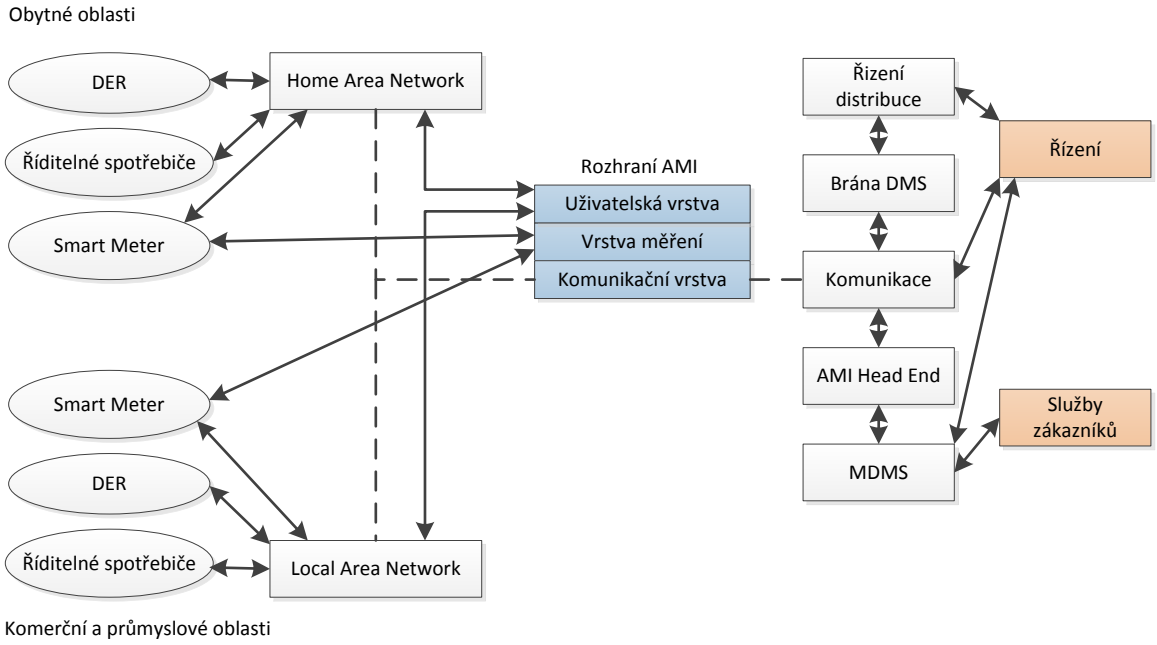


Obrázek 2 – Konceptuální model Smart Grid [5]

3.3 AMI

Technologie AMI (advanced metering infrastructure) přináší rozšířené možnosti měření odběru elektrické energie v síti, jejím cílem je poskytovat lepší kontrolu a správu spotřeby elektrické energie.

Pro svoji činnost vyžaduje komunikační síť, která spojí zákazníky, elektrárny, energetické společnosti a další prvky, které zasahují do elektrické sítě. Tato komunikační síť zahrnuje rozsáhlé území a mnoho uživatelů. Pro její vybudování je možné využít širokou škálu komunikačních technologií a protokolů. Jedním z hlavních problémů AMI jsou náklady na vybudování takto rozsáhlé sítě a zajištění kompatibility mezi různými komponentami sítě (naznačeny na obrázku 3) [1].



Obrázek 3 – Komponenty AMI [4]

Do základních komponent systému AMI patří:

- měřící zařízení – smart meter,
- sběrné zařízení – agregační zařízení, které získává data ze smart meterů a přeposílá je dále,
- MDMS (meter data management system) – řídící systém.

3.3.1 Smart meter

Standardní dnes používané elektroměry jsou nahrazeny tzv. „smart metery“, které kromě měření spotřeby elektrické energie umožňují zaznamenaná data odesílat do energetické společnosti. Podporována je obousměrná komunikace s centrálou.

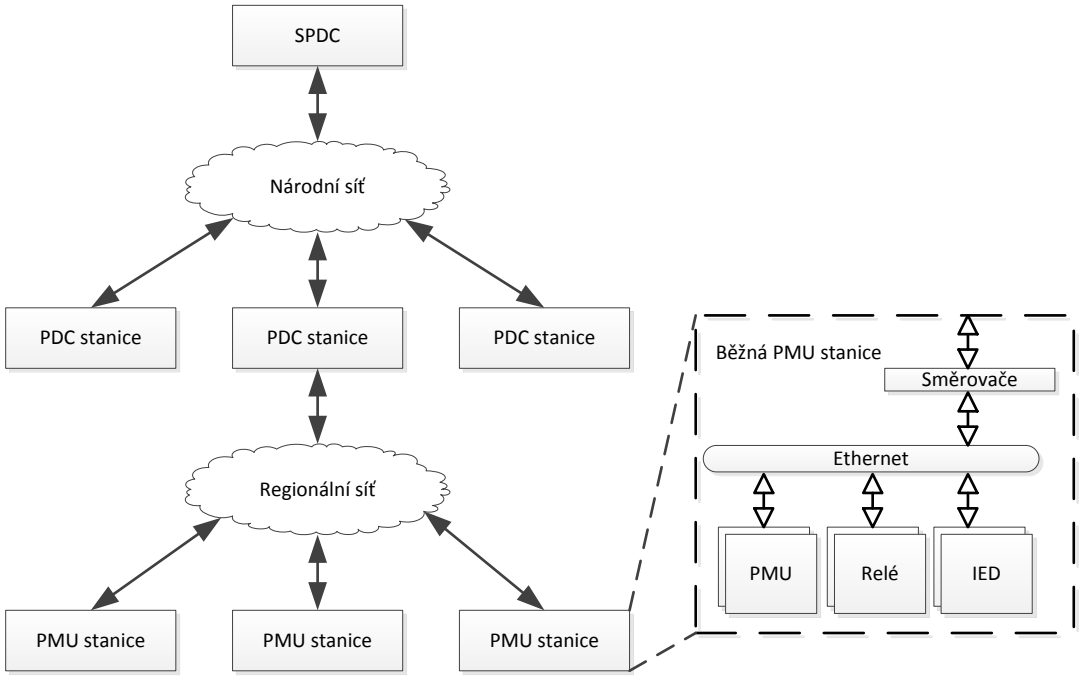
Pro komunikaci se využívají různé protokoly:

- ANSI C12.18, C12.19, C12.21, C12.22 – využívané především v Severní Americe,
- IEC 61107, 62056 – protokoly vytvořené komisí IEC, využívané především v Evropské Unii,
- Open smart grid protocol – protokoly publikované institutem ETSI, používány celosvětově.

Pro připojení do sítě se využívají především různé druhy rádiových technologií nebo technologie PLC (power line communications).

3.4 WAMS

Pro analýzu stavu elektrické sítě se využívají stávající systémy SCADA a novější systémy WAMS (wide area measurement system). Systémy WAMS analyzují v reálném čase stav celé elektrické sítě, tím je umožněno efektivně reagovat na případné poruchy v různých částech sítě [21].



Obrázek 4 – Architektura WAMS systému [1]

Systém se skládá z několika základních komponent:

- řídící centrum (SPDC – super phasor data collector) – slouží pro analýzu dat, vyhodnocení a zobrazení výsledků;
- PMU (phasor measurement unit, synchrofázor) – měří veličiny na elektrickém vedení a odesílá je do nadřazeného zařízení PDC;
- PDC (phasor data collector) – sbírá data z jednotlivých senzorů a následně je odesílá do řídícího centra.

Zařízení PDC shromažďuje měření z více jednotek PMU, data jsou kontrolována na chyby a sjednocena dle časových razítek. Zpracovaná data jsou následně odeslána do nadřazeného PDC nebo do řídícího centra (SPDC).

Pro přenos dat se využívá především protokolů UDP a IP přes sériové linky, mikrovlnné spoje, sítě VPN či Ethernet [33].

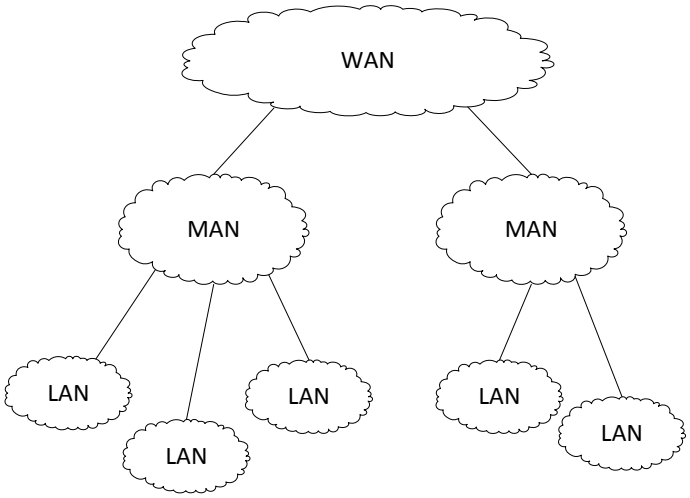
Data ze systému WAMS slouží k vyhodnocení stavu celé elektrické rozvodné sítě. Na jejich základě je možné automatizovat řízení sítě a odesílat příkazy pro relé a další zařízení typu IED. Datová síť musí zajistit bezpečný a spolehlivý přenos dat.

4 TOPOLOGIE DATOVÉ SÍTĚ

Topologie datové sítě Smart Gridu se odlišuje od klasických datových sítí, ale využívá se zde podobný hierarchický přístup k organizaci sítě. V následující kapitole je představen hierarchický model klasických datových sítí a přístup sítí Smart Grid.

4.1 Klasické datové sítě

V klasických datových sítích se sítě nejčastěji rozdělují dle velikosti do kategorií LAN (local area network), MAN (metropolitan area network), WAN (wide area network) a Internet. LAN sítě představují nejmenší sítě, skládající se obvykle z desítek až stovek počítačů v rámci jedné budovy. Termín MAN označuje metropolitní sítě a je reprezentován městem či kampusem, který sdružuje více LAN sítí a připojuje je k WAN. WAN sítě spojují vzdálená místa, Internet představuje veřejnou celosvětovou WAN síť. Hierarchie je znázorněna na obrázku 5.



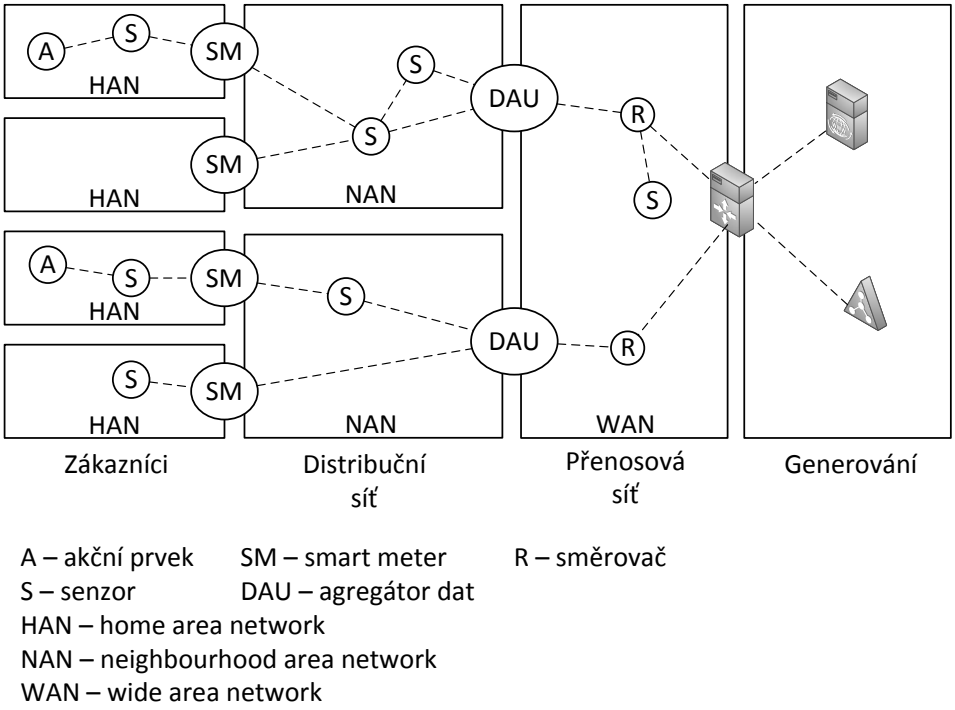
Obrázek 5 – Hierarchie klasických datových sítí [5]

4.2 Topologie Smart Grid

V sítích Smart Grid je nejmenším logickým blokem domov či budova zákazníka, jednotlivé zařízení uvnitř budovy patří do sítě HAN (home area network). Budovy v sousedství jsou sdružovány do sítí NAN (neighbourhood area network), které se napojují do rozsáhlých WAN sítí, které poskytují připojení do sítí energetických společností.

Do komunikační sítě jsou také zahrnuty další entity (poskytovatelé služeb, aj.), které představují externí úroveň.

Příklad jednotlivých oblastí a obsažených zařízení je zobrazen na obrázku 6.



Obrázek 6 – Komunikační infrastruktura sítí SmartGrid [1]

4.2.1 Home area network

Home area network představuje nejmenší topologickou část Smart Grid sítě, někdy bývá také označována jako premise area network (PAN) nebo building area network (BAN). HAN poskytuje prostředí pro řízení spotřeby elektrické energie, zvýšení efektivity a zapojení zákazníka do procesu výroby elektrické energie.

V HAN sítí se nachází smart meter a také další zařízení, schopná využívat možností správy spotřeby elektrické energie [2]. Mezi HAN zařízení také patří:

- PCT (programmable communicating thermostat, programovatelný komunikační termostat) – termostat sloužící pro řízení topení a ventilace, umožňuje také komunikaci se službou PowerMeter od společnosti Google aj.,
- IHD (inhome display, domácí displej) – spolu s EMS rozšiřuje poskytované služby klasických termostatů, umožňuje řízení chytrých spotřebičů v domácnosti,
- EMS (energy management system) – systém pro správu spotřeby energie,

- PEV (plug-in electric vehicle, připojitelné elektrické vozidlo) – elektrické vozidlo schopné nabíjet se ze sítě, v případě potřeby může fungovat i jako zdroj elektrické energie.

Jednotlivá chytrá zařízení v síti HAN využívají ke komunikaci drátové technologie (PLC, BACnet protokol) a také rádiové technologie (Wi-Fi, ZigBee).

4.2.2 Neighbourhood area network

Sítě NAN představují oblasti sousedství a připojují pod sebe jednotlivé HAN sítě. NAN představuje agregační místo pro připojení většího množství domácností, k vlastní agregaci a jako komunikační rozhraní slouží zařízení DAU. DAU následně přeposílá data od jednotlivých zákazníků do sítě WAN [20].

V síti NAN se typicky používají technologie PLC, ANSI C12 protokoly, WiMAX, či ZigBee.

4.2.3 Wide area network

WAN obdobně jako v klasických datových sítích představuje rozsáhlou síť, která propojuje jednotlivé sítě NAN a HAN do podnikové sítě energetické společnosti.

