UNIVERZITA HRADEC KRÁLOVÉ

PŘÍRODOVĚDECKÁ FAKULTA

KATEDRA FYZIKY

Principy bezpečnosti Smart Grid sítí

Diplomová práce

Autor: Lukáš Petr

Studijní program: N1701

Studijní obor: Fyzikální měření a modelování

Vedoucí práce: Mgr. Josef Horálek, Ph.D.

Hradec Králové květen 2016

Prohlášení

Prohlašuji, že jsem diplomovou práci vypracoval samostatně a že jsem v seznamu použité literatury uvedl všechny prameny, z kterých jsem vycházel.

V Hradci Králové dne 10. 5. 2016 Podpis:

Poděkování

Děkuji vedoucímu diplomové práce Mgr. Josefu Horálkovi, Ph.D. za odborné vedení diplomové práce, cenné rady a připomínky v průběhu zpracování této práce.

Také bych chtěl poděkovat Ing. Oldřichu Horákovi, Ph.D. za cenné rady a podporu při tvorbě práce a paní Mgr. Martině Kubíkové za jazykovou korekturu.

Anotace

PETR, L. Principy bezpečnosti Smart Grid sítí. Hradec Králové, 2016. Diplomová práce na Přírodovědecké fakultě Univerzity Hradec Králové. Vedoucí diplomové práce Mgr. Josef Horálek, Ph.D. 72s.

Tato diplomová práce se zaměřena na přestavení problematiky energetických sítí Smart Grid. Tento typ sítí je pomocí systémového přístupu rozdělen na jednotlivé subsystémy, pro které jsou analyzována a popsána možná bezpečnostní rizika. V závěru práce jsou navržena pro vybraná rizika modely jejich řešení.

Klíčová slova

Smart Grid, bezpečnost, měřící zařízení, IP protokol SCADA, síť

Abstract

PETR, L. Principles of security of Smart Grid networks. Hradec Králové, 2016. Diploma Thesis at Faculty of Science University of Hradec Králové. Thesis Supervisor Mgr. Josef Horálek Ph.D. 72p.

The diploma thesis focuses on introducing problems of the energy net SmartGrid. This type of net is divided into subsystems for which the safety risks are described and analyzed. The last chapter deals with possible solutions to the safety risks.

Keywords

Smart Grid, security,IP protocol, advanced metering infrastructure, SCADA, network

Obsah

Úvod

Energetická náročnost našich životů je v dnešní době vyšší než kdykoliv v minulosti. Elektrická energie a její využití se na počátku nového tisíciletí staly každodenní potřebou pro většinu obyvatel Země. V porovnání s lidským organismem, který pro svou činnost potřebuje denně přijmout cca 7000 kJ, naše spotřeba v České republice odpovídá v průměru 55 MJ na obyvatele denně. Přestože jsou současné rozvodné sítě i elektrárny svou kapacitou značně naddimenzované, značné problémy a vysoké náklady v energetice tvoří nedostatečné možnosti v sledování poptávky na odběr energie domácnostmi a podniky, dále znemožňuje kvalitně sledovat zatížení přenosové a distribuční soustavy a na základě toho a regulovat výrobu (konvenční i z obnovitelných zdrojů) a transport elektrické energie.

Myšlenka SMART Grid sítí byla představena v roce 2006 a způsobila evoluci rozvodných sítí, kdy k samotné přenosové soustavě přidává komunikační prvek, který spojuje domácnosti, transportní společnosti i energetické výrobce v jeden informační kanál. Tak se umožnila obousměrná komunikace v reálném čase a elektrárny tak mohou informovat zákazníky o své spotřebě, energetické společnosti mohou monitorovat stav sítě, obchodovat s energiemi v reálném čase a transportní společnosti řídit přenosovou soustavu na dálku. Mezi hlavní cíle této technologie patří zefektivnění činnosti rozvodných a transportních soustav, vytvoření soustavy schopné pružně reagovat na potřeby zúčastněných stran, ale také umožnit efektivní připojení „zelených zařízení“ pro tvorbu i spotřebu energie (obnovitelné zdroje, elektromobily), ale také zařízení z oblasti internetu věcí, který v současné době prochází evolučním boomem.

Cílem této práce je popsat principy Smart Grid sítí, identifikovat možná bezpečností rizika s ohledem na modely běžných datových sítí a navrhnout jejich eliminaci.

Cíle a metody

Cílem diplomové práce je popsat principy Smart Grid sítí a analyzovat možná bezpečností rizika. Součástí diplomové práce bude i návrh modelu řešení zabezpečení vybraných bezpečnostních rizik.

Cíle a metody teoretické části

Dílčími cíli teoretické části práce jsou:

- definovat pojem inteligentní síť (Smart Grid),
- popsat principy fungování sítě,
- popsat principy bezpečnosti datových sítí,
- identifikovat možná bezpečností rizika Smart Grid sítí.

Těchto cílů bude dosaženo zpracováním literární rešerše odborné literatury a elektronických zdrojů.

Cíle a metody praktické části

Dílčím cílem praktické části diplomové práce je navrhnout modely řešení vybraných bezpečnostních rizik s přihlédnutím k bezpečnostním modelům běžných datových sítí.

Teoretická část práce

1 Inteligentní sítě

Inteligentní sítě neboli Smart Grid jsou sítě, které monitorují odběr i dodávku jednotlivých energií a umožnují tak regulaci výroby a její optimální přenos od elektrárny přes tranzitní a distribuční soustavu až ke koncovému zákazníkovi. Nosným základem celé této technologie jsou data o stavu sítě, které je nutné dostat co nejrychleji do řídících center distributorů a výrobců, tato data jsou však také poskytována i spotřebitelům a díky tomu mají možnost detailně sledovat svojí aktuální spotřebu, aktuální cenu jednotky energie. Spotřebitelé tak mají možnost hlídat své výdaje i v oblasti dodávek energií. Jako jednu z definic inteligentní sítě lze uvést:

„Pojem Smart Grid lze definovat jako inteligentní, samočinně se regulující elektrické sítě, schopné přenášet vyrobenou energii z jakéhokoli zdroje centralizované i decentralizované výrobny elektrické energie až ke koncovému zákazníkovi.“ [1]

nebo

„*Rozvodná síť budoucnosti bude rozšířenou verzí současné sítě s větším množstvím monitorovacích a komunikačních systémů, nových propojení, dvousměrným tokem energie a informací a větším podílem lokální výroby energie a energie z obnovitelných zdrojů. Systém bude vysoce automatizován, aby byly zajištěny spolehlivé, energeticky hospodárné dodávky energie pro odběratele energie z průmyslové, obchodní a soukromé sféry.“* [2]

nebo

Je to síť, která: „*zahrnuje distribuční síť inovovaného pojetí, která dokáže efektivně začlenit působení všech připojených uživatelů, centralizovaných i lokálních výrobních zdrojů energie, odběratelů s možností jejich aktivní role a začlenění nových funkcí distribuční sítě pomocí obousměrné komunikace mezi výrobními zdroji a spotřebiči.*“ [3]

Díky tomu, že data o aktuální spotřebě mají jak zákazníci, tak dodavatelé vždy okamžitě dostupné, je možné energii účtovat okamžitě a lze tak odstranit zavedený systém

fakturačních období, které zpravidla fungují na principu ročního zúčtování s měsíčními zálohovými platbami. I pro samotné distributory může tento typ sítě přinést další perspektivní obchodní modely v podobě nových tarifů spotřeby energie a mohou tak nabídnou širší portfolio cen, tak jako jsme zvyklí například u mobilních operátorů.

Z analogie obchodních modelů mobilních operátorů lze predikovat rozvoj v oblasti okamžitých změn tarifů, limitů pro spotřebu energie (obdoba FUP), lze si také představit napojení inteligentních zařízení v zahraničí a plateb svému smluvnímu dodavateli, jako je tomu třeba u roamingových služeb, a mnoho jiných parametrů dané služby.

Informace poskytované touto sítí a možnost řízení prvků lze také využít v mimořádných situacích, kdy výsledek rozhodovacího procesu podpořeného přesnými a aktuálními daty může zabránit kolapsu elektrické sítě. Zdroj [3] uvádí jako výhody této technologie následující:

Spotřebitelé:

- Využití nových tarifů,
- Možnost okamžitého sledování spotřeby,
- Snížení neoprávněných odběrů,
- Vzdálený online odečet dat,
- Podpora pro dodávky od spotřebitelů.

Dodavatelé:

- Přehled o odběrných místech,
- Sběr dat pro DDS,
- Zkvalitnění dispečerského řízení,
- Vzdálené ovládání měřidel.

1.1 Historie světové energetiky

Celosvětovým trendem současné doby v oblasti energetiky jsou různé ekologické směry v oblasti výroby a spotřeby energií. První náznaky tohoto hnutí lze datovat na počátek 70. let 20. století, kdy začala na mezinárodní úrovni jednání o existenci, možnostech a důsledcích globálního oteplování. Tento problém je do současnosti přiřazován největší měrou k zvyšování koncentrace skleníkových plynů v atmosféře vlivem spalování fosilních paliv při průmyslové výrobě a výrobě energií. Roku 1979 se v Ženevě pod záštitou OSN konala konference na téma globálního oteplování. [4]

Tato konference zažehla mnoho dalších jednání v otázce globálního oteplování a roku 1992 vznikla v Riu de Janeiru v Brazílii Rámcová úmluva Organizace spojených národů (dále jen OSN), která přinesla základní principy a obecné závazky. Konkrétní závazky a konkrétní cíle obsahuje však až Kjótský protokol (1997), jež se stal prvním právním podkladem pro snižování emisí skleníkových plynů na přijatelnou úroveň. [5]

1.2 Transformace tradičních sítí až do sítí Smart Grid

V Kjótském protokolu k Rámcové úmluvě OSN o změně klimatu z prosince roku 1997 se nostrifikující země zavázaly do konce prvního kontrolního období, mezi roky 2008 a 2012, snížit emise skleníkových plynů nejméně o 5,2% oproti stavu odpovídajícímu roku 1990. [4]

V prosinci roku 2012 byl na konferenci smluvních stran schválen dodatek, kterým bylo zajištěno pokračování v plnění Kjótského protokolu a stanoveno jeho druhé kontrolní období na léta 2013 až 2020. V rámci tohoto dodatku se některé země zavázaly přijmout nové omezující závazky pro snížení emisí alespoň o 18% oproti roku 1990. [5]

Řídícím dokumentem v rámci celoevropské spolupráce v rámci Evropské unie (dále jen EU) je dokument s názvem **Strategic Energy Technology Plan** (SET Plan), jehož smyslem a účelem je:

- snížit do roku 2020 emise o 20 % oproti úrovni klíčového roku 1990,
- **zvýšit energetickou účinnost** v EU o 20 %,
- zvýšit podíl **obnovitelných zdrojů energií** v celkové spotřebě v rámci zemí Unie na 20 %.

V rámci tohoto plánu SET bylo roku 2010 započato činností EEGI (Evropské průmyslové iniciativy pro chytré sítě). EEGI je spolek distributorů energií a technologických společností, které kladou důraz na rozvoj konceptů Smart Gridových sítí. V rámci této iniciativy byla vytvořena množina demonstračních projektů po celé Evropě, jejichž cílem je vyvíjet a testovat nové funkční celky Smart Gridových sítí. V rámci této skupiny působí i česká společnost ČEZ. [6]

Mezi základní legislativní předpisy patří dle [7] směrnice:

- 2009/29/ES, kterou se mění směrnice 2003/87/ES o obchodování s povolenkami na emise skleníkových plynů,
- 406/2009/ES rozhodnutí o rozdělení úsilí k dosažení redukčních cílů emisí skleníkových plynů,
- 2009/28/ES **o podpoře využívání energie z obnovitelných zdrojů**.

Na základě zmíněných předpisů vyvíjejí členské státy Unie řadu iniciativ a v mnoha z nich byly vytyčeny shodné hlavní cíle, které uvádí [8]:

- Tvorba skutečného vnitřního trhu s energií (konkurenceschopný, integrovaný a propojený trh),
- Zaručit zabezpečení dodávek energií,
- Snížení emisí skleníkových plynů (**energetická účinnost**, **obnovitelné zdroje**),
- Neustálý rozvoj energetických technologií,
- Společná mezinárodní energetická politika.