WAN sítě mohou být založeny na mnoha různých technologiích, například Ethernet, mobilní sítě, broadband připojení (MPLS, ...).

4.2.4 Podnikové sítě

Veškerá data získaná na nižších vrstvách sítě jsou přeposílána do podnikových sítí, kde jsou následně analyzována. Nacházejí se tu také servery a řídící centra pro technologie SCADA a WAMS.

Pro komunikaci uvnitř podnikových sítí se využívá Ethernet a spoje realizované pomocí kroucené dvojlinky a optických vláken.

4.2.5 Externí entity

Mezi externí entity jsou zahrnuti obchodníci s elektrickou energií, poskytovatelé služeb a další subjekty, kteří zasahují do procesů souvisejících s dodávkou elektrického proudu

(technická podpora zákazníků, aj.). Externí entity mohou poskytovat různé služby a procesy pro zákazníky (fakturace, tarifikace, ...).

4.3 Síťová vrstva

Úkolem síťové vrstvy dle OSI modelu je adresace stanic a zajištění přeposílání datagramů. V prostředí Smart Grid sítě se střetává mnoho různých technologií a je potřeba vytvořit sjednocující vrstvu, která zajistí kompatibilitu [19, 22].

Vhodnou volbu představuje internetový protokol (IP), který je v dnešní době využívá pro realizaci většiny počítačových sítí a celosvětové sítě internet. IP představuje nespojový protokol, který nezaručuje spolehlivost přenosu dat (tato funkcionalita může být zajištěna protokoly vyšších vrstev).

IP protokol je v současnosti převážně zastoupen verzí IPv4. V poslední době se začíná nasazovat protokol IPv6, který přináší větší adresní prostor, podporu mobility, bezpečnostní služby aj. V prostředí Smart Grid sítí se předpokládá velké množství zařízení, i proto se protokol IPv6 jeví jako lepší varianta. Některá stávající zařízení však nemusejí IPv6 plně podporovat, proto je pravděpodobné využití obou protokolů IPv4 i IPv6 při budování sítě.

4.4 Transportní vrstva

Transportní vrstva slouží k přenosu dat aplikací a zajišťuje požadovanou spolehlivost přenosu. V sadě IP existují dva základní protokoly transportní vrstvy – transmission control protocol (TCP) a user datagram protocol (UDP).

TCP je spojovým protokolem, který zajišťuje spolehlivost přenosu dat. V případě ztráty dat, jsou data automaticky opětovně poslána přes síť. TCP je náročnější na prostředky a má vyšší režii při přenosu dat.

UDP je nespojovým protokolem, který nezajišťuje spolehlivé doručení dat. Vzhledem ke své jednoduchosti má nižší režii při přenosu dat. UDP také podporuje vícesměrové zasílání dat (tzv. multicast). Jeden paket je možné zaslat najednou více příjemcům.

V sítích Smart Grid může být požadováno spolehlivé spojení, ale také rychlé „nespolehlivé“ spojení, využity budou oba protokoly dle požadavků v dané oblasti.

5 KOMUNIKAČNÍ TECHNOLOGIE

Budoucí sítě Smart Grid budou využívat širokou škálu technologií a přenosových médií. V závislosti na podmínkách prostředí a požadavcích na kvalitu a vlastnosti spojení je k dispozici několik způsobů přenosu signálu po drátových spojích nebo rádiově. V následující kapitole jsou představeny technologie, které mohou být využívány ve Smart Grid sítích.

5.1 Drátové technologie

5.1.1 Power-line communications

Technologie PLC využívá k přenosu dat elektrické vedení, datový signál je namodulován na nosnou vlnu. Hlavní výhodou technologie je využití stávajících elektrických linek. Není tak nutné budovat nová spojení nebo tvořit paralelně s vedením samostatnou datovou síť. PLC se již v elektrických sítích využívá delší dobu, nízkokapacitní spoje jsou využívány ke vzdálenému řízení některých zařízení [23, 25].

Přenos dat přes elektrickou síť přináší několik zásadních problémů:

- elektrické vedení představuje silný zdroj rušení, linky obvykle nejsou stíněné a negativně tak působí na signál i elektromagnetická interference,
- vedení signálu přes transformátory je nutné přemostit (kromě nízkých frekvencích),
- volba vhodných frekvenčních kanálů může být problematická, podmínky v různých částech sítě se mohou značně měnit,
- při přerušení vedení dojde ke ztrátě spojení, kritické části sítě musí disponovat záložní konektivitou,
- dosažené přenosové rychlosti nemusí být dostatečné.

PLC představuje sdílené komunikační médium, pro zachování důvěrnosti dat je nutné použít šifrování.

5.1.2 Kroucená dvojlinka

Kroucená dvojlinka zcela nahradila zastaralou technologii koaxiálních kabelů. Kroucení párů vodičů snižuje vliv okolního elektromagnetického rušení a přeslechy mezi vodiči.

V dnešní době se tento typ kabeláže nejvíce využívá pro domácí, kancelářské a budovní sítě. V místech s vyššími nároky na přenosové rychlosti, vzdálenost a odolnost na rušení se preferují optická vlákna [1].

Dle použitého typu kabeláže (kat. 5, 6, a další) se na kroucené dvojlince dosahuje přenosových rychlostí 100, 1000 nebo 10000 Mb/s. Maximální délka kabelu je omezena na 100 metrů.

Spojení je pouze dvoubodové, pro zapojení více počítačů do společného síťového segmentu se využívají přepínače.

5.1.3 Optická vlákna

Optická vlákna využívají k přenosu dat transformaci elektrického signálu na světelné záření. Světlo putuje skrze optické vlákno na jehož konci je detektor, který signál transformuje zpět na elektrický signál. Optické spoje se již na některých místech (páteřní spoje budov, spoje na velkou vzdálenost) v elektrické síti využívají [1].

Optická vlákna disponují přenosovou kapacitou od jednotek gigabitů za sekundu až po 40 – 1600 Gb/s s využitím technologie WDM (wavelength-division multiplexing).

Přenos pomocí světelného záření není nijak ovlivněn rušením z vnějšího elektrického pole, optická vlákna mohou být pokládána v blízkosti vedení vysokého napětí, transformátorů nebo kolejí. Mezi optickými vlákny nevzniká problém přeslechů a utlumení signálu je mnohem nižší než na vedeních využívající elektrické signály. Opakovače signálu jsou potřeba na každých 100 – 1000 kilometrech (dle použité technologie).

Největší nevýhodou optických vláken je jejich vysoká pořizovací cena. Vybudování rozsáhlé infrastruktury s využitím optických spojů je finančně velmi nákladné.

Optická vlákna představují dvoubodové spojení a není je možné odposlouchávat bez přerušení vedení.

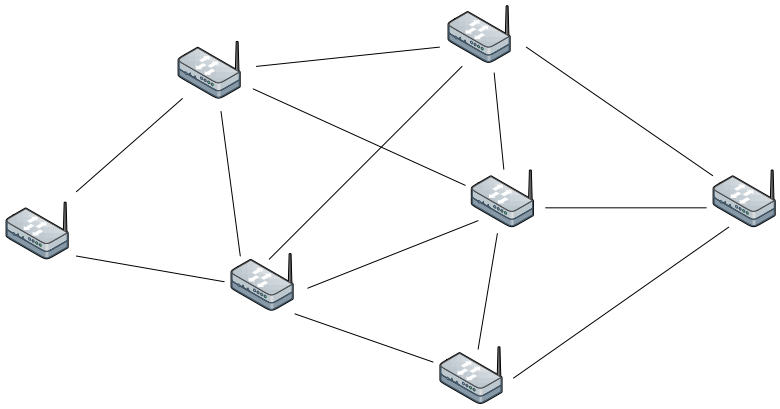
5.2 Rádiové technologie

Rádiové technologie využívají k přenosu signálu elektromagnetického záření o různých frekvencích. Dnešní technologie dosahují vyšších přenosových rychlostí i dostatečného pokrytí. Bezdrátové technologie poskytují vyšší flexibilitu, pro připojení nových zařízení není nutné instalovat novou kabeláž.

Společnou nevýhodou všech rádiových technologií je citlivost na elektromagnetické rušení či rušení z jiných sítí využívající stejná frekvenční pásma.

Bezdrátové sítě je možné rozdělit na dvě skupiny dle způsobu organizace:

- strukturované – využívají centrální přístupové body (nazývané BS, AP, aj.), které řídí jednotlivé klienty a komunikace probíhá skrze přístupové body,
- mesh – využívají decentralizovaný přístup; jednotlivé prvky sítě navazují spojení s blízkými prvky a předávají si zprávy přímo mezi sebou (příklad topologie na obrázku 7).



Obrázek 7 – Příklad topologie bezdrátové sítě typu mesh

5.2.1 ZigBee

Protokol ZigBee je tvořen skupinou ZigBee Alliance a představuje řešení pro bezdrátové přenosy na krátkou vzdálenost s nižším datovým tokem. ZigBee je definován standardem IEEE 802.15.4 [1].

Pro přenos dat se využívají nelicencovaná pásma – 868 MHz v Evropě, 915 MHZ v USA a Austrálii a 2,4 GHz celosvětově. Přenosové rychlosti dosahují 20 kb/s, 40 kb/s a 250 kb/s.

ZigBee rozlišuje tři typy zařízení:

- koordinátor – pracuje jako most do dalších sítí, řídí autentizační proces a bezpečnostní klíče a vystupuje jako kořen ve stromové topologii,
- směrovač – přeposílá data přijatá od ostatních zařízení, může také sloužit i jako koncové zařízení,
- koncové zařízení – umí odesílat data pouze směrovačům a koordinátorovy.

Technologie ZigBee podporuje směrování a adresaci využitím stromové a mesh topologie. Původní ZigBee standard z roku 2004 nepodporuje IP a nebyl dobře škálovatelný. Novější standard ZigBee PRO z roku 2007 řeší problém škálovatelnosti zavedením 16ti bitového adresování. Nativní podporu IPv6 adresace přináší standard ZigBee IP (představen v roce 2013).

ZigBee je vhodnou technologií k tvoření bezdrátových senzorických sítí (WSN). Jako další možné využití se předpokládá bezdrátové propojení zařízení v domácnostech.

5.2.2 Wi-Fi

Wi-Fi představuje protokoly založené na standardech IEEE 802.11. Používá se především pro budování domácích a kancelářských sítí nebo k poskytování připojení k internetu na kratší vzdálenosti. Wi-Fi podporuje IP protokoly, o certifikaci zařízení se stará organizace Wi-Fi alliance [1].

Wi-Fi pracuje v pásmu 2,4 GHz (standardy 802.11 b, g, n) a 5 GHz (802.11 a). Lze teoreticky dosáhnout přenosových rychlostí 54 Mb/s až 300 Mb/s. Dosah Wi-Fi sítě od přístupového bodu je okolo 30 metrů v budově a 100 metrů mimo budovu.

Kromě vlastních protokolů popisující přenos dat, zahrnuje rodina protokolů 802.11 také protokoly:

- standard 802.11i – definice šifrování WPA2,
- standard 802.11s – definuje mesh sítě,
- standard 802.11e – podpora QoS.

Wi-Fi sítě představují atraktivní volbu pro budování sítí krátkého dosahu. Wi-Fi je optimalizováno pro vysoké přenosové rychlosti, proto zařízení spotřebovávají více elektrické energie než je například spotřeba zařízení využívajících ZigBee [27, 28].

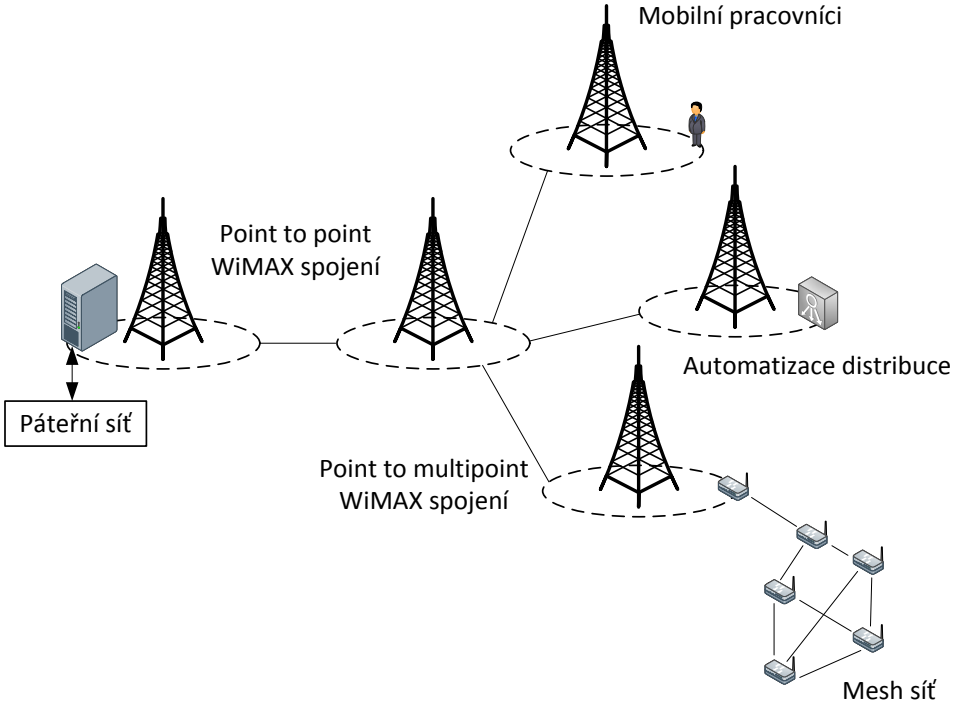
5.2.3 WiMAX

Technologie WiMAX je založena na standardech IEEE 802.16, produkty využívající WiMAX jsou certifikovány organizací WiMAX Forum [24, 30].

Technologie poskytuje přenosové rychlosti až 140 Mb/s s nízkou latencí (10–50 ms). Podporovány jsou jak fixní spojení (IEEE 802.16d), tak mobilní spojení (IEEE 802.16e).

WiMAX je možné využít pro spoje na dlouhou vzdálenost, více jak 20 km v předměstských oblastech.

WiMAX pracuje v širokém rozsahu frekvencí od 2 do 66 GHz. Na rozdíl od jiných mikrovlnných technologií mohou WiMAX spoje fungovat v podmínkách bez přímé viditelnosti koncových bodů. Podporovány jsou spoje typu point-to-point a point-to-multipoint.



Obrázek 8 – Příklad topologie využívající WiMAX technologii [1]

Některé energetické společnosti již začaly zahrnovat technologii WiMAX do plánovaných Smart Grid sítí.

5.2.4 Mobilní sítě

Mobilní sítě poskytují bezdrátové připojení pro velké množství uživatelů v rozsáhlých oblastech. Oblasti jsou děleny do menších částí, označovaných jako buňky. Každá buňka obsahuje zařízení zvané „base transceiver station“ (BTS, či BS), které komunikuje a řídí všechna zařízení komunikující uvnitř buňky. Základní předpoklad návrhu mobilních sítí předpokládá, že signál z BTS a zařízení uživatelů je omezen pouze na jedinou buňku. Jednotlivé rádiové kanály jsou tak opětovně používány v dalších buňkách. Mobilní sítě

disponují téměř globálním pokrytím a s využitím technologií 3. a 4. generace poskytují i dostatečné přenosové rychlosti pro datová spojení [26].

Technologie 3GPP LTE představuje další rozšíření 3G UMTS sítí. LTE zachovává zpětnou kompatibilitu s 3GPP standardy, pro přenos dat se využívá technologie MIMO a přístupové metody OFDMA. Teoretická přenosová rychlost LTE dosahuje až 300 Mb/s.

Dokument NIST PAP 2 [29] obsahuje analýzu pokrytí a kapacity pro provoz Smart Grid AMI s využitím LTE sítí.

5.2.5 Satelitní komunikace

Satelitní technologie poskytuje připojení i do velmi odlehlých lokací bez nutnosti instalace kabeláže nebo přenosových stanic. Satelitní připojení je možné jednoduše realizovat instalací satelitní antény s modemem [23].

Satelity se rozdělují do tří kategorií dle výšky oběžné dráhy kolem Země. Jedná se o geostacionární oběžnou dráhu (GEO), střední oběžnou dráhu (MEO) a nízkou oběžnou dráhu (LEO). Jednotlivé kategorie se odlišují vlastnosti, ale i technickými omezeními.

Satelity GEO obíhají Zemi ve výšce 35 786 km, jejich velkou výhodou je stálá poloha pro pozorovatele z povrchu Země. Pro realizaci připojení stačí fixní anténa. Velká vzdálenost od povrchu negativně ovlivňuje výkon spoje, jednosměrná latence spoje je okolo 250 ms. Některé síťové protokoly, jako je TCP nebo VPN spojení, v prostředí s vysokou latencí nemusejí dobře fungovat. Satelity LEO Zemi obíhají ve výšce 160–2000 km nad povrchem a poskytují podstatně nižší latence okolo 40 ms, pro udržení spojení je ale potřeba síť satelitů.

Satelitní spoje vyžadují přímou viditelnost a jsou velmi ovlivňovány počasím. Přes své nevýhody poskytuje satelitní technologie cenově výhodnou variantu pro připojení vzdálených lokací nebo jako záložní spojení.

5.3 Internet

Celosvětová síť internet představuje jednu z dalších možností při navrhování Smart Grid sítě. Její výhodou je cenová dostupnost a již existující vysokorychlostní páteřní síť. Internet však představuje sdílené médium a negarantuje rychlost, latenci nebo i dostupnost [23].

Pro zajištění bezpečného přenosu a dosažení záruky kvalit linky je možné využít VPN technologie. VPN vytváří virtuální privátní síť a poskytuje tak bezpečné komunikační médium.

Přesto používání VPN přes internet naráží na několik dosud nevyřešených problémů, jako je efektivní směrování, správa zdrojů nebo správa vzdálených sítí, které mohou být potřeba pro efektivní využívání v rámci Smart Grid sítí.

6 BEZPEČNOST SMART GRID

Cílem Smart Grid je poskytnout spolehlivou, efektivní a bezpečnou distribuci elektrického proudu. Toho se dosahuje zavedením obousměrné komunikace mezi elektrárnami a zákazníky a integrací moderních informačních technologií. Elektrická síť postupně přejde ze zastarávajících systémů na běžnější osobní počítače, operační systémy Microsoft Windows či Linux a síťovou infrastrukturu postavenou nad protokolem IP. Zavádění nových systémů a komunikačních kanálů ovšem otevírá nová možná bezpečnostní rizika [37].

V minulosti se již stalo několik případů, kdy došlo k napadení elektrické sítě prostřednicím zranitelností v softwaru [34]. V článku Gormana [38] se uvádí, že hackeři byli schopni vložit software do elektrické sítě USA, který potenciálně umožňoval narušení sítě. Dle Krebse [40] aplikací špatné aktualizace softwaru vedlo k nouzovému odstavení jaderné elektrárny v Georgii, které trvalo dva dny.

V nedávné době došlo k rozšíření červa zvaného Stuxnet, který cílil na systémy SCADA od společnosti Siemens. Využitím některých zranitelností dokázal převzít řídící a monitorovací procesy v PLC zařízeních. Dne 29. listopadu 2010 Irán potvrdil, že jejich jaderný program byl poškozen červem Stuxnet. Dle některých teorií byl červ vytvořen v USA a Izraeli s cílem poškození jaderných zařízení v Íránu [39].

Moderní systémy řídící elektrickou síť doposud nebyly vystaveny takovému riziku napadení zvenčí a nedisponují bezpečnostními mechanismy jako klasické IT systémy. Proto je nutné se zaměřit jejich zabezpečení již při jejich návrhu. V následující kapitole jsou popsány obecné bezpečnostní termíny a problematika hrozeb a útoků v IT systémech.

6.1 Bezpečnostní organizace

V současnosti se bezpečností sítí Smart Grid zabývají skupiny různého charakteru [3]:

- vlády států, státní (bezpečnostní) organizace,
- nadnárodní skupiny a organizace,
- soukromé organizace.

6.1.1 ENISA

European Network and Information Security Agency (ENISA) spadá pod správu Evropské unie. Organizace byla založena v roce 2004 a plně začala fungovat od 1. září 2005.

Cílem organizace je zlepšování síťové a informační bezpečnosti v rámci Evropské unie. V rámci sítí Smart Grid ENISA vypadala několik doporučení ke zvýšení bezpečnosti. Další doporučení byla vydána pro řídící a SCADA systémy.

6.1.2 Federální vláda USA, DOE, FERC

Bezpečnost elektrické sítě úzce souvisí s bezpečností státu, proto vlády významně zasahují do správy elektrické sítě a mohou zákony ovlivnit, jaké technologie a postupy budou dovoleny či zakázány. V USA vláda reguluje energetický průmysl již od roku 1920. V počátcích se jednalo o ne příliš dobře organizovaný přístup ke správě, později v roce 1977 bylo ustanoveno ministerstvo energetiky (DOE). Současně s DOE byla ustanovena federální komise pro regulaci energetiky (FERC) [3].

V roce 2007 vstoupil v platnost zákon Energy and Independence Security Act (EISA), který oficiálně podpořil modernizaci elektrické sítě a zároveň ustanovil nové pracovní skupiny, které se týkají sítí Smart Grid.

6.1.3 NERC

North American Electric Reliability Corporation (NERC) je nezisková organizace založená v roce 2006. Jejím úkolem je zajištění spolehlivosti elektrické soustavy. Organizace spolupracuje na vývoji standardů, poskytování školení a v dalších činnostech.

Společnost NERC vytvořila koncept Critical infrastructure protection (CIP), který pokrývá několik různých sektorů (bankovnictví, doprava, energetika, ...) a definuje bezpečností politiky. Zabývá se například identifikací kritických prvků, vyhodnocení jejich rizik, postupy při vzniku incidentů a jejich odstraňování.

Na základě konceptu CIP vznikly podobné programy i v dalších státech. V Evropské Unii se jedná o European Programme for Critical Infrastructure Protection (EPCIP).

6.2 Hrozba

Hrozbou se v počítačové bezpečnosti označuje událost, která může mít negativní dopad na zařízení či služby. Negativní dopad může být ve formě neoprávněného přístupu, zničení, odhalení, modifikací dat, zamezení dostupnosti služby či zařízení [15].

Hrozby je možné rozdělit do dvou základních kategorií:

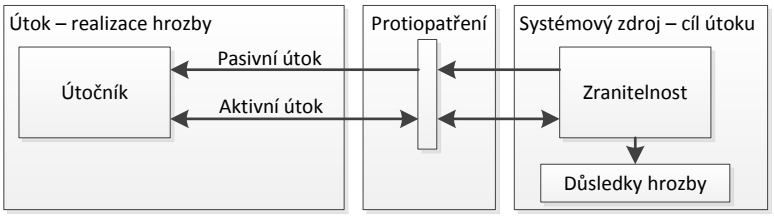
- záměrné (inteligentní) – úmyslné provedení činnosti s cílem poškození systému hackerem, či kriminální organizací,
- náhodné – náhodné chyby či nehody (selhání vybavení), zásahy „vyšší moci“ (počasí, přírodní jevy).

Záměrné hrozby mohou využívat zranitelností v systémech. Zranitelnost představuje slabinu, kterou je možné zneužít. V softwaru se může jednat o špatné ošetření vstupů, chyby v algoritmech aj.

Záměrné i náhodné hrozby existují v každém systému a je nutné s nimi počítat a připravit se na ně (management rizik). Nelze však eliminovat veškeré hrozby a dosáhnout dokonalého systému.

6.3 Útok

Útok představuje realizaci konkrétní hrozby. Jedná se o čin, při kterém se útočník pokouší získat přístup, poškodit či nějak narušit systém nebo jeho součásti.



Obrázek 9 – Schéma útoku[1]

Útoky je možné rozdělit na aktivní či pasivní:

- aktivní útok – pokus o změnu systémových prostředků nebo ovlivnění funkčnosti,

[1]RFC 2828: Internet Security Glossary. SHIREY, R. *Internet Engineering Task Force* [online]. 2000 [cit. 2013-05-10]. Dostupné z: http://tools.ietf.org/html/rfc2828

- pasivní útok – pokus o získání informací ze systému nebo jejich využití, neovlivňuje systémové prostředky.

Dle polohy útočníka je možné útoky rozlišovat na:

- vnitřní – útok je zahájen uvnitř systému,
- vnější – útok je zahájen vně systému (např. přes internet).

Úspěšná realizace útoku vede k narušení činnosti systému a může narušit dostupnost, důvěrnost či integritu systému nebo jeho některých částí.

6.3.1 Útočník

Útočníkem může být každý jednotlivec nebo skupina, která se pokusí o útok na systém. Útočníkem můžou být nezkušení uživatelé (tzv. script kiddie), profesionální hackeři, zaměstnanci, zákazníci, konkurenti nebo teroristé. Podle jejich motivace je možné útočníky rozlišit na:

- Neškodící útočníci – útočníci, kteří hledají chyby a považují prolomení systému za výzvu. Nemají snahu poškodit systém, pouze jej prolomit.
- Zákazníci – jejich cílem může být poškození jiných zákazníků (odpojení od přívodu elektrického proudu) nebo vlastní obohacení (snížení výdajů za el. proud).
- Teroristé – jejich cílem je poškodit rozsáhlou část systému a způsobit tak masivní problém (zasažení velkého množství zákazníků).
- Zaměstnanci – zaměstnanci se mohou chtít mstít společnosti nebo způsobovat problémy jejich neopatrným chováním.
- Konkurenti – jejich cílem je finanční zisk.

6.4 Dostupnost, důvěrnost, integrita, účetnictví

Trojice dostupnost, důvěrnost a integrita představuje jeden ze základních principů informační bezpečnosti. Tento model je někdy rozšiřován i o další prvky jako je účetnictví, neodvolatelnost, autentizace [15].

Hrozby a útoky způsobují narušení těchto základních principů. Útok může narušit jeden nebo i více principů najednou.

6.4.1 Důvěrnost

Důvěrnost (confidentiality) znamená, že data jsou ochráněna před jejich odhalením cizím osobám. Zajištění důvěrnosti vyžaduje ochranu dat při jejich přenosu i při jejich uchovávání. Zachování důvěrnosti je důležité pro zachování soukromí uživatelů.

Energetické společnosti mohou uchovávat mnoho údajů o svých zákaznících (a to včetně osobních údajů, informací o platebních kartách aj.), které by mohli útočníci zneužít ke svému obohacení. Mezi další potenciálně zneužitelná data mohou patřit záznamy o spotřebě elektřiny zákazníků a další soukromé informace společností.

6.4.2 Integrita

Integrita (integrity) zajišťuje, že data nebyla neoprávněně modifikována. Data je třeba udržovat v konzistentním stavu a zamezit jejich náhodné nebo úmyslné změně.

Manipulací s elektroměrem by mohl zákazník odesílat nesprávná data o spotřebě a záměrně tak poškodit energetickou společnost. V případě manipulace se senzory PMU na elektrické síti by mohlo dojít k chybným rozhodnutím o stavu sítě a útočník by mohl způsobit rozsáhlý výpadek elektřiny.

6.4.3 Dostupnost

Dostupnost (availability) znamená, že služba je dostupná v okamžiku, kdy je potřeba.

V elektrické rozvodné síti je jedním z nejdůležitějších faktorů dostupnosti stálá dodávka elektrického proudu. Mnoho útoků může cílit na narušení dodávek elektrického proudu nebo být jejich druhotným projevem. Přerušená dodávka elektrického proudu je zákazníky vnímána jako větší problém než pouhá nedostupnost informací o svém účtu nebo aktuálních cenách elektrické energie.

6.4.4 Účetnictví

Účetnictví (accountability) zaručuje, že pro jednotlivé akce a události je dohledatelné, kdo a kdy je způsobil. Účetnictví podporuje neodvolatelnost, izolaci poruch, detekci průniků do systému a prevenci.

6.5 Management rizik

Management rizik je definován standardem ISO 31000, jedná se o metodiku pro identifikaci a vyhodnocení rizik. Cílem standardu je vytvořit univerzálně uplatnitelnou metodiku, která nahradí ostatní roztříštěné standardy a postupy [52]. Do metodiky patří standardy:

- ISO 31000:2009 – Principles ang Guidelines on Implementation,
- ISO/IEC 31010:2009 – Risk Management – Risk Assessment Techniques,
- ISO Guide 73:2009 – Risk Management – Vocabulary.

Pro prostředí informačních technologií existuje sada standardů ISO 27000, která se věnuje bezpečnosti, managementu rizik a různým bezpečnostním doporučením.

Management rizik představuje vhodnou techniku pro vyhodnocení a řešení rizik a bezpečnostních hrozeb v malých i rozsáhlých systémech, včetně Smart Grid sítí.

6.5.1 Proces managementu rizik

Vlastní proces managementu se skládá z několika kroků:

1. Identifikace a charakterizace hrozeb – představuje analýzu možných bezpečnostních problémů, které se mohou v systému vyskytnout. Může se jednat o narušení činnosti systému nebo jeho komponent, odposlech dat, neoprávněné vniknutí a manipulace aj. Množství a druhy hrozeb záleží na systému, který je analyzován.
2. Vyhodnocení zranitelností důležitých objektů – proces, při kterém jsou hrozby spojeny s konkrétními objekty (narušení autentizace v programu, odposlech dat přes bezdrátové sítě, ...).
3. Vyjádření míry rizika – pro jednotlivá rizika je vyhodnocena pravděpodobnost výskytu rizika a jeho možný dopad. Na základě těchto informací se později přistupuje ke snižování rizik s vysokou pravděpodobností výskytu nebo velkého negativního dopadu, analýza tak musí být objektivní a přesná.
4. Identifikace způsobů, jak snížit riziko – pro jednotlivá rizika jsou vyhodnoceny možné způsoby, jak riziko snížit. Snížení rizika nemusí znamenat jeho úplné odstranění. Například při plánování stavby nové budovy může být rizikem její poškození tornádem. Jedno řešení může být použití lepších materiálu a silnějších zdí, které budovu ochrání, jiné může navrhnout budovu vystavět na jiném místě,

kde takové riziko nehrozí. Řešení pak mají různou nákladnost a jiný účinek při snižování rizika.