V rámci České republiky (dále jen ČR) byla v roce 2004 schválena **Státní energetická koncepce**, jež definuje prioritní osy a cíle ČR v energetickém sektoru a popisuje konkrétní realizační nástroje energetické politiky českého státu. V rámci republiky vznikl také tzv. **Akční plán energetické účinnosti**, který navazuje na směrnice Evropského parlamentu a Evropské rady 2006/32/ES **o energetické účinnosti u konečného uživatele a o energetických službách**.

S přihlédnutím k dostupným energetickým technologiím nebylo možné zmíněných cílů dosáhnout, proto jako jedno z východisek vznikl roku 2006 koncept Smart Grid, považovaný za budoucnost moderní inteligentní energetiky.

1.3 Současný stav inteligentních sítí

Základním cílem technologie inteligentních sítí je redukce odchylek mezi aktuální výrobou energií na straně dodavatelů energií (i domácností produkujících elektřinu formou např. fotovoltaických článků) a spotřebou energie na straně odběratelů. S ohledem na požadavky využití technologií pro výrobu energií z obnovitelných zdrojů se stává samotná výroba hůře predikovaná, jelikož je nutné neustále regulovat výkyvy v množství dodávané energie (fotovoltaické články i větrné elektrárny vyrábějí různé množství energie za různé meteorologické situace). Jedním z přínosů technologie Smart Grid je regulace spotřeby na základě aktuální výroby a dále přináší motivaci pro spotřebitele formou různých cenových hladin energie odpovídající tržním principům (střet nabízeného množství energie s poptávaným množstvím energie), což, jak je uvedeno na začátku této kapitoly do současnosti nebylo možné.

Společnost ABB v současné době provádí výzkum a vývoj v oblasti moderních energetických technologií a popisuje Smart Gridové sítě takto: *„Rozvodná síť budoucnosti bude rozšířenou verzí současné sítě s větším množstvím monitorovacích a komunikačních systémů, nových propojení, dvousměrným tokem energie a informací a větším podílem lokální výroby energie a energie z obnovitelných zdrojů. Systém bude vysoce automatizován, aby byly zajištěny spolehlivé, energeticky hospodárné dodávky energie pro odběratele energie z průmyslové, obchodní a soukromé sféry.“* [2]

V ABB svůj výzkum klasifikovali do následujících skupin [9]:

- Měření elektrické energie,
- Služby zákazníkům,
- Domácí automatizace,
- Regulace spotřeby,
- Distribuovaná výroba,
- Mikroregiony a mikrosítě,
- Zásobníky elektrické energie,
- Elektromobily,
- Stabilizace parametrů elektrických sítí,
- Specifické funkce monitorování, řízení a automatizace,

- Řízení toků v sítích,
- Virtuální elektrárny,
- Podpůrné a systémové služby,
- Dálkové přenosy elektrické energie,
- Stabilita distribučních a přenosových systémů.

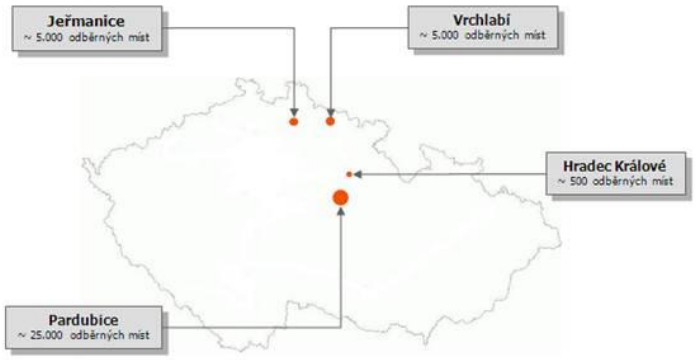
1.4 Pilotní projekty

V rámci SET Planu začaly země Unie realizovat pilotní projekty nasazení technologií Smart Grid. Evropské společenství nabízí v rámci rozvoje těchto technologií financování ze strukturálních fondů Unie. V této kapitole budou představeny pilotní projekty ve vybraných evropských zemích jako je Česká republika, Německo, Francie, Itálie a Španělsko.

Česká republika

Společnost ČEZ v rámci svého pilotního projektu nainstalovala do českých domácností kolem 30 000 inteligentních elektroměrů, které měří spotřebu elektrické energie. Tyto měřicí přístroje jsou zkušebně instalovány ve čtyřech lokalitách a to v:

- Pardubicích,
- Hradci Králové,
- Vrchlabí,
- Jeřmanicích. [3]



Obrázek 1 - Mapa testování na území ČR

Zdroj: [3]

Autoři v [3], [10] také detailněji popisují testovací oblast Vrchlabí v rámci projektu Smart Region ve Vrchlabí, kde ČEZ nasazuje nejmodernější technologie do distribuční sítě a testuje provoz inteligentních elektroměrů včetně zapojení koncových zákazníků. Při realizaci toho projektu je použito k řízení sítě prostředků informačních technologií a jsou zapojeny lokální výrobní zdroje.

Obrázek 2 - Technologie v tzv. smart house na sídlišti Liščí kopec

Zdroj: [10]

Projekt je z velké části financován ze strukturálních fondů Evropské unie a z rozpočtu České republiky. [3]

Německo

V SRN byl v roce 2009 spuštěn projekt výstavby chytré sítě v průmyslové oblasti Karlsruhe-Stuttgart na jihu Německa pod názvem MeRegio pod záštitou konsorcia firem a univerzity Karlsruhe. Do projektu je zapojeno kolem 1000 odběratelů (domácnosti, průmysl, výrobní a skladovací jednotky). [3], [52]

Dalšími realizovanými projekty na území Německa jsou například projekt Model City Manngeim (někdy také MoMa) a mnoho dalších projektů, které si samostatně vyvíjejí velcí provozovatelé distribučních sítí (RWE, E.ON, aj.). [3]

Německo je v současné době považováno za „mekku“ obnovitelných zdrojů, jelikož jsou zde obnovitelné zdroje výrazně podporovány vládou, což jde v ruku v ruce s opuštěním jaderné energetiky v této zemi.

Francie

V březnu 2010 distribuční společnost ERDF spustila ve dvou regionech pilotní projekt Smart Grids, zahrnující na 300 tisíc domácností. Na základě poznatků z tohoto testování pak v letech 2012 až 2017 proběhne instalace Smart Meters v 35 milionech francouzských domácností. ERDF také spouští rozsáhlý projekt s novou architekturou na úrovni nízkonapěťových i vysokonapěťových distribučních sítí na jihu Francie, v příměstské části Nice. Projekt bude zahrnovat integraci lokálních výrobních zdrojů, testování konceptu active demand response, jednotek akumulace elektrické energie, testování infrastruktury dobíjecích stanic i konceptu chytrých budov, tzv. smart homes.[3]

Itálie

V Itálií platí od roku 2006 vládní nařízení na povinnou instalaci Smart měřících zařízení, dle tohoto nařízení mělo být osazeno 95% odběrných míst těmito měřícími zařízeními. Doposud je realizováno pouze 85% celkového počtu italských domácností (odpovídá 32 milionům domácností). V jižní Itálii připravuje společnosti Enel projekt na testování aktivního řízení decentralizovaných zdrojů a spotřeby na vysokonapěťové úrovni distribuční sítě, předpokládá se zapojení 8 tisíc odběratelů a decentralizované zdroje (hlavně VTE[1] a FVE[2]). [3]

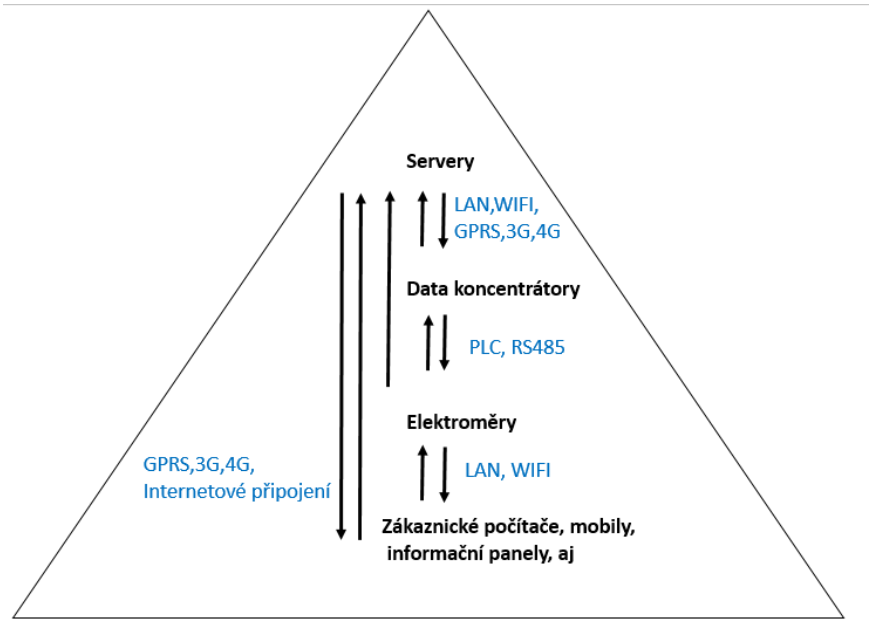
Španělsko

Energetická firma Iberdrola spustila v roce 2010 pilotní projekt v regionu Valencie (region Castellón). Na 100 tisíc domácností je v tomto regionu již vybaveno Smart Meters. Projekt pokračuje s cílem vyzkoušet řízení nn a vn distribučních sítí pomocí víceúrovňového řešení implementace Smart Meteringu. Energetická společnost Endesa v roce 2009 spustila čtyřletý pilotní projekt SmartCity v lokalitě Málaga. [3], [53]

[1] VTE - větrná elektrárna
[2] FVE - fotovoltaická elektrárna

1.5 Popis komponent v inteligentních sítích

V následující kapitole budou představeny základní komponenty inteligentních sítí, jejich pyramidová struktura je znázorněna na obrázku č. 3.



Obrázek 3 - Pyramidová struktura komponent

Zdroj: [vlastní]

Elektroměry

Pomocí elektroměrů je měřeno napětí v odběrném místě, maximum výkonu, ale hlavně spotřeba elektrické energie. Jsou zde zachyceny různé události a další užitečná data. Elektroměr může vykonávat úkony jako odpojení zákazníka od distribuční sítě, limitování odběru (FUP), změnu tarifu, spínání relé v závislosti na tarifu, apod. V elektroměru se může nacházet modem pro PLC síť, po které jsou data přenášena na data koncentrátor. Modem může být zhotoven modulárně nebo jako součást elektroměru. Mezi další způsoby komunikace patří přenos pomocí mobilních sítí (GPRS, 3G, 4G), který je využíván v místech, kde selhává PLC, v tomto případě jsou data přenášena přímo na server. Mezi další možnosti patří rádiový přenos na data koncentrátor.