5. Priorizace snižování rizik dle zvolené strategie – na základě všech předchozích analýz je zvolen postup při kterém se postupně vybírají různá rizika a aplikují se jejich (i částečná) řešení. Jako první je možné řešit rizika s vysokou pravděpodobností výskytu nebo závažnými důsledky, zvolená strategie záleží na konkrétním použití. Některá rizika nemusejí být snižována vůbec.

6.5.2 Identifikace rizik

Na začátku procesu je nutné identifikovat potenciální rizika. Na začátku je potřeba vyhledat možné příčiny problémů:

- analýza zdrojů – vyhledání možných zdrojů rizik (interních i externích),
- analýza problémů – rizika jsou vztažena k hrozbám.

Po znalosti zdrojů a problémů je možné následně vykonávat analýzy za účelem identifikace možných rizik [52, 53]:

- cílově založená analýza – organizace a týmy mají přiřazeny úkoly, jakákoliv událost, která může zabránit splnění cíle je identifikována jako riziko,
- scénářově založená analýza – jsou vytvářeny různé scénáře, které popisují, jak dosáhnout cílů; jakákoliv událost, která zapříčiní nevhodnou alternativu scénáře je identifikována jako riziko,
- taxonomicky založená analýza – vytvoření taxonomického členění možných zdrojů rizik,
- běžná rizika – pro některé případy existují seznamy běžných rizik.

Konkrétní postupy vztažené na prostředí Smart Grid sítí je možné najít v:

- NIST SP800-53A – Guide for Assessing the Security Controls in Federal Information Systems [16],
- Information Systems Security Assessment Framework [17],
- Open Source Security Testing Methodology [18].

Dokument NIST SP800-53A popisuje základní postupy při vyhodnocování systémů a následně popisuje velké množství konkrétních scénářů. Zahrnuty jsou obecné scénáře týkající se požární bezpečnosti, využívání nouzového osvětlení a správy bezpečnostních

politik a další. Pro oblast informačních systémů jsou obsaženy scénáře vyhodnocující řízení přístupu (logování neúspěšného přihlášení, princip co nejmenších práv, auditování), tok informací (šifrování), politiky vzdáleného přístupu do systému. V dalších scénářích je možné najít vyhodnocení bezpečnosti bezdrátových sítí, přístup přes mobilní zařízení, ochranu před malwarem nebo správu kryptografických klíčů. V dokumentu je obsaženo několik stovek různých scénářů.

Framework ISSAF popisuje obecný proces managementu rizik, problematiku bezpečnostní politiky a penetračního testování. Popsány jsou hrozby týkající se fyzické bezpečnosti, narušení dat a řízení aktualizací systémů. V dalších částech je popsán princip a důležitost školení bezpečnosti pro všechny uživatele systémů. Na závěr jsou vypsány možné konkrétní zranitelnosti v konfiguracích pro operační systémy Windows, Linux a Solaris.

Metodika OSSTM popisuje vyhodnocení a testování bezpečnosti v šesti základních kategorií:

- bezpečnost informací (sběr informací a validace, správa lidských zdrojů, ...),
- bezpečnost procesů (testování požadavků, doporučení, sociální inženýrství, ...),
- bezpečnost internetových technologií (skenování sítě, testování internetových aplikací, testování IPS/IDS, firewallů a směrovačů, crackování hesel, ...),
- bezpečnost komunikací (testování telefonního systému, záznamníků, faxů, VoIP, řízení vzdáleného přístupu, ...),
- bezpečnost bezdrátových sítí (testování WiFi a bluetooth sítí, bezdrátových zařízení, RFID přístupů, ...),
- fyzická bezpečnost (vyhodnocení řízení přístupu, monitorování, reakce na poplach, vyhodnocení umístění a prostředí, ...).

6.5.3 Míra rizika

Míru rizika je možné číselně vyjádřit vzorcem [1]:

$$R = P_{hrozba} \cdot P_{zranitelnost} \cdot I,$$

kde R je míra rizika, P_{hrozba} je pravděpodobnost přítomnosti hrozby, $P_{zranitelnost}$ je pravděpodobnost, že hrozba využije zranitelnosti a I kvantifikuje potenciální dopad (k vyjádření se může využít například cena za způsobené škody). Někdy se využívá podobný vzorec, kde jsou pravděpodobnosti sloučeny do jediné.

Ve složitějších případech se pravděpodobnost a hodnota dopadu abstrahuje na stupnici od jedné do pěti a vyjadřuje se tak subjektivní hodnocení.

6.5.4 Redukce rizik

Po identifikaci a priorizaci rizik se přistupuje k redukci rizik. Optimálním řešením by bylo vyřešit všechna možná rizika, ale to prakticky není možné vzhledem k rozsahu problému nebo finanční nákladnosti pro taková řešení.

Rizika lze redukovat čtyřmi způsoby:

- Předejití riziku (eliminace) – úplné odstranění rizika. Může se jednat o změnu technologie, postupů nebo zahrnutí takových opatření, které zamezí jakémukoliv výskytu daného rizika. Obvykle představuje nejvíce nákladné řešení.
- Snížení rizika – provedení takových opatření, která rizika sníží, ale neodstraní úplně. Riziko zůstává, ale jeho pravděpodobnost výskytu nebo možné následky jsou sníženy. Například zpřísnění politiky hesel sníží pravděpodobnost, že by heslo bylo odhaleno při bruteforce[1] metodě útoku, ale neodstraní ji úplně.
- Sdílení rizika – riziko je sdíleno nebo převedeno na někoho jiného. Zahrnuje například pojištění objektů. Riziko zůstává, ale při jeho výskytu jsou případné finanční ztráty převedeny na jiný subjekt.
- Přijetí rizika – riziko je akceptováno v nezměněné formě. Řešení s nulovými náklady, obvykle využitelné u velice nepravděpodobných rizik nebo u rizik s minimálním dopadem.

[1]Metoda při které jsou zkoušeny všechny možné kombinace vstupů. Otestuje tak všechny varianty, ale může trvat velmi dlouho (zavisí na vstupní sadě znaků a délce hesla).

7 BEZPEČNOSTNÍ HROZBY

V následující kapitole jsou analyzovány bezpečnostní hrozby a rizika v jednotlivých částech Smart Grid sítě, využívaných technologiích, protokolech či aplikacích [4, 14].

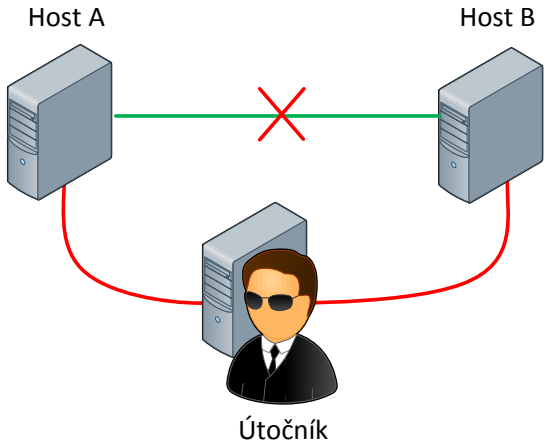
7.1 Bezpečnostní hrozby AMI

Technologie AMI (advanced metering infrastructure) zasahuje od zákazníka po energetické společnosti a uchovává a přenáší mnoho informací včetně soukromých údajů. Následující typy hrozeb se mohou vyskytnout při využívání AMI [4, 35]:

- Odposlouchávání – představuje neautorizované zachycení soukromé konverzace. Běžné nebezpečí na sdílených komunikačních médiích, především rádiové přenosy nebo také přepínané sítě (útoky na přepínače, ARP spoofing) [44]. Odposlouchávání může vést k narušení důvěrnosti a vyzrazení citlivých údajů.
- Analýza provozu – zachycení a následná analýza zpráv s cílem zjištění informací z přenosu (lze tak identifikovat uživatele či systémy, kteří spolu komunikují, analyzovat topologii sítě a případně i zachytit vlastní obsah komunikace) [14, 44].
- Indiskrétní personál – zaměstnanci mohou pod nátlakem, pomocí úplatků nebo vlastní neopatrností vyzradit důvěrné informace (včetně přístupových údajů, soukromých informací o společnosti nebo zákaznících).
- Změna dat – pokud útočník získá přístup ke směrovači či stanici přes kterou jsou přeposílána data nebo se mu jiným způsobem podaří manipulovat s daty, může měnit informace ze senzorů, smart meterů, aj. Změnu dat lze také realizovat modifikací odesílací stanice či zařízení.
- Maškaráda – útočník se vydává za autorizovaného uživatele systému s cílem získání přístupu do systému, nebo aby získal vyšší oprávnění. Podobně lze využít techniky phishing[2] pro získání informací od uživatelů, které může útočník později využít k přístupu do systému [47].
- Obcházení kontroly – útočník se může pokusit obejít bezpečnostní mechanismy (využitím chyb a zranitelností), aby získal přístup k datům a mohl manipulovat se systémem a daty.

[2]Technika phishing se často využívá na internetu, útočník vytvoří webové stránky, které napodobují známé stránky různých společností (sociální sítě, aukční portály, aj.) a následně se snaží nalákat uživatele na tyto stránky a získat jejich přihlašovací údaje.

- Narušení autorizace – útočník může poškodit autorizační mechanismus systému AMI pro získání přístupu. Útok se může týkat získání přístupu do počítačového systému, ale také do budovy transformátorové stanice nebo jiných částí sítě.
- Fyzické narušení – útočník může fyzicky vniknout do komponent systému AMI. Například poškození nebo manipulace se smart meterem nebo jiného vybavení, které je veřejně přístupné [14].
- Man-in-the-middle – MITM je technika aktivního odposlechu, kdy útočník vytvoří spojení s oběťmi a přeposílá zprávy mezi nimi. Útočník tak vystupuje jako prostředník mezi oběťmi. Oběti neví o přítomnosti útočníka a považují komunikaci za soukromou. Schéma útoku je znázorněno na obrázku 10 [45].



Obrázek 10 – Princip MITM útoku

- Krádež – velké množství komponent systému se nachází na veřejně přístupných místech a jsou tak snadno dostupné pro útočníky nebo vandaly. Odcizením zařízení vzniká společnostem finanční ztráta, může dojít k výpadku služeb a k vyzrazení důvěrných dat na zařízení, které mohou být dále zneužity [49].
- Opakovací útok – síťový útok, při kterém jsou data zachycena a zpožděna nebo opakovaně odeslána. V některých zranitelných komunikačních protokolech, které nedisponují ochranou proti takovému útoku, zopakovaná data jsou přijata jako korektní a následně zpracována. Systém tak reaguje na stejná data vícekrát a je možné ho uvést do nestandardního stavu, případně narušit jeho činnost [50].
- Viry/červi – virus představuje počítačový program (druh škodlivého softwaru), který se umí šířit a infikovat další počítače (například rozesíláním emailů nebo jiným způsoben po počítačové síti). Červi na rozdíl od virů cíleně využívají zranitelností a jejich překonáním získají oprávnění pro své šíření a poškozování systému [45].

- Trojský kůň – druh škodlivého softwaru, který navenek vykonává svoji regulérní funkci. Skrytě však umožňuje útočníkovi přístup k počítačovému systému. Může tak efektivně vytvářet tzv. botnet[3] nebo sloužit k ukradení dat z počítače [45, 46].
- Trapdoor/backdoor – nedokumentované vstupní místo do počítačového programu. Obvykle je vytvořeno programátorem pro získání diskrétního přístupu do programu (bez nutnosti provést regulérní autentizaci a autorizaci nebo logování vstupu) [46].
- Vyčerpání prostředků – prostředky počítačových systémů (paměť, procesor, diskový prostor, ...) jsou omezené. Útočník může využít různých způsobů k jejich vyčerpání (například velké množství připojení k serveru může zabránit dalším připojením) a tím zablokovat přístup ostatním uživatelům [47].
- Narušení integrity dat – integrita je narušena, pokud někdo změní data v systému (například úprava databáze uživatelů) a zamezí tak regulérním uživatelům v používání systému. Narušení integrity může mít i další dopady na různé rozhodovací procesy.
- Interní útok – útočník může využít přístupu z koncového bodu zákazníka pro přístup do centrálních komponent systému AMI. Přístup z interních sítí je obvykle méně zabezpečen a existuje tak vyšší riziko, že se daný útok podaří.
- Neautorizovaný přístup z koncového bodu zákazníka – útok zahrnuje potenciální možnost získat přístup k elektrické síti. Útočník může využít napadení bezdrátové komunikace mezi smart meterem a koncentrátorem nebo jiným koncovým zařízením a získat přístup k lokální či centrální řídící stanici [4].
- Podvádějící zákazník – zákazník se může pokusit upravit smart meter nebo jeho firmware za účelem snížení ohlašované spotřeby elektrické energie. Špatné informace o spotřebě finančně poškozují energetické společnosti a při jejich využití pro vyhodnocení zatížení sítě mohou vést ke špatným rozhodnutím při regulaci distribuční soustavy [48].
- Manipulace s trhem – útočník může manipulovat se sítí (šíření falešných dat, blokování signálu) za účelem manipulace s trhem. Například útočník disponuje možností prodávat elektrickou energii a následnou manipulací si připraví výhodné podmínky pro vlastní obohacení [36].

[3]Botnet představuje skupinu programů (resp. počítačů), které spolu komunikují. V negativním kontextu se jedná o skupinu napadených počítačů řízených útočníkem, takové botnety jsou využívány k šíření spamu nebo útokům typu DDoS.

7.1.1 Smart meter

Smart meter může být vystaven některým rizikům:

- Neoprávněná manipulace se smart meterem – s cílem snížit měřené množství, vydávat se za jiného zákazníka, aj.
- Neoprávněný příkaz k odpojení – smart meter je možné na dálku řídit a odpojit zákazníkovi přívod elektrického proudu. Útočník může příkaz podvrhnout a cíleně nebo plošně poškodit zákazníky.
- Nebezpečná implementace komunikačního protokolu – útočník může odeslat příkazy, které jsou různě deformovány. Pokud je smart meter nedokáže zpracovat korektně, může dojít k různým chybám typu přetečení bufferu.

7.2 Bezpečnostní hrozby DR

Systém DR (demand response) umožňuje zvýšit efektivitu sítě a předcházet výpadkům v síti. V případě zneužití nebo poškození systému může dojít k závažným problémům, zvláště pokud by útočník dokázal ovládat rozsáhlou část systému. Mezi možné hrozby patří [4]:

- Hromadné vypnutí všech zařízení – útok, který má dopad především na pohodlí a spokojenost zákazníků. Napadení systému může vést k následné nespokojenosti a dalšímu odmítání používaní technologie DR. V některých případech by mohlo dojít k ohrožení zdraví uživatelů.
- Způsobení nestability sítě – vytvoření velkého zatížení v síti by mohlo způsobit nestabilitu a vést k výpadkům.
- Blackout/zvýšení nákladů – zamezením funkčnosti systému DR nebude možné efektivně snížit spotřebu a pokud dojde k vyššímu zatížení sítě může dojít k výpadkům. Neúčinnost DR také povede k vyšším nákladům na výrobu elektrické energie.