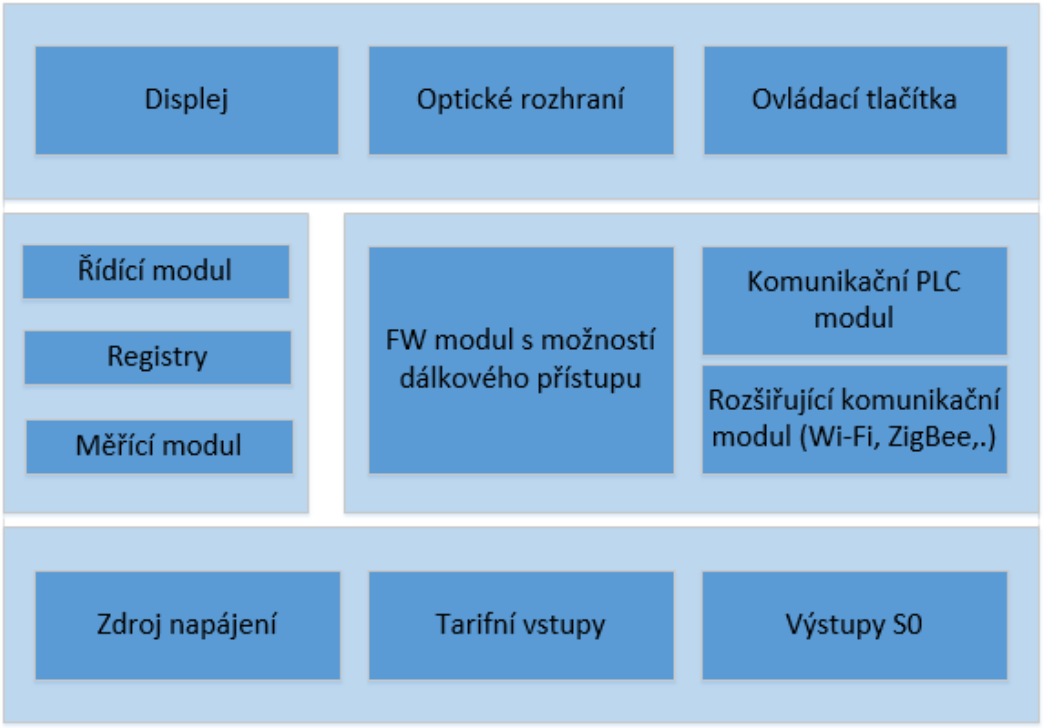
Součtový elektroměr v rozvaděči nebo elektroměr instalovaný v průmyslové společnosti může být připojen k data koncentrátoru metalickým vedením jako je RS-485, M-BUS, Ethernet a další.

Popis smart metru

Základním požadavkem distributorů pro výrobce smart měřidel je měření veličin v dané přesnosti, archivace dat, komunikace s okolím, spolehlivost a přijatelná cena. Soustava elektroměru je tvořena měřicím transformátorem, Hallovou sondou a Rhogowského cívkou. Naměřené veličiny lze prostřednictvím smart meteru vyhodnotit. Měřenými a vyhodnocovanými veličinami jsou například:

- Efektivní hodnota napětí (URMS),
- efektivní hodnota proudu (IRMS),
- činný výkon (P),
- jalový výkon (Q),
- účiník (cosφ),
- frekvence (f).

Součástí měřicího modulu je také univerzální mikroprocesor s AD převodníkem, který se postará o výpočet a další zpracování dat vedlejších požadovaných veličin. Do paměti elektroměru jsou zaznamenávány hodnoty činného výkonu v daných časových intervalech (např. 15 min). Dále jsou ukládány průměrné hodnoty proudu a napětí v daných intervalech po fázích. Je možné zvolit různé periody vyhodnocení pro záznam (15min, 24h,…).



Obrázek 4 - Koncepce měřicího zařízení

Zdroj:[autor]

Archivace událostí je řešena pomocí záznamníku událostí, který sleduje a ukládá vybrané události s časovou značkou. Příkladem registrovaných událostí je například výpadek napětí nebo napadení elektroměru. V případě fyzického napadení elektroměru je elektroměr schopen detekovat otevření krytu svorkovnice, silné magnetické pole v blízkosti elektroměru a potenciálně nebezpečnou komunikaci přes optické rozhraní. Tyto události (po opatření časové značky) vyšle do řídicího centra a vyvolá tak podnět pro návštěvu techniků distributora s podezřením na neoprávněný zásah do měřicí soustavy.

Komunikace v místě měřícího zařízení je řešena displejem umístěným na elektroměru a domácím displejem propojeným přes radiové rozhraní elektroměru (případně GPRS nebo ZigBee). Pro vzdálenou komunikaci s řídicím centrem elektroměr používá technologie uvedené v kapitole 2.3.1

Data koncentrátory

Data koncentrátor představuje mezistanici, tedy rozhraní mezi přenosem dat po elektrické nebo rádiové síti a jiným přenosem, nejčastěji typu TCP/IP. Data koncentrátor se nachází v trafostanici (DTS), jelikož PLC přenos přes transformátor neprojde a pro energetickou společnost je velmi výhodné umístit jej do stávající instalace. Koncentrátor obsluhuje v průměru přibližně 100 elektroměrů, ale v případě sídlišť a jiných hustých zástaveb může počet elektroměrů překročit 1000. Data jsou na server zasílána prostřednictvím metalické sítě nebo Wi-Fi, v případě nedostupnosti těchto spojení, nebo jejich selhání je připraveno záložní řešení s využitím mobilních datových sítí (GPRS, 3G, 4G).

Servery

Na opačné straně distribučního kanálu se nachází server, který data zpracovává a vhodným způsobem ukládá a interpretuje. Některá data ze serverů jsou poskytnuta zákazníkům a jiný výběr dat je zase důležitý pro výrobu energií a řízení rozvodné sítě. Zaměstnanci operátorského a dohledového centra můžou zasílat příkazy a měnit tak stav jednotlivých zařízení. Díky tomu můžou předejít kolapsu sítě, nebo nastavit levnější tarif pokud je přebytek elektrické energie v síti.

Klientské počítače, mobilní telefony, informační panely

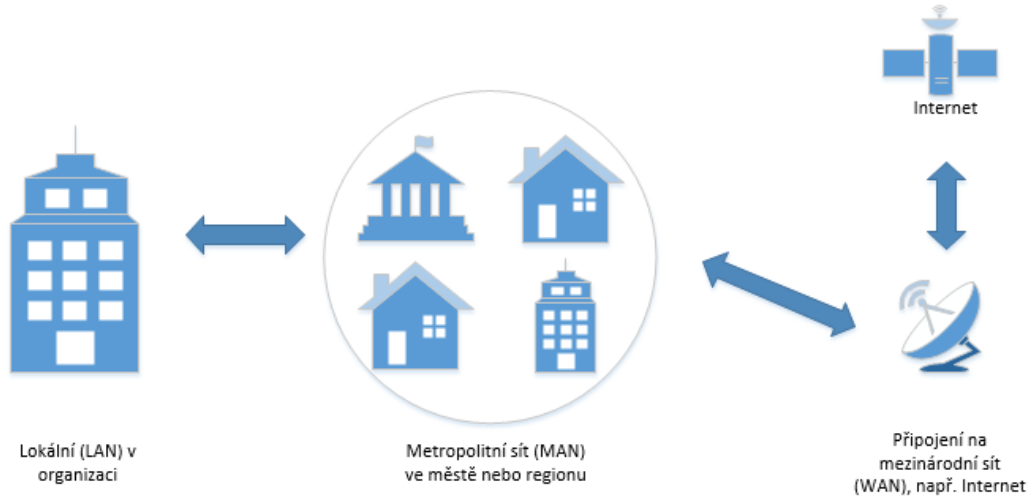
Pomocí těchto zařízení je zákazník informován o aktuálním stavu spotřeby, aktuálním tarifu a jiných užitečných informacích, které mu umožňují měnit spotřebu, tarif, či sledovat aktuální vyčerpaný balík elektrické energie a tím efektivně hospodařit s energiemi a uspořit náklady.

2 Topologie datové sítě a komunikační technologie

Topologie datové sítě Smart Grid je od klasické datové sítě odlišná, avšak využívá obdobný hierarchický přístup k její organizaci a splňuje teoretické vlastnosti přenosu dat pomocí modelu ISO/OSI. V této kapitole bude představen nejprve model klasické datové sítě a model sítě Smart Grid a referenční model pro přenos dat ISO/OSI.

2.1 Klasické datové sítě

Klasické datové sítě se dělí dle velikosti do kategorií LAN (local area network), MAN (metropolitan area network), WAN (wide area network), SAN (storage area network) a PAN (personal area network). Sítě PAN a SAN představují speciální typy sítí, kdy PAN je malá sít tvořená osobními zařízeními jako je mobilní telefon, pda, notebook v blízkosti jedné osoby, a SAN je speciální datová sít vytvořená v okolí serverů pro připojení externích zařízení, oba tyto speciální typy sítí nebudou dále v této práci uvažovány.



Obrázek 5 - Dělení datových sítí dle rozlehlosti

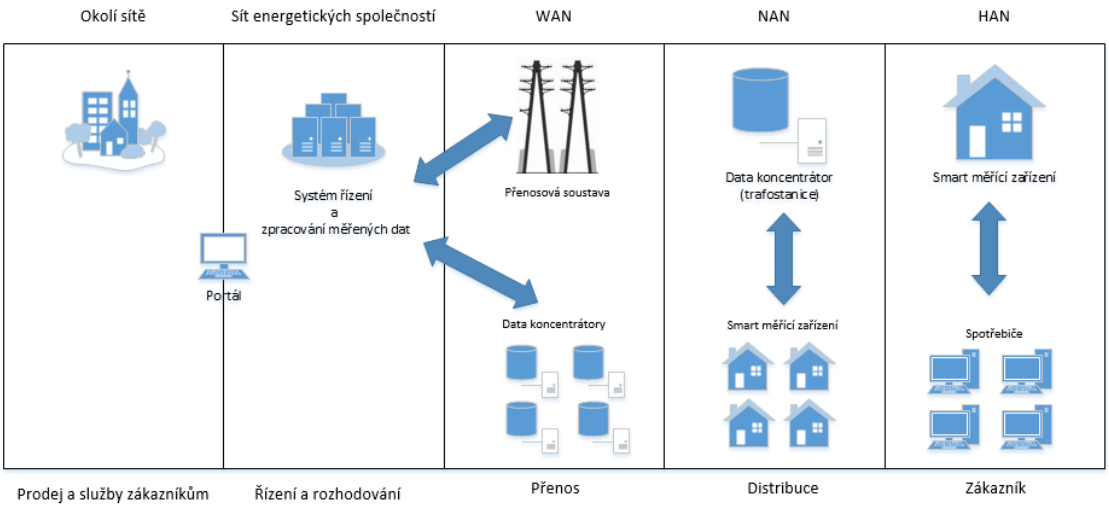
Zdroj: [autor]

Sít LAN tedy představuje nejmenší možnou síť, která se skládá z dvou až stovek počítačů v rámci jedné budovy či organizace (ohraničené danou lokalitou). Sítí MAN označujeme metropolitní sítě, které sdružují několik sítí LAN a svým rozsahem přesahují ohraničenou lokalitu. Obvykle jsou rozprostřeny v oblasti odpovídající městu či kampusu a připojují

danou lokalitu k WAN. Sítě WAN spojují vzdálená místa a jejich propojení v rámci světa tvoří mezinárodní datovou síť zvanou Internet.