7.3 Bezpečnostní hrozby sítí HAN, NAN

Analyzovány jsou možné problémy v síti HAN, NAN a v přístupové bráně mezi těmito sítěmi [4].

7.3.1 Sítě HAN

Rizika při používání ZigBee:

- Výpadky elektřiny – jednorázové hodnoty užívané pro šifrování jsou inicializovány na výchozí hodnoty a jsou v tu chvíli známé potenciálnímu útočníkovi.
- Rychlý DoS útok na AES-CTR.
- Vytváření falešných potvrzovacích rámců.
- Slabá ochrana integrity při používání AES-CTR.
- Dovoluje používat shodné klíče na více ACL záznamech. Umožňuje využívat skupinové klíče.

7.3.2 Sítě NAN

Rizika při používání Wi-Fi (IEEE 802.11):

- Veřejně oznamovaná přítomnost sítě – přítomnost sítě je oznamována pomocí tzv. beacon rámců.
- Cizí (tzv. rogue) přístupové body – cizí přístupové body se mohou vydávat za legitimní přístupové body.
- MAC spoofing – řídící rámce nejsou autentizovány ve standardu 802.11 a obsahují zdrojovou adresu. Útočník může využít podvrženého rámce pro přesměrování toku dat a poškození ARP tabulek.
- DoS útoky – zahlcením rádiového spektra je možné zvýšit šum natolik, že síť nebude schopna přenášet žádná data.
- Síťové útoky – útočník může zahltit bránu pomocí ICMP paketů a snížit tak přenosové rychlosti ostatních klientů.
- MITM útoky – útoky mohou být využity k odposlouchávání anebo k manipulaci s daty.

Rizika při používání technologií založených na IEEE 802.15.4:

- Důvěrnost – nutné použít šifrovací algoritmus.

- Ztráta stavu ACL záznamů – záznamy v ACL tabulce uchovávají jednotlivé klíče a přiřazené jednorázové hodnoty. Pokud dojde k výpadku napájení nebo se zařízení přepne do režimu s nízkým odběrem el. proudu, dojde k vymazání ACL tabulky.
- Problém managementu klíčů – ACL tabulky nepodporují různé druhy modelů pro správu klíčů. Není možné specifikovat stejný klíč pro více záznamů. Při používání stejného klíče pro celou síť existuje riziko využití opakovacího útoku.
- Ochrana důvěrnosti a integrity – používáním šifrovaných režimů bez autentizace vede k možnému narušení integrity i důvěrnosti.
- DoS – opakovací útok může být zneužit, aby zařízení odmítalo legitimní pakety.
- Chybějící integrita u potvrzujících paketů – odesílatel může vyžadovat potvrzení o doručení paketů. Potvrzující pakety nejsou nijak šifrovány či autentizovány a útočník může potvrzující pakety podvrhnout.

Rizika při používání WiMax (IEEE 802.16):

- Autentizace – stanice BS neposkytují autentizaci a představují riziko MITM útoku pro uživatele.
- Šifrování – standard 802.16e definuje podporu pro šifrování AES. Šifrování se týká pouze uživatelských dat, řídící rámce zůstávají nešifrované a útočník může získat informace o uživatelích a charakteristice sítě.
- Dostupnost – WiMax využívá licencované rádiové spektrum, přesto je možné pomocí snadno dostupných zařízení provádět rušení sítě. Útočník také může vytvářet řídicí rámce, které slouží k deautentizaci klientů.
- Útok „vodní mučení“ – forma útoku na fyzické vrstvě, kdy útočník odesílá množství rámců na cílové zařízení, aby vybil jeho baterii.

7.4 Bezpečnostní hrozby SCADA systémů

SCADA systémy slouží k monitorování a řízení mnoha komponent elektrické sítě, v některých případech může jít o zastarávající technologie, které jsou napojeny na počítačovou síť a mohou tak být snadno zranitelné.

7.4.1 Dostupnost veřejných informací

Mnoho informací o energetických společnost se dá získat z běžných dotazů. Tyto informace mohou být využity k lépe cílenému útoku proti společnosti. Mezi běžně veřejné informace patří informace na webových stránkách (struktura společnosti, jména a emailové adresy zaměstnanců, ...) nebo informace dostupné z DNS serverů (IP adresy serverů, emailové informace).

7.4.2 Zranitelnosti konfigurace systémů

- Aktualizace operačního systému a aplikací nejsou udržovány.
- Nesprávné řízení přístupu – uživatelé mohou disponovat příliš mnoho oprávněními (nebo mohou důležité oprávnění postrádat).
- Nepřítomnost politiky hesel – definuje, jak silná hesla musejí být a jejich udržování.

7.4.3 Softwarové zranitelnosti

- DoS útoky – SCADA software může být postižitelný DoS útoky, což může mít za následek odepření přístupu uživatelům a zpoždění systémových operací.
- Absence IDS/IPS systémů – IDS a IPS systémy mohou aktivně zabránit mnoha typům útoků a škodlivému softwaru v napadení systému.
- Absence softwaru na ochranu před malwarem, neaktuálnost definičních souborů, nasazení bez důsledného testování – podobně jako systémy IDS/IPS, ochrana proti malwaru je důležitá pro zajištění stability a bezpečnosti systému. Neaktuální definiční soubory nedokáží systém chránit před novými druhy škodlivého softwaru.

7.4.4 Zranitelnosti síťové konfigurace

Návrh síťové architektury je důležitý, aby dostatečně oddělil segment internetu, firemní sítě společnosti a SCADA sítě. Zranitelnosti v síťové architektuře mohou vést k možnosti napadnout systémy SCADA z internetu.

Mezi časté problémy patří:

- Konfigurace FTP, HTTP nebo emailových služeb zbytečně umožňuje přístup k podnikové síti.

- Komunikace s partnery není zabezpečena pomocí firewallu, IDS/IPS nebo pomocí VPN.
- Firewall a jiné řídící mechanismy nejsou implementovány v interní síti a jednotlivé segmenty sítě nejsou vůbec nebo pouze minimálně separovány.

7.4.5 Zranitelnosti protokolu Modbus

Starší systémy SCADA mohou využívat přenosový protokol Modbus. Protokol Modbus nebyl navržen do nebezpečného prostředí a obsahuje více druhů zranitelností [14]:

- Odesílání falešných všesměrových zpráv pro podřízená zařízení.
- Opakovací útok na zprávy odesílané na server.
- Vyblokování serveru a převzetí kontroly nad podřízenými zařízeními.
- Odesílání zpráv na všechny možné adresy pro zjištění informací o zařízeních.
- Pasivní odposlech Modbus zpráv.
- Zpoždění odpovědních zpráv určené pro servery.

7.4.6 Zranitelnosti protokolu DNP3

Protokol DNP3 představuje nástupce protokolu Modbus a je využíván v mnoha novějších SCADA systémech. Přestože je velmi spolehlivý, v základu neposkytuje dobré zabezpečení proti útokům [4]:

- Pasivní průzkum sítě – útočník, který dokáže zachytit DNP3 zprávy může získat informace o síťové topologii, funkcionality zařízení a další informace.
- Opakovací útoky ze serveru – na základě znalosti normálních datových toků je možné simulovat odpovědi serveru.
- MITM útok – zařízení umístěné mezi serverem a vnějšími zařízeními může zachytávat a modifikovat síťový provoz.
- Přetečení délky/DFC příznak – útočník může uvést neplatnou hodnotu do pole délky nebo nastavit příznak DFC, pro server pak bude vnější zařízení vypadat jako zaneprázdněné. Tyto útoky mohou vést k poškození dat nebo k pádu zařízení.
- Resetovací funkce/nedostupná funkce – Útočník může odeslat zprávu s příkazem na resetování cílového zařízení. Zařízení provede restart a bude nějakou dobu

nedostupné. Útočník také může vytvořit zprávu s kódem oznamujícím nedostupnost služby, kterou odešle serveru. Server následně přestane odesílat požadavky na cílové zařízení, protože předpokládá, že daná služba není dostupná.

- Změna cílové adresy – útočník může přepsat cílovou adresu a přesměrovat tak požadavky a odpovědi na jiné zařízení. Útočník také může použít všesměrovou adresu pro odeslání požadavků všem zařízením.
- Poškození fragmentovaných zpráv – příznaky FIR a FIN slouží k indikaci prvního (posledního) rámce z fragmentované zprávy. Pokud dorazí zpráva s příznakem FIR, všechny předchozí nekompletní fragmenty jsou zahozeny. Útočník může po zahájení fragmentovaného přenosu odeslat rámec s příznakem FIR a způsobit tak zahození začátku zprávy, což povede k přenosu neplatné zprávy. Alternativně může předčasně přenos ukončit pomocí FIN příznaku.
- Změna sekvenčního čísla – sekvenční číslo slouží k zajištění správného pořadí při zasílání fragmentovaných zpráv. Útočník může podvrhnout zprávu, kterou vloží do sekvence zpráv a může tak vložit vlastní data nebo způsobit chybu při zpracování.
- Reset dat vzdálených zařízení – útočník může odeslat zprávu s kódem pro reinicializaci dat.

7.4.7 Zabezpečení sériových komunikačních linek

Na mnoha místech se ve SCADA systémech využívají pomalé sériové linky. Používané protokoly obvykle nezajišťují integritu ani důvěrnost přenášených dat a je nutné je zabezpečit.

Jednoduché řešení využitím protokolů SSL nebo IPsec over PPP však nemusí být vhodné. Jejich použitím se zvýší nároky na výpočetní výkon zařízení a datové toky, což může vést k velmi pomalé odezvě na těchto sériových linkách.

7.5 Zranitelnosti webových aplikací

V aplikační vrstvě se často využívají webové aplikace, které je možné zpřístupnit z mnoha míst a různých druhů zařízení. Jejich využití může být velmi široké, od správy nastavení smart meteru po rozsáhlý portál energetické společnosti s komplexními informacemi o zákazníkovi, jeho spotřebě, tarifech aj [2].

Webové aplikace mohou obsahovat několik druhů zranitelností:

- Nezabezpečené spojení – mnoho webových aplikací nevyužívá zabezpečený protokol HTTPS. Data tak mohou být odposlouchávána včetně přihlašovacích údajů do systému.
- SQL injection – webové aplikace obvykle pracují s databázemi a v některých případech je možné využít neošetřených vstupů a provést libovolné operace přímo nad databází. Následkem může být ztráta dat, jejich poškození nebo získání neoprávněného přístupu pro útočníka.
- XSS, CSRF – útoky, které cílí na uživatele. Do webových stránek je přidán škodlivý kód, který se snaží manipulovat s webovým prohlížečem uživatele [50].
- Kompilované aplikace – webové aplikace založené na kompilovaném kódu mohou být zranitelné na různé útoky typu stack overflow, buffer overflow. Tyto útoky umožňují útočníkovi manipulovat s kódem a daty prováděného programu.
- Výchozí hesla – v mnoha zařízeních se využívají podobná či shodná hesla pro přístup. Neškolení uživatelé mohou opomenout důležitost změny hesla a útočník může využít známých hesel pro získání přístupu do administrace zařízení.

7.6 Zranitelnosti IP protokolu

Protokol IP disponuje velkou výhodou díky kompatibilitě s mnoha komponentami a stávajícími počítačovými sítěmi. Sada protokolů TCP/IP, ale může být cílem různých druhů útoků [14, 56]. Mezi zranitelnosti patří:

- Smurf útok – DoS útok, při kterém útočník vytvoří ICMP echo-request požadavek, který odešle na všesměrovou adresu sítě. Jako odesílatele nastaví adresu oběti a následně všechna zařízení v síti začnou odesílat odpovědi oběti.
- Source routing – útočník může využít specifikace směrování k zjištění informací o topologii sítě.
- Land útok – útočník vytvoří paket, kde uvede shodnou adresu a port odesílatele i adresáta. U některých operačních systémů při přijetí tohoto paketu dojde k chybě při zpracování a systém může skončit v nekonečné smyčce.
- SYN flood – DoS útok realizovaný pomocí TCP protokolu. TCP protokol využívá k navázání spojení tzv. třícestný handshake. Při tomto útoku útočník vytváří velké množství spojení u kterých handshake nedokončí a spojení zůstávají částečně navázána. Vytvořením velkého množství spojení vyčerpá systémové prostředky a další spojení budou odmítnuta.

- Odhalení sekvenčního čísla TCP spojení – pokud útočník dokáže uhádnout sekvenční číslo, může vložit data do spojení nebo způsobit jeho přerušení odesláním příznaku RST.
- Podvržení ICMP Redirect zpráv – útočník může vytvořit podvržené zprávy typu ICMP Redirect a způsobit tak přesměrování dat přes sebe.
- Podvodný DHCP server – v prostředí využívající DHCP server může útočník vytvořit vlastní DHCP server. Klienti pak mohou obdržet IP adresu a adresu výchozí brány od útočníka, který může realizovat odposlouchávání a útok typu MITM.

7.7 Přepínané sítě Ethernet

Přepínané sítě jsou využívány ve Smart Grid sítích v rámci sítí energetických společností, transformátorových stanic nebo u zákazníků. Představují možná rizika pro interní útok [41, 42]:

- ARP spoofing/poisoning – útočník může vytvořit podvržené rámce s upravenou MAC adresou odesílatele, které následně odesílá přes přepínač. Přepínač se z těchto rámců naučí nové umístění hosta s podvrženou MAC adresou. Následující data odeslaná na zneužitou MAC adresu nejsou odeslány skutečnému cíli, ale útočníkovi, který může realizovat útok typu MITM.
- Přetečení CAM tabulky/MAC flooding – počet záznamů v CAM tabulce, která slouží k mapování MAC adres na porty přepínače, je omezen. Útočník může generovat velké množství rámců s neexistujícími MAC adresami a způsobit tak zahlcení CAM tabulky. Přepínač, který nenachází záznamy v CAM tabulce, se následně chová jako hub a odesílá data přes všechny porty. Útočník pak může odposlouchávat data.
- STP root bridge manipulation – protokol STP zajišťuje, že v přepínané síti nevzniknou smyčky. Prakticky je tak možné budovat redundantní topologie, které jsou odolné výpadkům. Útočník může využít vlastní přepínač nebo software, vytvořit upravené BPDU zprávy a rozšířit informaci do sítě, že se stal novým kořenem STP topologie. Všechna data v síti budou následně směrována přes útočníka a ten může data odposlouchávat nebo realizovat útoky typu MITM.