2.2 Smart Grid sítě

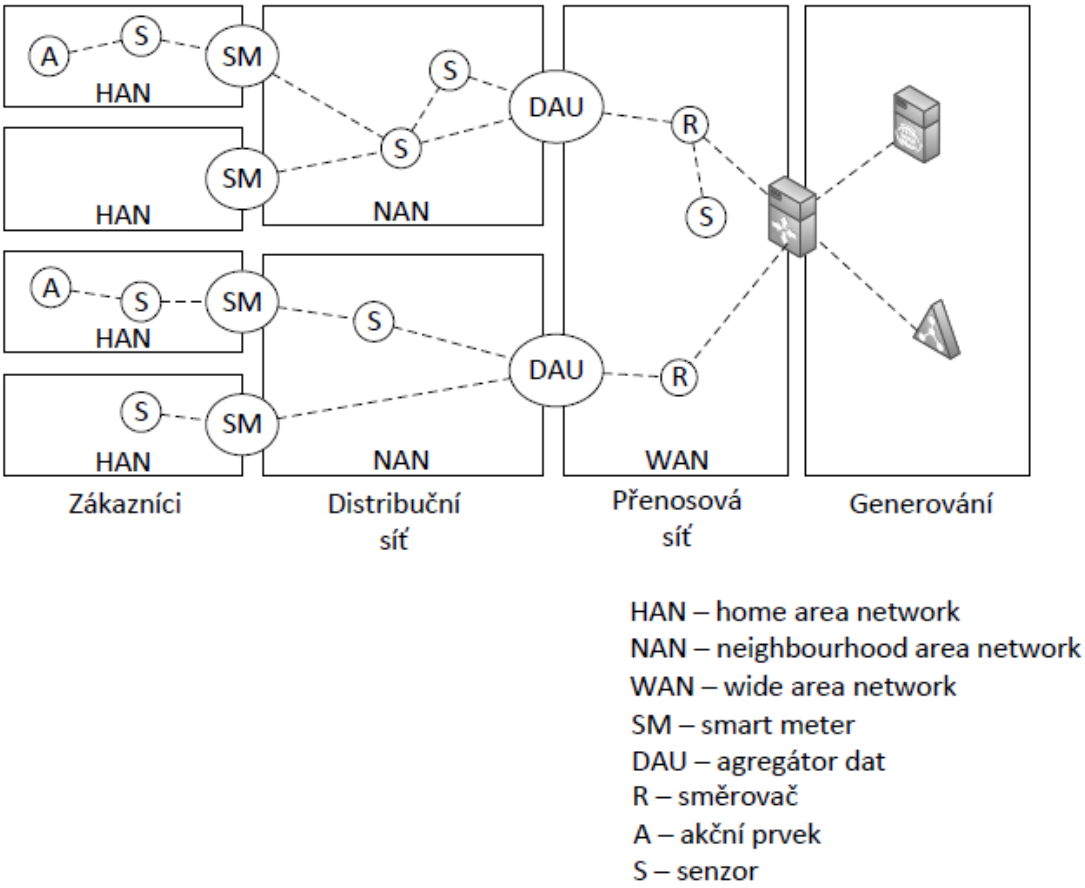
V Smart Gridových sítích je nejmenší logickou jednotkou budova zákazníka, či blok. Veškerá zařízení uvnitř budovy (za elektroměrem) patří do sítě HAN (home area network). Budovy v okolí jsou propojeny do nejbližší trafostanice (součástí je data koncentrátor) a tento vzniklý celek lze označit jako síť NAN (neighbourhood area network). Takto vzniklé oblastní NAN sítě jsou dále připojeny do WAN (wide area network) sítí energetických společností (enterprise). [12]



Obrázek 6 - Dělení Smart Gridové sítě dle rozlohy

Zdroj:[autor]

Do celé komunikační infrastruktury jsou také zahrnuty další (například poskytovatelé služeb, aj.), kteří představují okolí přenosového systému (external). Na následující ilustraci lze vidět příklad oblastí a obsažených zařízení v daných úrovních Smart Grid sítě.



Obrázek 7 - Komunikační infrastruktura inteligentní sítě

Zdroj: upraveno podle [13]

2.2.1 Sítě oblasti domácností

Sítě oblasti domácností (HAN) neboli home area network tvoří nejmenší topologický prvek Smart Gridové sítě, někdy též označovaný jako PAN (premise area network) nebo BAN (building area network). Tento typ sítě poskytuje prostředí pro řízení spotřeby elektrické energie a zapojuje zákazníka do procesu výroby elektrické energie. [13], [14]

V této síti se nachází inteligentní měřicí zařízení (smart meter) a také další zařízení se schopností využití správy spotřeby elektrické energie. [15]

Všechna Smart zařízení v této síti využívají ke komunikaci klasické komunikační prostředky jako je PLC WIFI, BACnet protokol, ZigBee. [13]

Mezi zařízení patřící do HAN lze dle [13], [15] zařadit:

- PCT (programmable commuicating thermostat) – termostat, který slouží pro řízení topení a ventilace,
- EMS (energy management system) – systém pro správu spotřeby energie,
- IHD (inhome display) – spolu s EMS umožňuje rozšíření poskytovaných služeb klasických termostatů a umožnuje řízení chytrých spotřebičů,
- PEV (plug-in electric vehicle) – elektrické vozidlo schopné nabíjet se ze sítě, ale také energii do sítě dodávat

2.2.2 Sítě oblasti sousedství

Sítě NAN (Neighbourhood area network) představují oblasti připojených HAN do jedné trafostanice a představují tak agregační místo. Nejčastěji se jedná o připojení domácností a objektů v blízkém okolí sítě. NAN představuje agregační místo pro připojení většího množství domácností, k vlastní agregaci a jako komunikační rozhraní slouží zařízení DAU. které následně přeposílá data od jednotlivých zákazníků do sítě WAN. [13], [16]

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

2.2.3 Rozsáhlé sítě

WAN jsou naprostou analogií jako v klasických datových sítích a představují rozsáhlou síť, která propojuje jednotlivé sítě NAN (v klasických sítích MAN) do podnikové sítě energetické společnosti. [13]

WAN sítě mohou být založeny na mnoha různých technologiích, například na Ethernetu, mobilní síti, broadband připojení, apod. [13]

2.2.4 Síť energetických společností

Všechna data získaná na nižších vrstvách sítě (HAN, NAN) jsou přeposílána do podnikových sítí prostřednictvím WAN, kde jsou následně analyzována. Nacházejí se tu také servery a řídící centra pro technologie SCADA a WAMS. Komunikace uvnitř podnikových sítí je technologicky postavena na Ethernetu a spoje realizované pomocí kroucené dvojlinky či optických vláken. [13]

2.2.5 Okolí sítě

Mezi externí objekty jsou zahrnuty poskytovatelé služeb, obchodníci s elektrickou energií a další subjekty, které zasahují do procesů souvisejících s dodávkou elektrického proudu. Externí entity mohou poskytovat různé služby a procesy pro zákazníky. [13]

2.3 Vrstvy referenčního modelu ISO/OSI

Referenční model OSI je obecný model architektury propojení otevřených systémů definovaný normou ISO 7498. Cílem tohoto modelu je poskytnout základ pro koordinované vypracování norem pro síťovou komunikaci. Tento model je formální (všeobecný) a nestanovuje žádné přesně definované postupy, jak technicky realizovat přenos v rámci sítě. ISO/OSI se tedy používá jako názorný příklad řešení komunikace v sítích. Jak je z obrázku patrné, tento model je sedmivrstvý. Cílem této práce není podrobné představení komunikačního modelu ISO/OSI, ale pouze přehled. Podrobný rozbor ISO/OSI lze nalézt například v [55].

Obrázek 8 - Referenční model ISO/OSI

Zdroj: [17]

Tento Smart gridový model sítě je postaven na stejném základu ISO/OSI, jako jsou datové a komunikační sítě. Z pohledu přenosu dat lze na Smart gridové sítě pohlížet prostřednictvím tohoto referenčního modelu. [18]. [19], [14]

Cílem této práce je popsat principy sítí Smart Grid a identifikace bezpečnostních hrozeb, proto budou v dalších kapitolách popsány pouze vrstvy modelu, které přímo souvisejí se samotným přenosem dat.

2.3.1 Fyzická vrstva

Nejnižší vrstva ISO/OSI, která zprostředkovává fyzický přenos dat v podobě bitů mezi odesílajícím zařízením a zařízením přijímajícím. Na této vrstvě se řeší technické parametry, jako jsou elektrické signály definující 0 a 1, typy konektorů, typ přenosového média, apod. Tato vrstva neřeší význam jednotlivých bitů, jen zajišťuje jejich samotný přenos. [18]

V sítích typu Smart Grid lze ke spojení zařízení použít následujících technologií:

- Power-line communications,
- Kroucená dvojlinka,
- Optické vlákno,
- Radiové technologie,
- Wi-Fi,
- WiMAX
- ZigBee,
- Mobilní sítě,
- Satelitní komunikace.

Power-line komunikace

Technologie power-line komunikace (dále jen PLC) je využívána k přenosu dat pomocí elektrického vedení. Datový signál je zde modulován na nosnou 50 Hz vlnu. PLC je již v elektrických sítích využíváno delší dobu, u nízkokapacitních spojů jsou využívány ke vzdálenému řízení zařízení. [20], [21]

Přenos dat přes elektrickou síť má tyto výhody a nevýhody[20], [21]:

Výhody:

- Lze využít stávajících elektrických rozvodů a není tak třeba realizovat nová spojení, nebo paralelní vedení datové sítě.

Nevýhody:

- Vedení přes transformátory je problematické a je nutné jej řešit přemostěním.
- Elektrické vedení představuje zdroj rušení, elektrické rozvody jsou taženy v nestíněných linkách a negativně je tak ovlivněn samotný signál elektromagnetickou interferencí.
- Při přerušení elektrického vedení dojde i k přerušení datového spojení.
- Nelze jednoznačně určit frekvenční kanály vzhledem k rozdílným podmínkám v různých částech sítě.
- Nízké přenosové rychlosti.
- Možnost odposlechu kvůli sdílenému komunikačnímu médiu.

Kroucená dvojlinka

Kroucená dvojlinka je moderní alternativou zastaralé technologie koaxiálních kabelů a je v současné době nejběžněji využívaným přenosovým médiem v datových sítích. Název kroucená dvojlinka vznikl z jejího technického provedení, kdy zakroucení párů vodičů snižuje (eliminuje) vliv okolního elektromagnetického rušení a přeslechy mezi vodiči.

Je to patrné z následující rovnice, ve které je elektrický potenciál na nosném vodiči φ_1 a na druhém vodiči v ideálním případě $\varphi_2 = 0V$. Signál U je pak dán vzorcem:

$$U = \varphi 1 - \varphi 2 \qquad (1)$$

Pokud však na pár působí elektromagnetické rušení, dojde vlivem elektromagnetické indukce k naindukování napětí $\Delta\varphi$. $\Delta\varphi$ je vlivem zakroucení vodičů (a tedy jejich totožné pozice v EM poli) naindukováno o stejné velikosti. Signál je pak dán vzorcem:

$$U = (\varphi 1 + \Delta\,\varphi) - (\varphi 2 + \Delta\,\varphi) \qquad (2)$$

Pomocí jednoduchých úprav získáme zpět původní vztah odečtením poruchového napětí.

V dnešní době se tento typ kabeláže nejvíce využívá pro rozvody v rámci jedné budovy. Pro přenosy na větší vzdálenosti se preferují optická vlákna či bezdrátové technologie.

Na kroucené dvojlince dosahuje přenosových rychlostí 10, 100, 1000 nebo 10000 Mb/s. Maximální délka kabelu je omezena na 100 metrů, poté je nutné využít opakovače signálu. Jedná se o P2P spojení, pro zapojení více zařízení do společného síťového segmentu je nutné využít přepínače (switch) či rozdělovačů (hub).

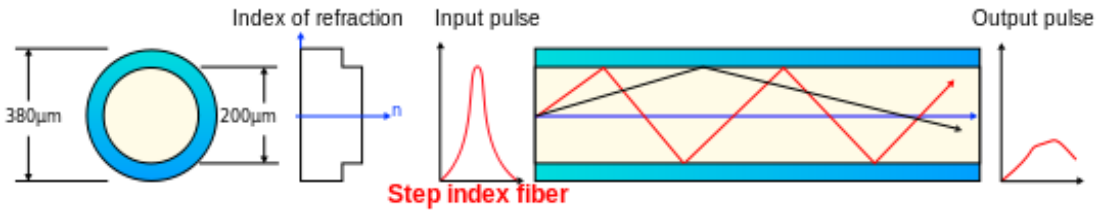
Optické vlákno

Optických vláken je využíváno k přenosu dat pomocí transformace elektrického signálu na elektromagnetické záření (ve světelném spektru). Světlo je vysláno diodou či laserem prostřednictvím optického vlákna, na jehož konci je fotodioda, která transformuje signál zpět na elektrický. [13]

Optická vlákna lze rozdělit na dvě kategorie:

- Jednovidová (single mode)
- Multividová (multi mode)

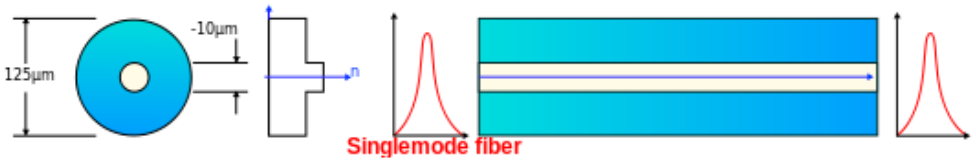
Multividová vlákna jsou využívána na kratší vzdálenosti a pro zvýšení kapacity přenosu dat. Pro vlastní přenos využívají více světelných signálů o různých vlnových délkách λ, avšak díky vzájemné interferenci signálů jej nelze použít na vzdálenosti vyšší než 2 km.



Obrázek 9 - Multividové vlákno

Zdroj: [23]

Jednovidová vlákna jsou využívána na delší přenosové vzdálenosti a vláknem je vysílán pouze jeden paprsek o specifické vlnové délce λ. Tomu musejí být přizpůsobeny i optické konvertory. Pomocí těchto vláken je dosahováno vzdáleností větších než 2km.



Obrázek 10 - Jednovidové vlákno

Zdroj: [23]

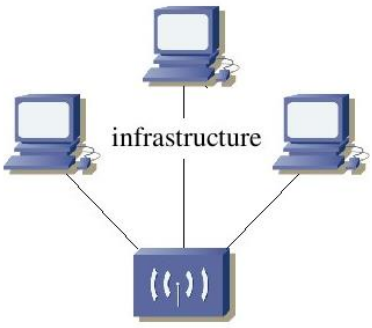
U optických vláken lze dosáhnout přenosových rychlostí až 10 Gbit. Samotný přenos pomocí světla nelze nijak ovlivnit vnějším elektrickým polem, optická vlákna tak mohou být pokládána v blízkosti vedení vysokého napětí, transformátorů, apod. Nedochází zde k přeslechům a samotný útlum je mnohem nižší než u metalických vodičů. Tento typ komunikace nelze odposlouchávat. Jedná se o P2P spojení a je nutné využít přepínačů pro zapojení více zařízení do sítě.

Radiové technologie

Rádiové technologie (RT) využívají k přenosu signálu elektromagnetického záření o frekvencích vyšších než infračervené záření. Bezdrátové technologie poskytují vyšší flexibilitu pro připojení nových zařízení, protože není nutné instalovat novou kabeláž.

Nevýhodou všech RT je citlivost na elektromagnetické rušení či rušení z jiných sítí využívajících stejná frekvenční pásma. Bezdrátové sítě je možné rozdělit na dvě skupiny dle způsobu organizace:

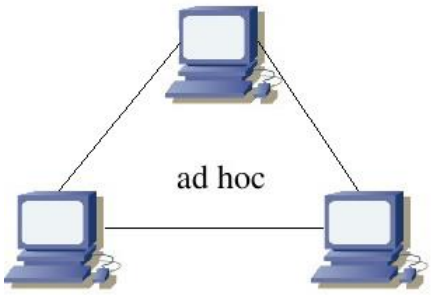
- **infrastructure** - využívají centrální přístupové body (AP – access point), které řídí jednotlivé klienty a komunikace probíhá skrze přístupové body,



Obrázek 11 - Infrastructure

Zdroj: [autor]

- **ad-hoc** - využívají decentralizovaný přístup; jednotlivé prvky sítě navazují spojení s blízkými prvky a předávají si zprávy přímo mezi sebou



Obrázek 12 - Ad-hoc

Zdroj: [autor]

Mezi rádiové technologie lze zařadit technologie, které budou rozebrány v následujících odstavcích a to: WIFI, WiMAX, ZigBee, satelitní komunikace a mobilní sítě.

Wi-Fi

Wi-Fi (Wireless Fidelity) představuje bezdrátovou technologii založenou na standardech IEEE 802.11. V současné době nalezla široké uplatnění v mnoha oblastech, především pro budování domácích a kancelářských sítí, nebo k poskytování internetového připojení na kratší vzdálenosti. Wi-Fi podporuje IP protokoly.[13].

Wi-Fi pracuje v pásmu 2,4 GHz (standardy 802.11 b, g, n) a 5 GHz (802.11 a) a dle použitého standardu dosahuje teoretických přenosových rychlostí 54 Mbit až 300 Mbit.

Wi-Fi sítě představují atraktivní a relativně lacinou 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 [24], [25]. Podrobnosti o této technologii lze nalézt například v [54].

WiMAX

Technologie WiMAX přestavuje bezdrátovou technologii přenosu dat založenou na standardech IEEE 802.16. [26].

Technologie poskytuje přenosové rychlosti až 140 Mbit s nízkou dobou odezvy do 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 (v příměstských oblastech na více jak 20 km).

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. Podrobnosti o této technologii lze nalézt například v [56].

ZigBee

Protokol ZigBee je tvořen skupinou ZigBee Aliance a představuje řešení pro bezdrátové přenosy na krátkou vzdálenost s nižším datovým tokem. ZigBee je definován standardem IEEE 802.15.4 [13].

Technologie ZigBee podporuje směrování a adresaci využitím stromové a síťové topologie. ZigBee je vhodnou technologií k tvoření bezdrátových senzorických sítí (WSN). Jako další možné využití se předpokládá bezdrátové propojení zařízení v domácnostech.

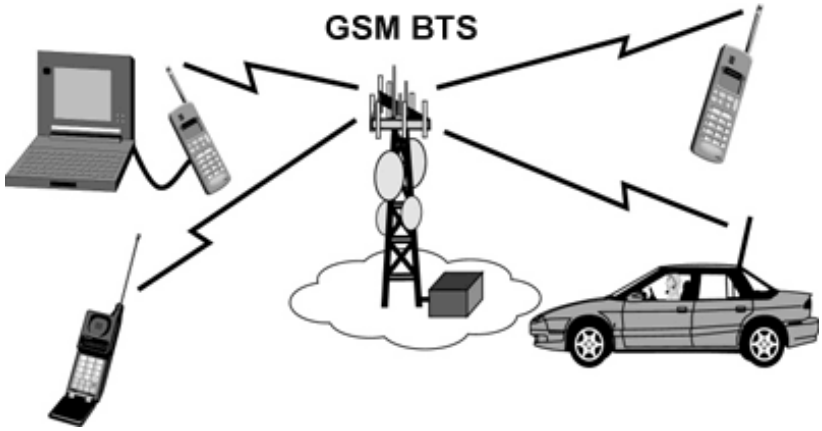
ZigBee rozlišuje tři typy zařízení:

- **koordinátor** - pracuje jako most do dalších sítí, řídí autentizační proces 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 koordinátorovi.

Podrobnosti o této technologii lze nalézt například v [57].

Mobilní sítě

Mobilní sítě poskytují bezdrátové připojení do celosvětové sítě Internet pro obrovské množství uživatelů ve většině míst světa. Oblasti působnosti jednotlivých operátorů jsou děleny do elementárních částí označovaných jako cells (buňky). Každá cell je řízena zařízením **Base transceiver station** (dále jen BTS), které řídí komunikaci všech zařízení komunikujících uvnitř cell. Základní předpokladem konstrukce mobilních sítí je, že signál z BTS a zařízení uživatelů je omezen pouze na jedinou buňku (analogie infrastructure). Jednotlivé rádiové kanály (frekvence) jsou tak opětovně používány v dalších buňkách. Mobilní sítě s využitím moderních technologií poskytují dostatečné přenosové rychlosti pro datová spojení [13].



Obrázek 13 - BTS

Zdroj: [26]

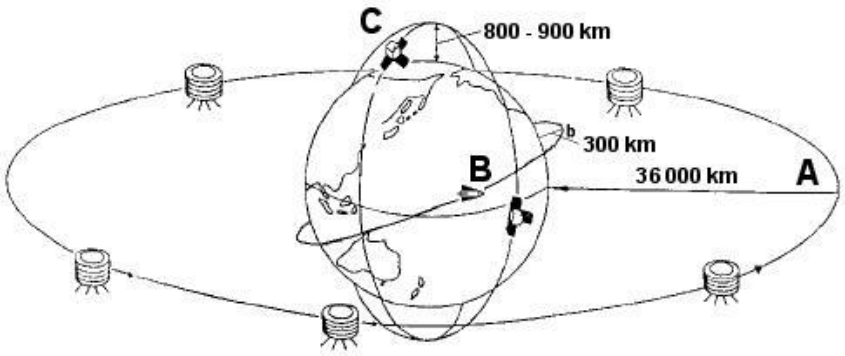
Technologie LTE představuje další pokrok v technologickém pokroku mobilních sítí, mnohonásobně zvyšuje rychlost přenosu dat a zároveň zachovává zpětnou kompatibilitu s 3G technologií. Pro přenos dat se využívá technologie MIMO a přístupové metody OFDMA. Teoretická přenosová rychlost LTE dosahuje až 300 Mb/s.

Satelitní komunikace

Připojení zařízení pomocí satelitní technologie je možné a někdy i jedinou variantou připojení u velmi odlehlých lokací bez nutnosti instalace kabeláže nebo přenosových stanic. Satelitní připojení je možné jednoduše realizovat instalací satelitní antény s modemem [27].

Družice (satelity) se dají klasifikovat do tří skupin (viz obrázek č. 14) dle oběžné dráhy kolem Země na:

- A - Geostacionární družice (GEO),
- B - Družice s nízkou oběžnou dráhu (LEO),
- C - Družice se střední oběžnou dráhu (MEO).



Obrázek 14 - Oběžné dráhy satelitů

Zdroj: [28]

Jednotlivé kategorie se odlišují vlastnostmi, ale i technickými omezeními. Satelity GEO obíhají Zemi ve výšce cca 36 000 km a jejich velkou výhodou je stálá poloha pro pozorovatele z povrchu Země. Pro realizaci připojení k tomuto typu satelitu stačí fixní anténa díky stálé poloze vzhledem k Zemi. Velká vzdálenost od povrchu má však negativní vliv na výkon spoje, kdy odezva spoje se pohybuje rychlostí 250 ms^{-1}, což může

způsobovat, že některé síťové protokoly v prostředí s vysokou odezvou nemusejí dobře, či vůbec fungovat. Satelity LEO Zemi obíhají ve výšce kolem 300 km nad povrchem a poskytují podstatné nižší odezvy pohybující se kolem 40 ms^{-1}, pro udržení spojení je ale potřeba sítě satelitů.

2.3.2 Linková vrstva

Linková vrstva je známá také jako spojová nebo vrstva datového spoje. V této vrstvě jsou data spojována do rámců o velikosti několika stovek bajtů. Linková vrstva již plní jistou kontrolní činnost správnosti přenosu informace pomocí CRC kontrolních součtů. Pokud je na linkové vrstvě požadováno zajištění spolehlivého přenosu, musí se zařízení na straně příjemce zajistit, aby byl odesílatel upozorněn, že rámec přišel poškozen a má ho poslat znovu. Mezi další činnosti linkové vrstvy patří řízení rychlosti přenosu dat tak, aby příjemce stíhal rámce zpracovávat. [18]

Linková vrstva se dále dělí na dvě podvrstvy a to LLC (Logical Link Control), která se zabývá úkoly již výše popsanými funkcionalitami, a podvrstvu MAC (Media Access Control), která hlídá kolizní stavy při přístupu více uzlů na společné medium v lokálních LAN sítích. [18]

Linková vrstva zajišťuje přenos pouze u přímého spojení a tudíž i adresy na úrovni linkové vrstvy jsou jedno rozměrné bez dalšího logického členění, nelze pomocí této vrstvy předávat data mimo danou LAN síť. Je třeba využít pro přenos mimo přímé spojení vyšších vrstev a aktivního zařízení na rozhraní dvou typů sítí.