7.8 Sociální sítě

Rozvoj Smart Grid sítí se může promítnout i ve využívání sociálních sítí. Zařízení jako je Tweet-a-Watt, SmartSync či PICOwatt umožňují sledovat spotřebu elektrické energie konkrétních zařízení a informace pravidelně sdílet pomocí sociálních sítí Facebook, Twitter nebo pomocí RSS kanálů [2, 43].

Podobné sdílení informací může prozradit zvyklosti uživatelů a informovat zloděje v jakou dobu je byt prázdný.

7.9 Generické bezpečnostní problémy

Generické bezpečnostní problémy se netýkají specifických komponent, ale mohou postihovat prakticky libovolné zařízení nebo části sítě [4].

7.9.1 Životnost elektrických systémů

Stávající přenosové a distribuční soustavy mohou obsahovat již zastarávající zařízení. Integrací nových počítačových systémů se mohou vyskytnout problémy s kompatibilitou. Starší zařízení rovněž mohou být zdrojem potenciálních bezpečnostních zranitelností.

Při implementaci systémů, hardwaru či protokolů je nutné brát v úvahu, že budou využívány pro delší časové období (řádově desítky let) a jejich případná aktualizace bude postupná. Proto je nutné dostatečné naplánování vybraných technologií kvůli životnosti i bezpečnosti.

7.9.2 Řešení autentizace a autorizace do zařízení IED/smart meterů

Zařízení IED se nacházejí na mnoha místech a také ve vzdálených transformátorových stanicích. Je nutné vyřešit, jakým centralizovaným způsobem bude spravována možnost autentizace a autorizace do těchto zařízení.

V současnosti mnoho zařízení IED používá pouze lokální databáze hesel. Ty jsou obvykle definována ne pro konkrétního uživatele, ale pro „roli“ (audit – pouze pro čtení, uživatel – čtení a zápis, ...). Tato hesla mohou být poskytována i uživatelům z jiných společností, kteří mohou vyžadovat občasný přístup. Vzhledem k velkému množství zařízení se často používají stejná hesla na mnoha zařízeních a jejich změny nejsou časté.

K zařízením IED je možné přistupovat lokálně nebo vzdáleně přes drátové a bezdrátové sítě. Důležité je také zřízení možnosti nouzového přístupu v kritických situacích.

Podobný problém se týká správy smart meterů. Hesla obvykle nejsou vázána na uživatele a využívá se stejných hesel v celé síti.

7.9.3 Řešení autentizace mezi smart meterem a DAU/řídícím prvkem AMI

Smart meter podporuje obousměrnou komunikaci a odesílá informace o spotřebě elektrické energie. Z opačného směru může přijímat řídící příkazy, aktualizace firmwaru aj. Je nutné vyřešit způsob autentizace smart meterů a nadřazeného zařízení (DAU či jiný prvek), aby bylo jisté, že smart meter komunikuje s legitimním řídícím prvkem a není manipulován útočníkem. Obdobně je potřeba mít jistotu, že se jedná o konkrétní smart meter, aby nedocházelo k podvodům s účty.

7.9.4 Řešení autentizace mezi HAN zařízeními s bránou

Podobný problém nastává u HAN zařízení, která se aktivně podílejí na procesu DR. Zařízení musejí být bezpečně autentizovány s bránou, aby nebylo možné převzít jejich kontrolu. Pokud by útočník dokázal ovládat velké množství zařízení, mohl by jejich řízením způsobit i problémy se stabilitou sítě.

7.9.5 Zabezpečení směrovacích protokolů 2. a 3. vrstvy

Interní směrovací protokoly (OSPF, RIP, EIGRP) používané v drátových sítích podporují autentizaci směrovačů. V sítích AMI se ale často mohou využívat bezdrátové sítě typu mesh.

Mesh sítě svojí povahou otevírají možnosti pro různé útoky (vložení cesty, vydávání se za jiný prvek, vkládání či změna dat, ...), které stávající směrovací protokoly neřeší. Podobný problém se týká i řešení autorizace a integrity při vytváření sousedství mezi prvky sítě. Bez dostatečné ochrany může být síť náchylná na odposlouchávání, útoky typu MITM či DoS.

7.9.6 Management klíčů smart meterů

V případech, kde smart metery budou obsahovat kryptografické klíče využívané pro autentizaci a šifrování dat, je nutné vytvořit vhodné schéma pro správu klíču, jejich ochranu a také různorodost v jednotlivých zařízeních. Klíče by měly být unikátní, v případě, že bude některý smart meter kompromitován, nesmí útočník získat přístup k celé síti.

Správa klíčů by také měla podporovat možnost pravidelné aktualizace klíčů za nové a jejich zablokování (pro zastaralé nebo kompromitované klíče).

Tento problém se netýká pouze smart meterů, pokud budou klíče a certifikáty využívány i na dalších zařízeních v sítí Smart Grid je nutné zajistit jejich správu. Jednotlivá zařízení mohou pocházet od různých výrobců a je tak nutné zajistit i kompatibilitu mezi různými výrobci.

7.9.7 Bezpečnost aktualizací firmwaru

Možnost aktualizovat firmware ve smart meterech zajistí možnost přidávání nových funkcí a oprav případných chyb. Aktualizace budou prováděny vzdáleně a proto je nutné zajistit bezpečný aktualizační proces a ochranu firmwaru, aby nebylo možné podstrčit malware.

7.9.8 Alternativní způsoby fyzických útoků na Smart Grid zařízení

Mnoho Smart Grid zařízení (smart metery, agregátory, ...) je volně přístupných a mohou být vystaveny alternativním způsobům fyzické manipulace. Útočník může využít jejich snadné dostupnosti a pokusit se odposlechnout data nebo šifrovací klíče alternativními způsoby, mezi které patří připojení sondy na elektrické spoje na desce plošných spojů, analýza elektromagnetického záření jednotlivých částí zařízení aj.

8 MODELY ŘEŠENÍ VYBRANÝCH RIZIK

V následující kapitole jsou analyzována konkrétní rizika a navrženy modely jejich řešení. Navržená řešení by měla být uplatnitelná v praktické realizaci a vybraná rizika zcela odstranit nebo minimalizovat.

8.1 Autentizace zařízení

V sítích Smart Grid budou spolu komunikovat různá zařízení, od smart meterů po servery spravující jednotlivé systémy. Aby bylo možné považovat data za správná, je nutné zajistit autentizaci zařízení – mít jistotu, že komunikujeme opravdu s tímto konkrétním zařízením.

Pokud by autentizace nebyla vyžadována, bylo by možné provádět různé útoky:

- vydávat se za jiný smart meter a nechat účtovat elektrickou energii cizímu uživateli,
- vydávat se za server/řídící prvek a řídit činnost smart meterů nebo jiných prvků v síti.

Autentizaci zařízení v sítí lze provádět několika způsoby:

- autentizace pomocí síťové/hardwarové adresy či klíče,
- autentizace pomocí PKI (public key infrastructure).

8.1.1 Autentizace pomocí síťového/hardwarového klíče

Pro autentizace je možné využít přímo síťovou adresu nebo klíč, který je v zařízení nastaven napevno. Samostatný identifikátor však neposkytne žádnou ochranu před útočníky, kteří mohou identifikátor podvrhnout a vydávat se tak za jiný subjekt.

Doplněním identifikátoru o tajný klíč je možné zajistit ochranu před podvržením. Jednotlivé zprávy by byly označeny identifikátorem a kontrolním součtem vypočítaným z tajného klíče. Útočník, který by komunikaci odposlechl, by získal identifikátor, ale nezískal by tajný klíč k výpočtu kontrolního součtu.

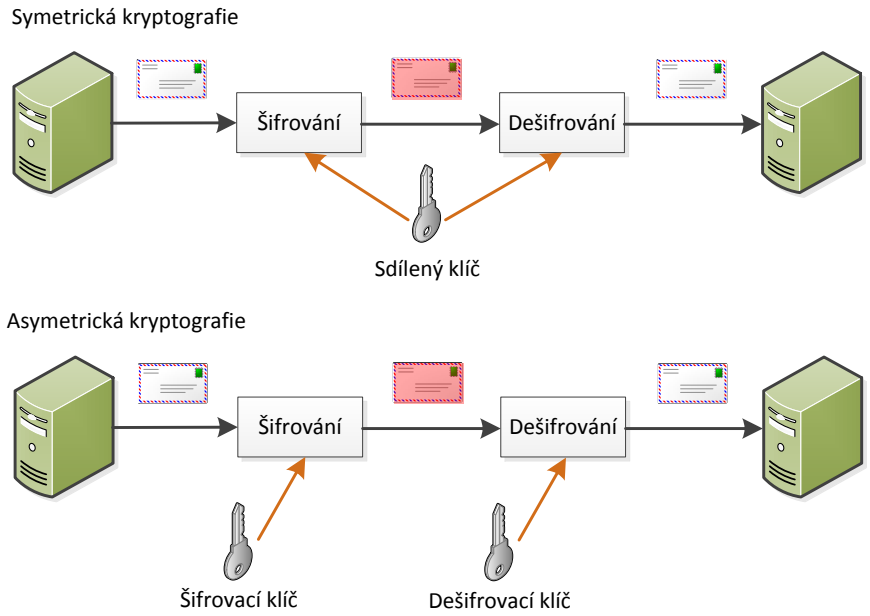
Uvedené řešení efektivně řeší problém autentizace klientů u serveru. Smart metery, ale musí být schopné provést autentizaci serveru, aby nepřijímaly příkazy od útočníka. Uvedený systém by vyžadoval vytvoření identifikátoru serveru pro každého klienta samostatně. Pokud by identifikátory byly sdíleny, uživatel jednoho smart meteru by měl snadný přístup ke klíči serveru a mohl tak manipulovat s ostatními smart metery.

Na serveru nebo zařízení, které autentizaci provádí, by musely být uchovány všechny identifikátory a příslušné klíče. Takový přístup představuje zvýšené riziko, pokud by došlo k napadení serveru a odcizení dat. Útočník by získal přístup ke všem zařízením.

8.1.2 Autentizace pomocí PKI

Systém PKI (public key infrastructure) představuje do jisté míry zobecnění a vylepšení předchozího naznačeného řešení. PKI představuje obecné řešení pro manipulaci s digitálními certifikáty, jejich vytvoření, správu, používání a zneplatnění [11, 51].

PKI je založeno na asynchronní kryptografii (vizte obrázek 11) nebo také označované jako kryptografii veřejných klíčů. Pro šifrování se využívají dva druhy klíčů – šifrovací a dešifrovací. Tyto klíče jsou různé a navzájem neodvoditelné.



Obrázek 11 – Princip symetrické a asymetrické kryptografie

Digitální podpis

Zprávy, které je nutné autentizovat, odesílatel tzv. digitálně podepíše. Digitální podpis je kontrolní součet, který je vypočítán ze samotné zprávy a následně zašifrován privátním klíčem. Po doručení zprávy adresát dešifruje kontrolní součet pomocí veřejného klíče a porovná ho s kontrolním součtem, který sám vypočítal. Pokud oba součty souhlasí, je zpráva považována za pravou.

Pro vlastní výpočet kontrolního součtu se používají jednosměrné hashovací funkce, mezi které patří MD5 či SHA1.

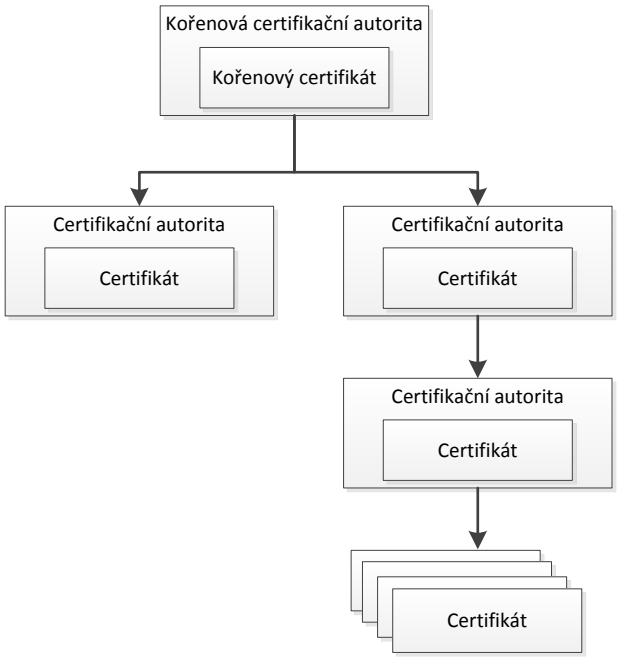
Digitální certifikát

Digitální certifikát pak obsahuje několik základních informací:

- identifikátor subjektu,
- veřejný klíč subjektu,
- vydavatel certifikátu (certifikační autorita),
- datum platnosti, ...

Digitální certifikáty je možné sdílet dalším subjektům. Privátní klíč zůstává pouze u jediného subjektu, který využívá tento certifikát ke své autentizaci.

Certifikační autorita slouží k vydávání a správě certifikátů. Jednotlivé certifikáty jsou sdružovány pod certifikační autority a je možné ověřit jejich pravost (certifikát je digitálně podepsán certifikační autoritou). Certifikační autority mohou tvořit stromovou hierarchii, příklad hierarchie je zobrazen na obrázku 12.



Obrázek 12 – Příklad stromové hierarchie certifikačních autorit

Certifikační autority tvoří tzv. strom důvěry, kdy jednotlivé certifikáty jsou ověřitelné u nadřazené certifikační autority. V případě kompromitování certifikační autority je možné zneplatnit příslušnou větev a zachovat tak funkčnost zbytku systému. V případě kompromitování kořenové certifikační autority by bylo nutné vyměnit certifikáty v celém systému [57].

Pro systém PKI se využívají certifikáty dle standardu X.509. Pro přenos certifikátu s privátním klíčem je využíván formát PKCS #12.

8.1.3 Shrnutí

Řešení autentizace pomocí systému PKI představuje komplexní a standardizované řešení [14]. Certifikační autority umožňují delegovat správu jednotlivých částí systému do oddělených celků a zvýšit tak stupeň segmentace. Segmentace systému zvyšuje komplexnost, ale podstatně zvyšuje bezpečnost v případě kompromitování některé certifikační autority, případné problémy by se týkaly menší množiny zařízení.

Při využívání PKI je velmi důležité zajistit dostatečně bezpečné prostředí pro certifikační autority a zejména pro kořenovou certifikační autoritu.

8.2 Důvěrnost a integrita dat

V sítích Smart Grid se přenáší velké množství informací různého charakteru:

- informační data,
- informace o spotřebě elektrické energie zákazníky,
- řídící příkazy pro zařízení.

Informace o zákaznících a jejich spotřebě mohou spadat do klasifikace osobních údajů a je nutné je taktéž patřičně chránit. Většina těchto dat musí být ochráněna z hlediska důvěrnosti (data nesmějí být čtena neautorizovanými subjekty) a integrity (data nesmějí být změněna nebo poškozena během přenosu).

Data se v sítích Smart Grid často přenášejí přes technologie, které jsou náchylné k odposlouchávání – různé druhy rádiových technologií, PLC technologie nebo i přepínané sítě mohou být napadeny.