2.3.3 Sítová vrstva

Jak je uvedeno výše, linková vrstva zajištuje přenos data pouze u přímého spojení mezi zařízeními. Pro přenos dat mezi sítěmi je třeba využít vrstvy síťové, která využívá procesu směrování k přenášení dat dále než k sousedním uzlům sítě. Data jsou zde členěna do packetů. Na úrovni síťové jsou jako adresy používány IP adresy obou koncových účastníků a také informace o potvrzování nebo o řízení toku. Úkolem této vrstvy je tedy mimo jiné adresace stanic a přenos datagramů (packetů). V prostředí Smart Grid sítí je tato vrstva sjednocující komunikační vrstvou, která nám zajištuje kompatibilitu přenosu dat. [28]

Pro přenos datagramů na této úrovni sítě je využíván protokol IP (internet protocol), který je v současnosti nejvyužívanějším protokolem pro přenos dat a je využíván i v celosvětové síti Internet. Protokol IP je nespojový protokol, ale samotnou funkcionalitu ověření spolehlivosti přenosu lze zajistit pomocí vyšších vrstev modelu ISO/OSI. Protokol IP je v současné době dostupný ve dvou verzích, a to v IPv4 a IPv6. IPv4 v současné době díky své 32 bitové adresní velikosti, již neposkytuje dostatečné množství adres pro všechna zařízení v rámci světa, a proto je postupně nahrazován IPv6, který díky svému 128 bitovému adresnímu prostoru poskytuje dostatek adres pro všechna zařízení. Některá starší zařízení však tuto adresaci pomocí IPv6 nepodporují, a proto je nutné při budování infrastruktury počítat i s využitím IPv4.

2.3.4 Transportní vrstva

Transportní vrstva ISO/OSI je poslední vrstvou, která řeší samotný přenos dat. Vyšší vrstvy se zabývají spíše interpretací a transformací dat. Transportní vrstva se zabývá rozdělením a složením balíku odesílaných/přijatých dat do/z packetů, které pak síťová vrstva posílá/přijímá směrem k příjemci nebo naopak od odesilatele. Jedním z jejich úkolů je tvořit mezičlánek mezi aplikační logikou síťové komunikace a datovým přenosem, a tak vyrovnávat rozdíly mezi spodními vrstvami a aplikačně orientovanými třemi vyššími.

Transportní vrstva obsahuje dva základní protokoly transmission control protocol (TCP) a user datagram protocol (UDP). TCP protokol zajišťuje spolehlivost přenosu dat (jedná se o spojovaný protokol) tak, že v případě ztráty dat (nepřijde potvrzení o přijetí) jsou data znovu odeslána. Proto je TCP protokol spolehlivým pro přenos dat, ale klade vyšší nároky na zatížení sítě. Pro ilustraci problematiky lze uvést příklad telefonního hovoru, v němž výměna informací proběhne až po potvrzení navázání hovoru (zvednutí sluchátka). UDP je protokol nespojovaný, a tedy nezaručuje doručení dat příjemci, a proto má nižší nároky na zatížení sítě. UDP také umožňuje vícesměrové vysílání, kdy jeden paket lze zaslat více příjemcům. Ilustračním příkladem nechť je televizní vysílání, kdy je signál vysílán bez ohledu na to, zda ho někdo přijímá. V případě výpadku televizního obrazu odesilatel neodesílá data znovu.

V sítích Smart Grid může být využito obou těchto protokolů vzhledem k požadavkům pro nasazení v dané oblasti.

Praktická část práce

3 Bezpečnosti Smart Grid sítí

Jak již bylo uvedeno v předcházejících kapitolách, cílem inteligentních sítí je spolehlivá, efektivní a bezpečná distribuce energií, které je dosahováno pomocí obousměrné komunikace mezi zúčastněnými stranami (výrobci energií, distributory a zákazníky) pomocí moderních informačních a komunikačních technologií. Transformací tradičních elektrických sítí na technologii Smart Grid (viz kapitola 1.2 Transformace tradičních sítí až do sítí Smart Grid), dojde k připojení do komunikační infrastruktury moderní výpočetní techniky (osobních počítačů, mobilních zařízení, apod.), která otevírají nové možnosti v oblasti řízení, ale přinášejí také nová bezpečností rizika. Jako příklady zneužití bezpečnostních slabin moderních technologií lze uvést následující incidenty, kdy došlo k napadení elektrické sítě prostřednictvím softwaru:

Jedním z hodně medializovaných bezpečnostních incidentů byl nález a infikace počítačů pomocí červa s názvem **Stuxnet**, který cílil na systémy SCADA dodávané společností Siemens. Tento Červ byl objeven běloruskou firmou VirusBlokAda a jeho účelem bylo převzít řízení a kontrolu nad procesy v PLC zařízeních. V roce 2010 došlo k poškození Íránského jaderného programu právě tímto červem. Dle dostupných informací mělo jít o aktivity Spojených států a Izraele s cílem poškodit Íránská jaderná zařízení. [29], [30]

Za zmínku stojí také případy útoků na elektrické sítě v USA, kdy bylo hackery vloženo speciálního softwaru do ovládání sítě. Tento útok vedl k odstavení jaderné elektrárny v Georgii.[31]

K podobným útokům dochází v současné době v masovém měřítku v Izraeli, jenž v současné době investuje miliardy dolarů do výstavby centra kybernetické bezpečnosti a výzkumu. Kybernetické útoky na rozvodné sítě byly realizovány během ukrajinského konfliktu, kdy byl ukrajinský systém SCADA napaden trojským koněm BlackEnergy, který zavinil výpadek dodávky elektrického proudu v oblasti Ivano-Frankivsk. [32]

Moderní řídicí systémy pro elektrickou síť nebyly vystavovány takovému napadení zvenku jako v posledním desetiletí, jelikož se jedná o poměrně mladé technologie, které

nedisponují tolik propracovanými bezpečnostními mechanismy jako klasické informační a komunikační systémy. Rozvody energií představují významný strategický cíl pro potenciální útočníky (kyberteroristy), ale i pro nepřátelské armády, a je nutné zabezpečení řídicích a kontrolních systému věnovat dostatečnou pozornost již nejen ve fázi návrhu, ale také během realizace a běhu a neustále tak reagovat na nové bezpečnostní hrozby. V následující kapitole bude popsána obecná problematika hrozeb v komunikačních systémech dle [15].

3.1 Hrozby

Hrozbou se v oblasti informačních a komunikačních technologií rozumí událost, která může mít negativní dopad na zařízení či služby. Negativní dopad může být ve formě neoprávněného přístupu, zničení, odhalení, modifikace dat, zamezení dostupnosti služby či zařízení [15].

Z principu věci je možné hrozby rozdělit do dvou kategorií:

- Organizované hrozby – úmyslně provedené činnosti s cílem poškození systému,
- Náhodné hrozby – náhodné chyby či nehody, zanedbání předpisů či nepředpověditelné události (počasí, přírodní jevy, apod.)

Organizované hrozby využívají zranitelnosti systému, představuje možnost jejího zneužití k proniknutí a vedení útoku. Oba typy hrozeb existují pro všechny systémy a je nutné s nimi počítat a odpovídajícím způsobem řídit obranu proti nim či je jinak eliminovat. V hodné postupy a metody přináší management rizik popsaný v kapitole 3.3.

3.2 Útoky

„Útok je úspěšný nebo neúspěšný pokus o narušení bezpečnosti informačního systému.“[33]

Podle [34] můžeme útoky rozdělit dle **formy** útoku na:

- **Přerušení** – patří mezi aktivní útoky na dostupnost dat (např. ztráta, vymazání, poškození dat).
- **Odposlech** – patří mezi pasivní útoky na důvěrnost, neoprávněný přístup k datům (např. odposlech přenášených dat počítačovou sítí, kopírování programu či dat).
- **Modifikace** – patří mezi aktivní útoky na integritu dat, neoprávněná změna dat (např. změna přenášených či uložených dat).
- **Přidání hodnoty** – patří mezi aktivní útok na integritu dat nebo na autenticitu (např. podvržení dat).

Útoky lze dále dělit na **aktivní** a **pasivní**. Při pasivním útoku jde o získání nebo využití informací. Při pasivní útoku dochází k buď k odposlouchávání, nebo k analýze provozu. K odposlechu dochází při komunikaci, ve které jsou přenášeny nezašifrované zprávy. Odposlechu lze zabránit pokud je použito šifrování přenášených zpráv. Při analýze provozu se zachycují a zkoumají přenášené zprávy. Zachycení a zkoumání přenášené zprávy je možno provádět, i pokud jsou zprávy zašifrované. [34]

Při aktivním útoku jde o změnu systémových prostředků nebo o ovlivnění jejich provozu. Při útoku útočník změní, odstraní či přidá data. Útočník může změnit data například tak, že změní číslo účtu. K odhalení tohoto útoku se může použít kontrolního součtu nebo digitálního podpisu. Při aktivním útoku se útočník může pokusit ukrást identitu tím, že získá autentizační informace, nebo převezme vzniklou autentizovanou komunikační relaci. Aby k tomuto útoku nedocházelo, je vhodné použít protokoly, které zabraňují krádeži identity. Útočník může také zničit přenášená data. [34]

Útoky lze dělit také podle **cíle** na [34]:

- Útok na hardware může nastat při útoku přerušením (např. odcizení, zničení, přírodní havárie), odposlechem (např. krádež místa v paměti), přidáním hodnoty.
- Útok na software může nastat při útoku přerušením, kde rozlišujeme útoky úmyslné (např. úmyslné smazání programu) a neúmyslné (např. neúmyslné smazání programu), odposlechem (např. kopírování programu), přidáním hodnoty (infiltrace programů).
- Útok na data může nastat při útoku přerušením (např. poškození dat), odposlechem (např. odposlech dat přenášených počítačovou sítí), změnou (např. změna přenášených dat) a přidáním hodnoty.

Podle polohy útočníka lze útoky dělit také na:

- Vnitřní – útok je zahájen uvnitř systému,
- Vnější – útok je zahájen vně systému.

3.3 Management rizik

Management rizik představuje vhodnou techniku pro identifikaci, vyhodnocení a řešení rizik a bezpečnostních hrozeb ve Smart Grid sítí a je definován mezinárodním standardem ISO 31000 a jedná se o soubor postupů a metod pro identifikaci a vyhodnocení rizik. Cílem tohoto standardu je přinést univerzální metodiku řízení rizik. [35]. Do metodiky řízení rizik patří standardy ISO 31000:2009 Principles and Guidelines on Implementation, OSI/IEC 31010:2009 Risk management a ISO Guide a 73:2009 – Risk Management.

V souvislosti s informačním a komunikačním prostředím je třeba zmínit také sadu standardů ISO 27000, které se věnují bezpečnosti, managementu rizik a bezpečnostním doporučením.

Proces řízení rizik pomocí ISO 31000 [35]

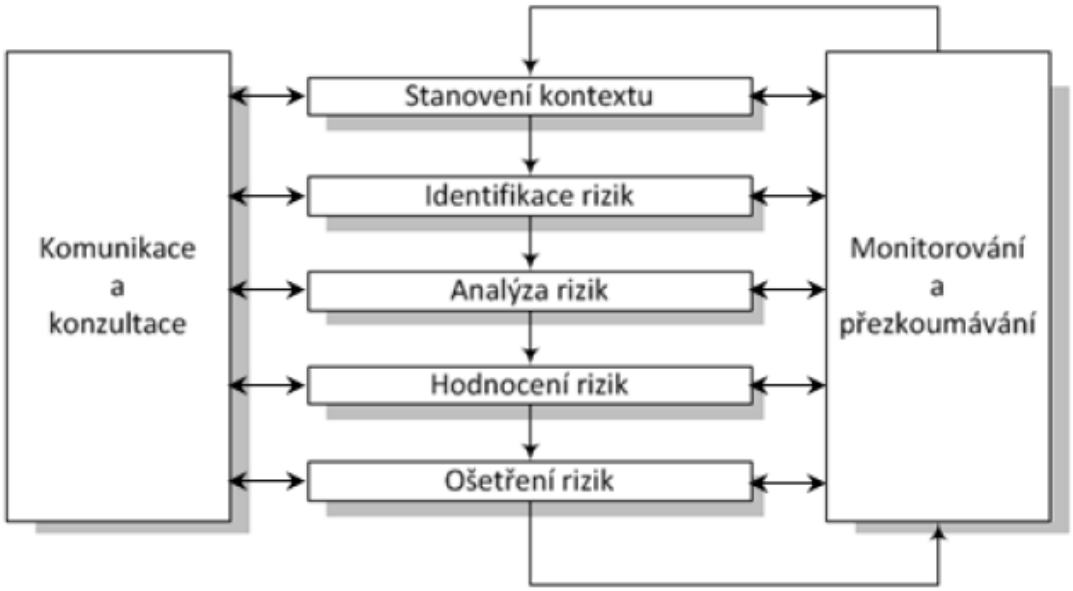
Veškerá rozhodnutí, která jsou činěná za nejistoty, by měla být podporována analýzami, které umožní identifikaci nejzávažnějších rizik a z nich plynoucích problémů. K tomuto je však potřeba mít dostatek informací, čím kvalitnější informace jsou dostupné tím je míra rizika a nejistoty nižší.

Řízení rizik má za úkol mapovat rizika a popsat jejich příčiny a dopady dle modelu **příčina-riziko-účinek**. Součástí tohoto procesu je priorizace a rozhodnutí o opatřeních k jejich minimalizaci. K předcházení rizikům jsou stanovena preventivní opatření, pro zmírnění událostí jsou naplánované reaktivní akce. Volba vhodné akce musí vždy vycházet ze závěrů analýzy rizik.

Proces řízení rizik podle [35] v sobě zahrnuje pět hlavních fází:

1. Identifikace rizik,
2. Vyhodnocení rizik,
3. Vyjádření míry rizika,
4. Identifikace způsobů řešení rizik,
5. Snižování rizik dle zvolené strategie.

Těchto pět fází v sobě zahrnuje počáteční rozpoznání rizik, jejich analýzu a vyhodnocení a vytvoření plánu reakcí, sledování a předcházení. Samotný proces řízení rizik je doplněný ještě o stanovení kontextu a komunikaci rizik, což je patrné z obrázku č. 15.



Obrázek 15 - Proces managementu rizik

Zdroj: [35]

3.3.1 Identifikace rizik a vyhodnocení rizik

Identifikace představuje nejdůležitější a časově nejnáročnější fázi. Cílem identifikace je nalézt relevantní rizika za pomoci vhodně zvolených metod a zaznamenat je. Součástí identifikace je určení vlastníka rizika, tedy jeho správce, který za něj nese odpovědnost, je odpovědný za jeho řízení a připravuje odezvy na něj.

Na začátku tohoto procesu je nutné vyhledat možné příčiny problémů provedením analýzy zdrojů a analýzy problémů. Po získání znalosti zdrojů a problémů je možné následně provést identifikaci možných rizik buď pomocí seznamu běžných případů ,anebo pomocí těchto analýz:

- Taxonomicky založená analýza,
- Scénářově založená analýza,
- Cílově založená analýza.

Pro prostředí Smart gridových sítí je možné najít postupy v:

- Open Source Security Testing Methodology [36],
- Guide for Assessing the Security Controls in Federal Information Systems [37],
- Information Systems Security Assessment Framework [38].

Jak [36] popisuje hodnocení a testování bezpečnosti v šesti oblastích Smart gridových sítí a to:

- Bezpečnost informací,
- Bezpečnost procesů,
- Bezpečnosti internetových technologií,
- Bezpečnost komunikací,
- Bezpečnosti bezdrátových technologií,
- Bezpečnost fyzická,

Dokument [37] popisuje základní postupy vyhodnocování systémů a přináší množství konkrétních scénářů i scénářů všeobecných jako například požární bezpečnost, správa bezpečnostních politik, apod. Pro oblast informačních a komunikačních systémů jsou zde scénáře pro vyhodnocení řízení přístupu, toku informací a vzdáleného přístupu do systému. Je zde možné také nalézt postupy pro vyhodnocení bezpečnosti bezdrátových

sítí, ochranu před škodlivým softwarem, správu veřejných a soukromých klíčů, či pro přístup z mobilních zařízení.

Jak [38] popisuje všeobecný proces managementu rizik a problematiku bezpečností politiky, jsou zde popsány hrozby z oblastí fyzické bezpečnosti, narušení dat a řízení aktualizací systémů, školení uživatelů.

3.4 Bezpečnostní organizace

V oblasti zabezpečení Smart Gridových sítí v současné době existují tři skupiny, které lze dle [15] rozdělit takto:

- vlády států, a státní bezpečnostní služby,
- soukromé organizace,
- nadnárodní korporace a organizace.

North American Electric Reliability Corporation (NERC) je neziskovou organizací založenou v roce 2006, která si za cíl klade zajištění spolehlivosti elektrické soustavy. Tato organizace spolupracuje na vývoji standardů a poskytuje školení v dané problematice. Z dílny NERC také vyšel koncept **Critical infrastructure protection** (CIP), jímž došlo k pokrytí různých sektorů v oblasti bezpečností politiky včetně oblasti energetiky. Na základě tohoto konceptu vznikají obdobné programy v rámci světa. V Evropské unii se jedná například o European Programme for Critical Infrastructure Protection (EPCIP). [34]

Jednou z těchto skupin je organizace **European Network and Information Security Agency** (ENISA) zřízena roku 2004 Evropskou unií. Cílem této organizace je dle jejich webových stránek zlepšování síťové a informační bezpečnosti v rámci Unie.[33]

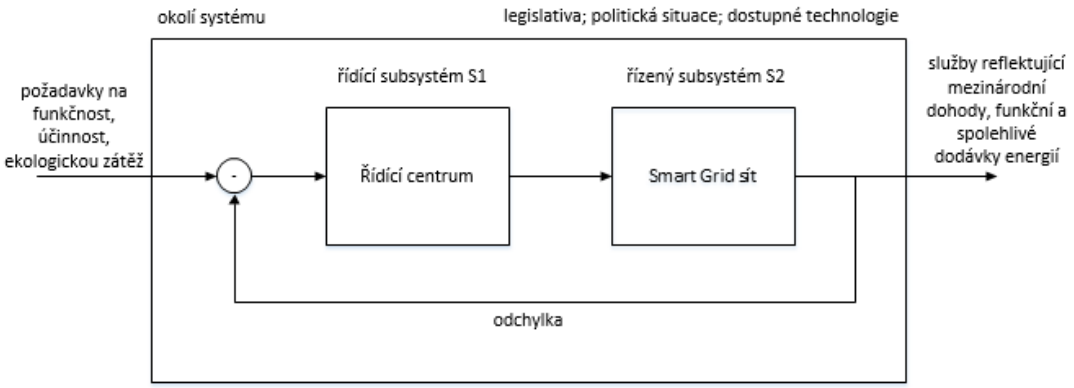
Ve Spojených státech amerických vláda reguluje energetický průmysl již po desetiletí v rámci činnosti ministerstva energetiky a federální komise pro regulaci energetiky. V roce 2007 vstoupil v USA v platnost zákon **Energy and Independence Security Act** (EISA), který podpořil modernizaci elektrické sítě v USA a ustanovil pracovní skupiny pro oblast Smart Grid. [15]

4 Bezpečnostní rizika

V následující kapitole bylo využito analýzy a syntézy Smart Sítě a následně analyzovány bezpečností hrozby a rizika v jednotlivých subsystémech. Důraz byl kladen na zranitelnost IP protokolu.

4.1 Systémový přístup při identifikaci rizik

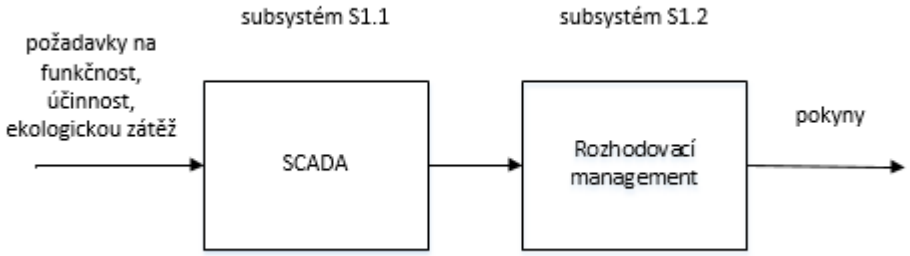
V předcházejících kapitolách byla popsána teoretická východiska a postupy, které je nutné před samotou identifikací bezpečnostních rizik znát. Vzhledem k širokému multioborovému rozsahu těchto poznatků (energetika, management, informační a komunikační technologie, marketing, a další) je vhodné Smart Gridovou sít popsat pomocí systémového přístupu a definovat samotný systém sítě a jejího okolí. Samotný systém se skládá z řídicího subsystému (S1), jímž je kontrolní centrum (popsané v kapitole 2.2., Enterprise) obsahující řídicí centra pro technologie SCADA a WAMS, a řízeného subsystému (S2), jež obsahuje celou soustavu Smart gridové sítě. Vstupem do systému jsou požadavky na funkčnost, účinnost, ekologickou zátěž (popsáno v kapitole 1.2. Transformace tradičních sítí až do sítí Smart Grid). Výstupem ze systému jsou služby reflektující mezinárodní dohody, funkční a spolehlivé dodávky energií. Aby toto bylo zajištěno a výsledné výstupy odpovídaly co nejvíce vstupním požadavkům, je nutné zde realizovat zpětnou vazbu. Okolím systému, které systém zcela jistě ovlivňuje, nechť je legislativa vztažená k dané oblasti, politická situace, dostupné technologie. Schéma systému je znázorněno na obrázku č. 16.



Obrázek 16 - Systémový přístup k Smart Grid

Zdroj: [vlastní]

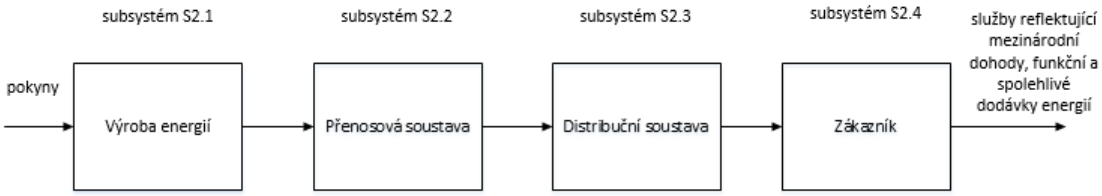
Takto definovaný systém složený ze dvou subsystémů, lze dále dekomponovat na další subsystémy. Subsystém S1 se skládá ze subsystému SCADA systému (S1.1), jehož činnost spočívá ve zpracování a analýze dat, Subsystému Manažerů a operačního centra (S1.2) jež na základě analýzy dat a rozhodovacích procesů volí strategie a způsoby řízení sítě. Dekompozice subsystému S1 je znázorněna na obrázku č. 17.



Obrázek 17 - Řídicí subsystém

Zdroj: [vlastní]

Řízený subsystém S2 lze dále dekomponovat na subsystémy: S2.1 výrobní subsystém, S. 2.2 přenosovou soustavu, S2.3 distribuční soustavu, S2.4 koncové zákazníky. Tyto subsystémy jsou znázorněny na obrázku č. 18.



Obrázek 18 - Řízený subsystém

Zdroj: [vlastní]

V následujících kapitole budou na základě analýzy systému identifikována bezpečnostní rizika při přenosu informací mezi subsystémy a možná rizika útoků na vybrané subsystémy, pro které budou v kapitole 6 navrženy modely řešení a následnou syntézou systému popsány kroky ke zvýšení bezpečnosti Smart Gridových sítí.

4.2 Útoky na komunikační sítě NAN a HAN

V [39] jsou analyzovány možné problémy v této části sítě a ve směrovačích mezi těmito sítěmi. Jak je popsáno v předcházejících kapitolách pro komunikaci v sítích HAN a NAN je používáno bezdrátové komunikace, která přináší bezpečnostní rizika. Jedním z typů bezdrátové komunikace je použití **ZigBee**, které přináší následující rizika a slabiny:

- Vytváření podvržených potvrzovacích rámců,
- DoS útok na AES-CTR,
- Použití totožných klíčů na více ACL záznamech,
- Skupinové klíče,
- Při výpadku elektřiny dojde k nastavení na výchozí hodnoty užívané při šifrování.

Dalším používaným standardem je IEEE 802.11, známý též jako **Wi-Fi**, který přináší následující rizika a slabiny:

- Zahlcení radiového spektra,
- Zahlcení brány pomocí ICMP paketů a snížení tak přenosové rychlosti sítě,
- Viditelnosti SSID,
- Podvržení přístupového bodu,
- MAC spoofing,
- MIMT.