Pro ochranu dat je možné využít několika různých způsobů:

- šifrování v rámci přenosové technologie,
- vlastní šifrovací protokol (aplikační vrstva),
- protokoly TLS (transport layer security)/SSL (secure sockets layer),
- IPsec.

8.2.1 Řešení pomocí přenosové technologie

Využití použité technologie pro šifrování přináší výhody v podobě jednoduchosti, ale má i několik nevýhod. Šifrování je omezeno pouze na přenosovou cestu, po změně technologie je nutné implementovat jiné řešení. Výběr šifrovacích metod a jejich síla je omezena dle specifikací použité technologie. Správa klíčů může být problematická u takto roztříštěných řešení do samostatných celků.

V případě bezdrátových technologií by mělo být šifrování používané vždy jako základní ochrana dat před jejich odposloucháváním. V sítích využívaných v rámci HAN či NAN existují šifrovací mechanismy [1]:

- Wi-Fi – standard 802.11i definuje protokol WPA2. Ten nahrazuje zastaralé (a potenciálně zranitelné) protokoly WPA a WEP. WPA2 podporuje autentizaci pomocí předpřipravených hesel nebo pomocí standardu 802.1x. Pro šifrování dat se používá algoritmus AES.
- WiMax – standard 802.16e definuje podporu pro šifrování pomocí algoritmu 3DES/AES a také podporu EAP.
- ZigBee – standard 802.15.4 definuje několik variant pro šifrování a autentizaci dat. Využívá se algoritmus AES a režimu CCM.

8.2.2 Aplikační šifrovací protokol

Pro jednotlivé aplikace a specifické potřeby je možné implementovat šifrování a autentizaci přímo do protokolu aplikační vrstvy. Takové řešení nabízí největší flexibilitu při výběru technologií a algoritmů. Je pak na autorovi protokolu pro jaké šifrovací algoritmy, sílu klíče, autentizační algoritmy se rozhodne.

Směrovače, přepínače a další zařízení, která v sítí přeposílají data, nemusejí mít algoritmus implementovaný a nemohou manipulovat s obsahem zpráv. Implementace je však nutná na koncových zařízeních. Při komunikaci se zařízeními typu IED, PLC nebo smart metery je nutné vzít v potaz omezené paměťové prostředky a rychlost procesoru, aby bylo dané šifrování zpracovatelné.

Zásadním problémem u vlastního protokolu zůstává, že se jedná o nový protokol, který nebyl podroben praktickému nasazení. Mnoho zranitelností se objeví až po uvedení algoritmu do praxe. V případě zařízení ve Smart Grid síti se může jednat o rozsáhlý

problém. Objevením zranitelnosti by útočník měl možnost manipulovat s velkým množstvím dat a úprava algoritmu nebo odstranění chyby může značnou dobu trvat.

8.2.3 Protokoly TLS/SSL

Protokol SSL (secure sockets layer) a jeho nástupce TLS (transport layer security) byly vytvořeny pro poskytnutí bezpečnosti při přenosu dat přes internet. Využívá se asymetrická kryptografie pro autentizaci při výměně klíčů, během přenosu dat se využívá symetrická šifra a autentizační kódy zpráv pro zajištění integrity a důvěrnosti [54].

Dle modelu TCP/IP pracuje TLS/SSL jako nižší podvrstva na aplikační vrstvě. Dle OSI modelu, činnost TLS/SSL je zahájena na spojové vrstvě a následně pracuje v prezentační vrstvě. TLS je internetovým standardem IETF a jeho aktuální specifikace je definována v RFC 5246 a RFC 6176.

Staré verze protokolů SSL 1.0 a 2.0 již nejsou považovány za bezpečné. U protokolů SSL 3.0 a TLS 1.0 se vyskytuje potenciální zranitelnost zvaná BEAST, kterou je možné ošetřit. Nejnovější standardy TLS 1.1 a 1.2 jsou považovány za zcela bezpečné.

TLS podporuje několik variant algoritmů šifrování (AES, 3DES, RC4) i kontrolních součtů (MD5, SHA). Pro výměnu klíčů se využívá systému certifikátů RSA.

TLS se tak dá použít jako silný nástroj pro zajištění důvěrnosti a integrity zpráv. V některých případech se mohou vyskytnout problémy s využíváním certifikátů a jejich verifikace z odlehlých míst. Problém je možné vyřešit instalací kořenových certifikátů přímo do zařízení.

8.2.4 IPsec

IPsec (internet protocol security) představuje rozšíření protokolu IP o podporu autentizace a šifrování komunikace. Na rozdíl od protokolů TLS/SSL poskytuje zabezpečení na síťové vrstvě OSI modelu. Šifrování je možné využít mezi koncovými uzly, bránami nebo mezi bránou a koncovým uzlem [55].

IPsec byl vyvíjen společně s protokolem IPv6 a původně byl nutnou součástí implementace IPv6. V současnosti je označen jako volitelný doplněk pro IPv4 i IPv6.

Sada IPsec se skládá z několika protokolů:

- Authentication header (AH) – zajišťuje autentizaci a integritu datagramů,

- Encapsulating security payload (ESP) – zajišťuje důvěrnost, autentizaci i integritu datagramů,
- Security association (SA) – sada algoritmů pro činnost ESP a AH protokolů,
- Internet security association and key management protocol (ISAKMP) – framework pro autentizaci a výměnu klíčů,
- Internet key exchange (IKE) – konkrétní protokol pro výměnu klíčů.

IKE využívá certifikáty X.509, které mohou být před sdíleny nebo distribuovány pomocí DNS. Pro vytvoření symetrického klíče se využívají algoritmy Diffie-Hellman.

IPsec pracuje s šifrovacími algoritmy 3DES, AES, pro autentizaci zpráv se využívají algoritmy SHA1 a MD5.

Protokol IPsec může pracovat ve dvou režimech:

- Transportní režim – uživatelská data jsou šifrována. Původní IP hlavička šifrována není, ale je chráněna proti případné změně.
- Tunelovací režim – celý datagram je zašifrován a je vytvořena nová IP hlavička. Tunelovací režim může být použit pro vytváření VPN sítí.

8.2.5 Shrnutí

Zabezpeční důvěrnosti a integrity dat je možné řešit více způsoby. Na sdílených médiích je velmi vhodné využívat dostupné šifrovací mechanismy pro zajištění základní ochrany všech přenášených dat. Tento způsob se omezuje pouze na dané komunikační médium a neřeší možné problémy v dalších částech sítě.

Implementace vlastního šifrovacího algoritmu může být výhodná v mnoha případech, kdy je nutné přizpůsobit se náročným požadavkům na paměť, výkon procesoru nebo nízké datové toky. Zároveň tento způsob přináší velké nebezpečí v podobě pozdějšího objevení chyby nebo zranitelnosti v algoritmu a pomalé možnosti nápravy.

Protokoly TLS/SSL a IPsec představují řešení na aplikační a síťové vrstvě, které poskytuje široké možnosti. Oba způsoby využívají systém certifikátů X.509, který poskytuje flexibilní řešení pro autentizaci velkého množství zařízení. Při využívaní certifikátů je nutné zabezpečit certifikační autoritu, aby nedošlo ke kompromitování celé sítě.

8.3 Obecná bezpečnostní doporučení

Přestože není možné zcela odstranit všechna rizika, existuje několik základních přístupů, které se využívají k minimalizaci rizik [3, 14].

Mezi obecná doporučení patří:

- Modelování hrozeb – již při vývoji a návrhu systému umožňuje dopředu odhalit možné hrozby a zaměřit se na jejich odstranění.
- Segmentace – rozdělením problému do menších částí se snižuje možnost napadení a následky útoku by měly omezený dopad. V počítačových sítí je možné vytvářet samostatné segmenty a oddělit je pomocí stavových firewallů, které zajistí bezpečnost mezi nimi.
- Výchozí zákaz komunikace na firewallu – firewally by měly obsahovat pravidlo pro zakázání nedefinovaných přenosů. Na mnoha místech se využívá zablokování nedefinované příchozí komunikace, ale odchozí komunikace není takto striktně hlídána. Odchozí komunikace by měla být filtrována přes proxy servery, sníží se tak možnost, že by napadený počítač byl ovládán ze vzdáleného místa.
- Podepisování kódu a příkazů – podepisování kódu a příkazů omezí možnost útočníka podstrčit vlastní kód a příkazy do zařízení.
- Honeypot systémy – představují past na útočníky. Systém se navenek tváří jako zranitelný produkční systém, po jejich napadení je možné útočníky mást falešnými informacemi a získat informace o útočnících.
- Ochrana proti malwaru, IDS/IPS systémy – na všech systémech by měla být implementována ochrana proti malwaru. Antivirový software umožňuje předcházet napadení systému škodlivým softwarem. Systémy IDS/IPS umožňují předcházet útokům ze sítě.
- Šifrování – data by měla být šifrována při přenosu i při jejich uskladnění. Šifrování by se mělo týkat databází, disků i vyměnitelných médií a záloh.
- Management zranitelností – společnosti by měly využívat metodik pro management zranitelností, na základě jejich znalostí je možné využívat metodik pro analýzu a vyhodnocení rizik.
- Penetrační testování – metoda pro testování a vyhodnocování zranitelností. Penetrační testování simuluje útok a ověřuje tak skutečná rizika.

- Revize zdrojového kódu – revize zdrojového kódu by měly být součástí vývojového cyklu softwaru. Kontrola zdrojového kódu vyhledává možné zranitelnosti programu ještě před jeho zveřejněním.
- Zabezpečení konfigurace – mnoho systémů ve výchozím nastavení obsahuje mnoho potenciálních zranitelností. Před jejich uvedením do produkčního prostředí by měla být konfigurace zabezpečena (zablokování nepoužívaných a nebezpečných služeb, zavedení bezpečnostních opatření, ...).
- Silná autentizace – autentizace by měla být složena z více různých faktorů. Mezi samostatné faktory patří:
  - něco, co uživatel zná (heslo),
  - něco, co uživatel vlastní (smart card, RFID čip),
  - něco, co uživatel je (otisk prstu, oční sítnice).

  Při kompromitování pouze jednoho z faktorů (např. vyzrazení hesla) útočník nemůže získat přístup do systému. Silná autentizace by měla být využívána všude, kde se operuje s citlivými informacemi nebo se jedná o kritické prvky infrastruktury.
- Logování a monitoring – zaznamenávání informací a událostí představuje způsob, jak zjistit jakým způsobem byl útok proveden a co bylo jeho cílem. Logování by mělo být zajištěno na všech možných úrovních (aplikace, operační systém, síť).

9 ZÁVĚR

Cílem této diplomové práce bylo analyzovat technologii sítí Smart Grid, vyhodnotit možná bezpečnostní rizika při jejich používání a pro vybraná rizika navrhnout modely řešení.

Technologie Smart Grid představuje komplexní vylepšení a rozšíření stávajících elektrických rozvodných sítí. Smart Grid zavádí možnost obousměrné komunikace mezi zákazníkem a energetickou společností. Přenos dat je realizován v reálném čase a je možné zákazníka informovat o současném stavu, aktuální ceně elektrické energie a naopak od zákazníka získávat informace o aktuálním odběru elektrického proudu. Na základě těchto informací a informací ze senzorů na síti je možné vytvořit automatizované řízení rozvodné sítě. Systém pak může automaticky reagovat na různé výpadky a poruchy a vyřešit je včasným zásahem. Celkově Smart Grid sítě přinášejí zvýšení spolehlivosti, kvality a také finanční úspory.

Zavedením rozsáhlé komunikační infrastruktury a zapojení zákazníků do systému přináší zvýšené nároky na bezpečnost sítě. Mnoho uživatelů se může pokusit o různé manipulace a podvody. Dostupnost zařízení a komunikační sítě se může pokusit útočník využít k napadení energetické společnosti a k manipulaci s rozvodnou sítí. V práci bylo představeno značné množství potenciálních rizik, která by útočník mohl zneužít k napadení Smart Grid sítě. Následky takových činů mohou být např. odposlechnutí dat, finanční ztráty nebo i globální výpadek elektrického proudu.

V další části práce byla analyzována konkrétní rizika a navržena jejich možná řešení. V práci bylo popsáno množství rizik technologií AMI a DR, od obecných případů jako je odposlech dat, po podvádějící zákazníky. Popsány byly také problémy týkající se různých komunikačních technologií využívaných v oblastech sítě HAN a NAN. Do analýzy byly zahrnuty i bezpečnostní rizika SCADA systémů, webových aplikací a dalších technologií využívaných ve Smart Grid sítích.

Autentizace zařízení v síti je důležitou součástí zachování bezpečnosti a správné funkčnosti. Při komunikaci různých zařízení je nutné zajistit, aby data nebyla odesílána nebo přijímána od útočníka, který se za dané zařízení pouze vydává. Jako vhodné řešení se jeví využití systému PKI a založení autentizace na systému certifikátů a asymetrické kryptografii.

Přenos dat v síti Smart Grid je na mnoha místech realizován pomocí sdílených komunikačních médií (PLC nebo bezdrátové technologie). Je nutné zajistit důvěrnost a integritu takto přenášených dat. Jako vhodná a standardizovaná řešení byly vybrány protokoly TLS a IPsec. Oba protokoly poskytují široké možnosti uplatnění při zabezpečení

dat při jejich přenosu. Protokol TLS pracuje jako zabezpečení na aplikační vrstvě, IPsec představuje řešení na síťové vrstvě a rovněž umožňuje vytváření virtuálních privátních sítí.

Odstranit všechna rizika v sítích Smart Grid není možné. Je však nutné zásadní problémy řešit a daná rizika odstranit nebo minimalizovat. V práci byly dále popsány obecné bezpečnostní zásady a technologie využívané v oblasti informačních technologií pro zajištění bezpečnosti.

10 POUŽITÁ LITERATURA

[1] HOSSAIN, Ekram, Zhu HAN a H. POOR. *Smart grid communications and networking*. New York: Cambridge University Press, 2012, xxviii, 481 p. ISBN 978-110-7014-138.

[2] SOREBO, Gilbert N a Michael C ECHOLS. Smart Grid Security: An End-to-End View of Security in the New Electrical Grid. Boca Raton: CRC Press, 2011, xxvi, 302 s. ISBN 978-1439855874.

[3] FLICK, Tony a Justin MOREHOUSE. Securing the smart grid: next generation power grid security. Boston: Syngress, c2011, xxv, 290 p. ISBN 15-974-9570-0.

[4] GHANSAH, Isaac. *Smart Grid Cyber Security Potential Threats, Vulnerabilities And Risk* [online]. Sacramento, CA, 2009 [cit. 2013-05-01]. Dostupné z: http://www.energy.ca.gov/2012publications/CEC-500-2012-047/CEC-500-2012-047.pdf

[5] HORÁLEK, Josef a Vladimír SOBĚSLAV. Technologie a požadavky na inteligentní sítě pro Smart Grid. *Elektrorevue* [online]. 2012, č. 65 [cit. 2013-05-01]. ISSN 1213-1539. Dostupné z: http://www.elektrorevue.cz/cz/clanky/energetika–vykonova-elektronika–elektrotechnologie/0/technologie-a-pozadavky-na-inteligentni-site-pro-smart-grid/

[6] HORÁLEK, Josef, Vladimír SOBĚSLAV a Jan MATYSKA. Technology and requirements for intelligent smart grid network. *3rd International conference on Applied Informatics and Computing Theory: Applied informatics and computing theory (AICT 12)*. 1. vyd. Athens: World scientific and engineering academy and society, 2012, s. 275-281. ISBN 1790-5109 ISSN 978-1-61804-130-2.

[7] KNAPP, Eric a Joel LANGILL. *Industrial Network Security Securing Critical Infrastructure Networks for Smart Grid, SCADA, and Other Industrial Control Systems*. Burlington: Elsevier Science, 2011, 360 s. ISBN 978-159-7496-469.

[8] *Introduction to NISTIR 7628: Guidelines for Smart Grid Cyber Security* [online]. The Smart Grid Interoperability Panel Cyber Security Working Group. US, 2010 [cit. 2013-05-01]. Dostupné z: http://www.nist.gov/smartgrid/upload/nistir-7628_total.pdf

[9] AUTHORS: STAN MARK KAPLAN. *Smart grid: modernizing electric power transmission and distribution; energy independence, storage and security; energy independence and security act of 2007 (EISA); improving electrical grid efficiency, communication, reliability, and resiliency; integrating new and renewable energy sources*. Stan Mark Kaplan. Alexandria, VA: TheCapitol.Net, 2009. ISBN 978-158-7331-626.

[10] KNAPP, Eric D. a Raj SAMANI. *Applied Cyber Security and the Smart Grid: Implementing Security Controls into the Modern Power Infrastructure*. Waltham, MA: Syngress, 2013, 224 s. ISBN 9780124046382.

[11] METKE, Anthony R. a Randy L. EKL. Security Technology for Smart Grid Networks. *IEEE Transactions on Smart Grid*. 2010, vol. 1, issue 1, s. 99-107. DOI: 10.1109/TSG.2010.2046347. Dostupné z: http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=5460903

[12] ERICSSON, Göran N. Cyber Security and Power System Communication—Essential Parts of a Smart Grid Infrastructure. *IEEE Transactions on Power Delivery*. 2010, vol. 25, issue 3, s. 1501-1507. DOI: 10.1109/TPWRD.2010.2046654. Dostupné z: http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=5452993

[13] OHEIMB, David. IT Security Architecture Approaches for Smart Metering and Smart Grid. *Smart grid security: First International Workshop, SmartGridSec 2012, Berlin, Germany,*

December 3, 2012, revised selected papers. 2013, č. 1, 24 s. DOI: 10.1007/978-3-642-38030-3_1. Dostupné z: http://link.springer.com/10.1007/978-3-642-38030-3_1

[14] ALOUL, Fadi, A. R. AL-ALI, Rami AL-DALKY, Mamoun AL-MARDINI a Wassim EL-HAJJ. Smart Grid Security: Threats, Vulnerabilities and Solutions [online]. *International Journal of Smart Grid and Clean Energy*. 2012, č. 1 [cit. 2013-05-01]. ISSN 2315-4462. Dostupné z: http://www.aloul.net/Papers/faloul_ijsgce12.pdf

[15] ENISA. *Annex II. Security aspects of the smart grid* [online]. 2012 [cit. 2013-05-01]. Dostupné z: http://www.enisa.europa.eu/activities/Resilience-and-CIIP/critical-infrastructure-and-services/smart-grids-and-smart-metering/ENISA_Annex%20II%20-%20Security%20Aspects%20of%20Smart%20Grid.pdf/at_download/file

[16] *Guide for Assessing the Security Controls in Federal Information Systems and Organizations* [online]. Gaithersburg, 2010 [cit. 2013-05-01]. Dostupné z: http://csrc.nist.gov/publications/nistpubs/800-53A-rev1/sp800-53A-rev1-final.pdf

[17] OPEN INFORMATION SYSTEM SECURITY GROUP. *Information systems security assessment framework* [online]. 2006 [cit. 2013-05-01]. Dostupné z: http://www.oissg.org/files/issaf0.2.1.pdf

[18] HERZOG, Pete. ISECOM. *Open Source Security Testing Methodology Manual* [online]. New York, 2010 [cit. 2013-05-01]. Dostupné z: http://www.isecom.org/mirror/OSSTMM.3.pdf

[19] SOOD, V.K., D. FISCHER, J.M. EKLUND a T. BROWN. Developing a communication infrastructure for the Smart Grid. *2009 IEEE Electrical Power*. IEEE, 2009, s. 1-7. DOI: 10.1109/EPEC.2009.5420809. Dostupné z: http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=5420809

[20] BENNETT, C. a D. HIGHFILL. Networking AMI smart meters. In: *2008 IEEE Energy 2030 Conference: Atlanta, Georgia, 17–18 November 2008*. Piscataway, NJ: IEEE, c2008, s. 1–8. DOI: 9781424428502.

[21] GIRI, J., D. SUN a R. AVILA-ROSALES. Wanted: A more intelligent grid. *IEEE Power and Energy Magazine*. 2009, roč. 7, č. 2, s. 34-40. ISSN 1540-7977. DOI: 10.1109/MPE.2008.931391. Dostupné z: http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=4787534

[22] LOBO, F., A. LOPEZ, A. CABELLO, D. MORA, R. MORA, F. CARMONA, J. MORENO, D. ROMAN, A. SENDIN a I. BERGANZA. How to design a communication network over distribution networks. In: *Proceedings of International Conference and Exhibition on Electricity Distribution*. Stevenage: The Institution, 2009, s. 1-4. DOI: 0537-9989.

[23] GUNGOR, V.C. a F.C. LAMBERT. A survey on communication networks for electric system automation. *Computer Networks*. 2006, roč. 50, č. 7, s. 877-897. ISSN 13891286. DOI: 10.1016/j.comnet.2006.01.005. Dostupné z: http://linkinghub.elsevier.com/retrieve/pii/S1389128606000193

[24] PAOLINI, Monica. Empowering the smart grid with WiMAX. *Energy Central* [online]. 2010 [cit. 2013-04-24]. Dostupné z: http://www.energycentral.com/reference/whitepapers/103333/

[25] BUMILLER, Gerd, Lutz LAMPE a Halid HRASNICA. Power line communication networks for large-scale control and automation systems. *IEEE Communications Magazine*. roč. 48, č. 4, s. 106-113. ISSN 0163-6804. DOI: 10.1109/MCOM.2010.5439083. Dostupné z: http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=5439083

[26] GOLDSMITH, Andrea. *Wireless communications*. 1. publ. Cambridge, U.K: Cambridge University Press, 2004. ISBN 05-218-3716-2.

[27] FADLULLAH, Z M, M M FOUDA, N KATO, A TAKEUCHI, N IWASAKI a Y NOZAKI. Toward intelligent machine-to-machine communications in smart grid. *IEEE Communications Magazine*. 2011, roč. 49, č. 4, s. 60-65. ISSN 0163-6804. DOI: 10.1109/MCOM.2011.5741147. Dostupné z: http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=5741147

[28] DOBKIN, Daniel M. a Bernard ABOUSSOUAN. Low power Wi-Fi for IP smart objects. *GainSpan* [online]. c2009 [cit. 2013-04-24]. Dostupné z: http://www.gainspan.com/docs2/Low_Power_Wi-Fi_for_Smart_IP_Objects_WP_cmp.pdf

[29] NIST Priority Action Plan 2: Guidelines for Assessing Wireless Standards for Smart Grid Applications. *NIST* [online]. 2011 [cit. 2013-04-24]. Dostupné z: http://collaborate.nist.gov/twiki-sggrid/pub/SmartGrid/PAP02Objective3/NIST_PAP2_Guidelines_for_Assessing_Wireless_Standards_for_Smart_Grid_Applications_1.0.pdf

[30] LAVERTY, David M, D John MORROW, Robert BEST a Peter A CROSSLEY. Telecommunications for Smart Grid: Backhaul solutions for the distribution network. *IEEE PES General Meeting*. IEEE, 2010, s. 1-6. DOI: 10.1109/PES.2010.5589563. Dostupné z: http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=5589563

[31] Assessment of demand response and advanced metering. *Federal Energy Regulatory Commission* [online]. 2011 [cit. 2013-04-26]. Dostupné z: http://www.ferc.gov/legal/staff-reports/11-07-11-demand-response.pdf

[32] MOLINA, A., A. GABALDON, J.A. FUENTES a C. ALVAREZ. Implementation and assessment of physically based electrical load models: application to direct load control residential programmes. In: *IEE Proceedings - Generation, Transmission and Distribution*. 2003, roč. 150, č. 1, s. 61-. ISSN 13502360. DOI: 10.1049/ip-gtd:20020750. Dostupné z: http://digital-library.theiet.org/content/journals/10.1049/ip-gtd_20020750

[33] HOROWITZ, Stanley H. a Arun G. PHADKE. *Power System Relaying*. 3rd ed. Chichester: John Wiley, 2005. ISBN 04-707-5879-1.

[34] SANDSTROM, E. a J. WEISS. Cyber security. In: *International Symposium CIGRE/IEEE PES, 2005*. IEEE, 2005, s. 282-289. DOI: 10.1109/CIGRE.2005.1532753. Dostupné z: http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=1532753

[35] VARODAYAN, David P. a Grace Xingxin GAO. Redundant Metering for Integrity with Information-Theoretic Confidentiality. In: *2010 First IEEE International Conference on Smart Grid Communications*. IEEE, 2010, s. 345-349. DOI: 10.1109/SMARTGRID.2010.5622065. Dostupné z: http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=5622065

[36] MPITZIOPOULOS, Aristides, Damianos GAVALAS, Charalampos KONSTANTOPOULOS a Grammati PANTZIOU. A survey on jamming attacks and countermeasures in WSNs. *IEEE Communications Surveys*. 2009, roč. 11, č. 4, s. 42-56. ISSN 1553-877x. DOI: 10.1109/SURV.2009.090404. Dostupné z: http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=5343062

[37] Smart Grid. *Department of Energy* [online]. [2007] [cit. 2013-04-26]. Dostupné z: http://energy.gov/oe/technology-development/smart-grid

[38] Electricity grid in U.S. penetrated by spies. *The Wall street journal* [online]. 2009 [cit. 2013-04-26]. Dostupné z: http://online.wsj.com/article/SB123914805204099085.html

[39] Iran Confirms Stuxnet Worm Halted Centrifuges. *CBS News* [online]. 2010 [cit. 2013-04-26]. Dostupné z: http://www.cbsnews.com/2100-202_162-7100197.html

[40] KREBS, Brian. Cyber Incident Blamed for Nuclear Power Plant Shutdown. *The Washington Post* [online]. 2008 [cit. 2013-05-01]. Dostupné z: http://articles.washingtonpost.com/2008-06-04/news/36929595_1_systems-computer-nuclear-regulatory-commission

[41] KING, Jeff a Kevin LAUERMAN. ARP Poisoning Attack and Mitigation Techniques: A CSSTG SE Residency Program White Paper. *Cisco* [online]. c2010 [cit. 2013-05-01]. Dostupné z: http://www.cisco.com/en/US/prod/collateral/switches/ps5718/ps708/white_paper_c11_603839.html

[42] KING, Jeff a Kevin LAUERMAN. STP MiTM Attack and L2 Mitigation Techniques on the Cisco Catalyst 6500. *Cisco* [online]. c2010 [cit. 2013-05-01]. Dostupné z: http://www.cisco.com/en/US/prod/collateral/switches/ps5718/ps708/white_paper_c11_605972.html

[43] Tweet-a-Watt!: A safe and simple wireless power monitor. *Ladyada.net* [online]. 2011 [cit. 2013-04-26]. Dostupné z: http://www.ladyada.net/make/tweetawatt/

[44] WANG, Jie. *Computer network security theory and practice*. Online-Ausg. Berlin: Springer, 2009, 384 s. ISBN 35-407-9698-3.

[45] GHORBANI, Ali A., Wei LU a TAVALLAEE. *Network Intrusion Detection and Prevention*. New York: Springer US, 2010, 224 s. ISBN 03-878-8923-X.

[46] LEHTINEN, Rick, Deborah RUSSELL a G. T. GANGEMI SR. *Computer Security Basics*. 2. vyd. Sebastopol, CA: O'Reilly Media, Inc., 2011, 312 s. ISBN 9781449317058.

[47] PFLEEGER, Charles P. a Shari Lawrence PFLEEGER. *Analyzing computer security: a threat/vulnerability/countermeasure approach*. Upper Saddle River, NJ: Prentice Hall, c2012, xxxvi, 799 p. ISBN 01-327-8946-9.

[48] MCCULLOUGH, Jeff. *Deterrent and detection of smart grid meter tampering and theft of electricity, water, or gas* [online]. Raleigh, NC, c2010, 5 s [cit. 2013-05-01]. Dostupné z: http://www.energyaxis.com/pdf/WP42-1010A.pdf

[49] NEWMAN, Robert C. *Computer security: protecting digital resources*. Sudbury: Jones and Bartlett Publishers, c2010, xxviii, 453 s. ISBN 978-0-7637-5994-0.

[50] CIAMPA, Mark D. *Security guide to network security fundamentals*. 4th ed. Boston, MA: Course Technology, Cengage Learning, c2012, xxvi, 628 p. ISBN 11-116-4012-2.

[51] Public-key infrastructure. *Wikipedia* [online]. 2003, 25. 4. 2013 [cit. 2013-04-30]. Dostupné z: http://en.wikipedia.org/wiki/Public_key_infrastructure

[52] ISO 31000 - Risk management. *ISO - International Organization for Standardization* [online]. 2009 [cit. 2013-04-30]. Dostupné z: http://www.iso.org/iso/home/standards/iso31000.htm

[53] SUNDERKÖTTER, Malte. *Software Engineering Risk Management*. Munich: GRIN Verlag, 2004, 114 s. ISBN 9783638310970.

[54] RFC 5246 – The Transport Layer Security (TLS) Protocol: Version 1.2. *IETF* [online]. Geneva: Internet Society, 2005- [cit. 2013-04-30]. Dostupné z: http://tools.ietf.org/html/rfc5246

[55] RFC 6071 - IP Security (IPsec) and Internet Key Exchange (IKE) Document Roadmap. *IETF* [online]. Geneva: Internet Society, 2005- [cit. 2013-04-30]. Dostupné z: http://tools.ietf.org/html/rfc6071

[56] SHIPLEY, Peter. *TCP/IP and its weaknesses and vulnerabilities* [online]. Berkeley CA, 2001 [cit. 2013-05-01]. Dostupné z: www.dis.org/filez/vun-1s.pdf

[57] LOS, Rafal. Hacked Certificate Authorities - Nothing Left to Trust. *Infosec Island* [online]. 12. 9. 2011 [cit. 2013-04-30]. Dostupné z: http://www.infosecisland.com/blogview/16383-Hacked-Certificate-Authorities-Nothing-Left-to-Trust.html