Poslední popsanou metodou komunikace je standard IEEE 802.16 označovaný jako **WiMAX**, který obsahuje tato rizika:

- Útočník může odesílat na cílové zařízení velké množství paketů za účelem zvýšení spotřeby energie daného zařízení,
- Rušení sítě,
- Řídící rámce nejsou šifrovány,
- MIMT.

4.3 Útoky na SCADA systémy

Útoky na SCADA systémy jsou známé a některé z nich jsou popsané v kapitole 3. Tyto systémy slouží k monitorování a řízení komponent celé elektrické sítě a bývají napojené na datovou síť, čímž přebírají i možná rizika z běžných datových sítí jako jsou například:

- Bezpečnostní rizika pro operační systémy, na kterých jsou systémy hostovány,
- Špatně řízené přístupové politiky uživatelů,
- Bezpečnostní politiky (požadavky na složitost hesla, platnost účtů, apod.),
- Možná absence antimalwarového softwaru na hostovaném serveru,
- DoS útok na hostovaný server,
- Špatné zabezpečení síťové architektury (http, ftp, smtp, pop, imap, rdp, apod.),
- Absence nebo špatné nastavení firewall,
- A mnoho dalších bezpečnostních rizik přejatých z datových sítích.

4.4 Útoky na pokročilá měřící zařízení

Pokročilá měřící zařízení (Advanced metering infrastructure, dále jen AMI) představuje soubor měřících zařízení, které jsou rozmístěny v celé síti od zákazníků až po energetické společnosti. AMI přenáší velké množství dat včetně soukromých údajů o zákaznících a parametrech jejich odběru. Podle [39] lze za bezpečností hrozbu považovat:

- Obcházení kontroly, kdy útočník úmyslně obejde bezpečnostní mechanismy za účelem přístupu k datům a k jejich manipulaci,
- Krádež zařízení, kdy dochází k finanční ztrátě a potenciální ztrátě uchovávaných dat v zařízení,
- Fyzické poškození zařízení,
- Odposlech zařízení třetím subjektem,
- Napadení zařízení malwarem a možná rizika z toho vyplývající,
- Narušení integrity dat,
- Nastrčení zařízení vydávajících se za autorizovaného uživatele,
- Úniky informací od personálu energetických společností.

Jednotlivé útoky na měřicí zařízení lze klasifikovat do následujících oblastí:

- Komunikace,

- Fyzické útoky,
- Systémové útoky.

4.4.1 Útoky na komunikační systémy

Mezi útoky na komunikační část měřicího zařízení se řadí útoky na komunikační řetězec, který se skládá z elektroměru, přenosové trasy a datakoncentrátoru. Popsány budou zejména útoky na GPRS technologii. Útoky na komunikační infrastrukturu využívající technologie PLC, Wi-Fi, WiMAX a další, jsou popsány v kapitole 4.2.

Zachycení a analýza přenášených dat je jedním z možných útoků a je zaměřen na zjištění podrobností o poskytované službě a nalezení případných bezpečnostních „děr“, které by mohl útočník využít ve svůj prospěch. Útočník se pokouší zachytit a následně analyzovat komunikaci mezi elektroměrem a jeho nadřazeným systémem. Na základě analýzy těchto dat může dojít k sofistikovanému útoku na technologii GPRS, nebo k pokusu o modifikaci dat.

Triviální **útok na technologii GSM/GPRS** je „odvedení“ modemu pomocí femto buňky [58]. Tento typ útoku je lehce proveditelný a často i neúmyslný. Na vině je buď nesprávně nastavená femto buňka, to jde o záležitost operátora, nebo nestandardně chovající se modem, pak se jedná o chybu výrobce. Útočník se tak může napojit na zařízení, která jsou připojena na síťový modem.

Útok na úrovni spojení GPRS spočívá v postupu, kdy se útočník pokusí o navázání spojení přes GPRS na SIM v elektroměru s úmyslem vyvolání chybového stavu, zablokování modemu, nebo zaplnění paměti SIM (SMS). V případě krádeže SIM se může pokusit využít datové či hlasové služby z odcizené SIM pro vlastní účely. Úspěšnost útoku závisí na tom, zda útočník má k dispozici seznam telefonních čísel použitých v elektroměrech, tedy od zaměstnanců (například propuštěných) energetických společností.

4.4.2 Fyzické útoky

Fyzické útoky jsou prováděny přímo na elektroměr, kdy útočník má možnost dostat se do jeho fyzické přítomnosti. Nejčastěji jde o ovlivňování metrologických vlastností elektroměru elektromagnetickým polem. Útočníkovi jde o ovlivnění vlastností a zároveň

se snaží fyzicky nepoškodit elektroměr, aby jeho útok byl co nejméně nápadný při kontrole pracovníky energetiky.

Útokem s využitím magnetického pole může útočník ovlivnit pomocí silného permanentního magnetu funkci elektroměru. Útok je prováděn tak, že je permanentní magnet přikládán na různá místa elektroměru a je sledován jeho stav, kde je analyzována schopnost provedení přesného odečtu (ovlivnění metrologické části), schopnost komunikace nebo funkcionalita přepínání na nízký/vysoký tarif. Útočník se snaží během tohoto útoku nalézt co nejvhodnější lokalizaci pro umístění permanentního magnetu, aby dosáhl co největšího ovlivnění funkce elektroměru.

Útoky elektromagnetickým polem jsou koncipovány tak, že se útočník snaží o umístění různých radiových prostředků (jedná se například o GPRS rušičku, RF rušičku, komunikační prostředky PMR, osobní radiostanici CB) ve velmi těsné blízkosti elektroměru. Útočník sleduje stav elektroměru, kde se soustředí zejména na přesnost odečtu a schopnost komunikace nebo schopnost přepnutí na nízký/vysoký tarif. Útočník provede během těchto testů nejvhodnější lokalizaci pro umístění a nastavení zdroje radiových vln s cílem o co největší ovlivnění měřicích funkcí elektroměru.

Útok přemostěním elektroměru je zaměřen na mechanickou manipulaci s elektroměrem. Dochází k odpojení jedné z fází či fyzické přemostění elektroměru na jedné fázi. Útočník se snaží o co nejmenší znehodnocení krytů elektroměru, aby při případné kontrole pracovníků distributora mohl dát stav do původního stavu a útok tak mohl zopakovat.

Útok přepětím pomocí volně dostupného zařízení, kdy útočník přikládá do blízkosti elektroměru silný zdroj přepětí. Při tomto útoku dochází převážně k trvalému poškození elektronických obvodů uvnitř elektroměru.

Útok mechanickým poškozením komunikačního rozhraní za účelem přerušení komunikace elektroměru nebo komunikačního zařízení. Může se jednat útoky, jako je poškození nebo odstínění antény, nebo se může jednat i o útoky na přerušení vazby PLC komunikátoru na silovém vedení.

4.4.3 Systémové útoky

Inteligentní měřicí zařízení mají v sobě programové vybavení, nejčastěji firmware nebo triviálnější operační systém, než známe z běžné výpočetní techniky. Tento typ útoků se zabývá možnými útoky na systémové vybavení. Může se jednat o útoky na operační systém, firmware elektroměru, nebo na konfiguraci zařízení, na systémový hardware.

Jednou skupinou systémových útoků je **přetížení zařízení za účelem omezení či znemožnění komunikace** s autorizovanými uživateli. Představitelem tohoto typu útoku je útok zvaný DoS (Denial of Serice), kdy se jedná o úplné znepřístupnění služby. Útočník je schopen generovat velké množství legitimních požadavků, které cílový systém nestíhá vyřizovat, nebo je schopen zasílat nestandardně tvarované pakety dat, kdy systém obvykle vlivem nedostatečné kontroly vstupů přestane reagovat. Útoky tohoto typu lze realizovat na různých vrstvách OSI modelu. Útoky DoS mají za následek nemožnost provedení odečtu z elektroměru, ale nezpůsobují modifikaci (změnu) odečtených hodnot [59].

Útok fyzickým proniknutím do elektroměru - útočník mechanicky pronikne do elektroměru, aniž by byl spuštěn vnitřní „alarm“, který by způsobil okamžité odeslání chybového hlášení do řídícího centra. Útočník se zároveň snaží neporušit plomby elektroměru. V případě že se útočníkovi podaří fyzicky proniknout k elektronickým obvodům, hrozí útok na zablokování komunikačních kanálů, zamezí tím okamžitému informování o události z elektroměru, nebo se útočník pokusí o útok na paměť elektroměru, snaží se o vymazání událostí z paměti elektroměru.

Útoky na operační systém mají za cíl znemožnit komunikaci elektroměru s jeho okolím, nebo výrazně narušit jeho standardní chování ve prospěch útočníka. Typickým příkladem útoku na OS je:

- Zahlcení vstupu, kdy dochází k posílání nepovolených znaků nebo příliš dlouhých řetězců na vstupy elektroměru. Útočník může využít i jiné vstupy elektroměru a pokusit o zaslání nestandardních dat za účelem zamrznutí operačního systému.
- Zahlcení paměti, kdy je cílem zablokování elektroměru, nemožnost uložit naměřená data, nebo překrýt informace o útoku. Útočník může zahltit paměť například impulsními vstupy nebo pomocí uživatelského komunikačního rozhraní s domácností přes WIFI.
- Přetížení procesoru lze docílit pomocí opakovaných událostí, kdy dochází k přetížení. Výstupem tohoto útoku může být zablokování elektroměru, nebo neschopnost měření spotřeby a zápis těchto hodnot do paměti. Může se například jednat o vyvolání velkého počtu odečtů, které procesor elektroměru nebude schopen obsloužit, nebo přetížení komunikačních kanálů dle výše specifikovaných útoků.

Útoky na systémový hardware jako je například AD převodník, útok na paměť mohou být následující:

- Útok na A/D převodník spočívá v modifikaci vstupu/výstupu u A/D převodníku a tím dochází k manipulaci v oblasti přesnosti měření. Tento typ útoku je obtížně identifikovatelný, jelikož se jedná o nevýrazný zásah do elektroměru a data jsou postupně modifikována. Útočník tak může výrazně modifikovat data o naměřené spotřebě.
- Útok na paměť je nutné klasifikovat na útoky na operační paměť, na paměť určenou pro ukládání výsledků měření, pro ukládání událostí a na paměť s OS/firmware a konfiguracemi. Prvním pokusem o útok může být analýza s cílem identifikovat, jak výrobce rozdělil využití jednotlivých pamětí (například zda není sloučena paměť pro ukládání konfigurací s pamětí pro uložení OS/firmware, nebo zda není sloučena paměť určená pro ukládání výsledků měření s pamětí určenou pro ukládání vnitřních alarmů). Přetečení obsahu paměti je určen především pro paměti určené k ukládání konfigurace, poplachů nebo k ukládání

OS/firmware. Modifikací uložených dat v paměti se útočník snaží o získání informací o struktuře ukládání dat do paměti, či o získání nástroje pro mazání dat nebo modifikaci dat přímo v paměti elektroměru. Zamezení zápisu do paměti, kdy se může jednat například o zamezení uložení alarmových hlášení o fyzickém napadení elektroměru, nebo o nemožnost ukládání naměřených hodnot o spotřebě.

- Útoky pro získání hesla jsou motivovány získáním privilegovaných přístupových práv do elektroměru.

4.5 Útoky na systémy pro regulaci odběrů

Tato součást systému označovaná jako demand response (dále jen DR) je bezpečnostním prvkem, který umožnuje předcházet výpadkům sítě a zvyšuje jejich efektivitu. V případě, že by došlo k vyřazení z provozu či poškození systému, by mohlo dojít k výrazným škodám. Mezi možné hrozby dle [39] patří:

- Vytvoření velkého zatížení v energetické síti, jehož důsledkem by mohla být nestabilita a následné výpadky dodávky energií vedoucí až k tzv. blackoutu.
- Hromadné vypnutí všech zařízení.

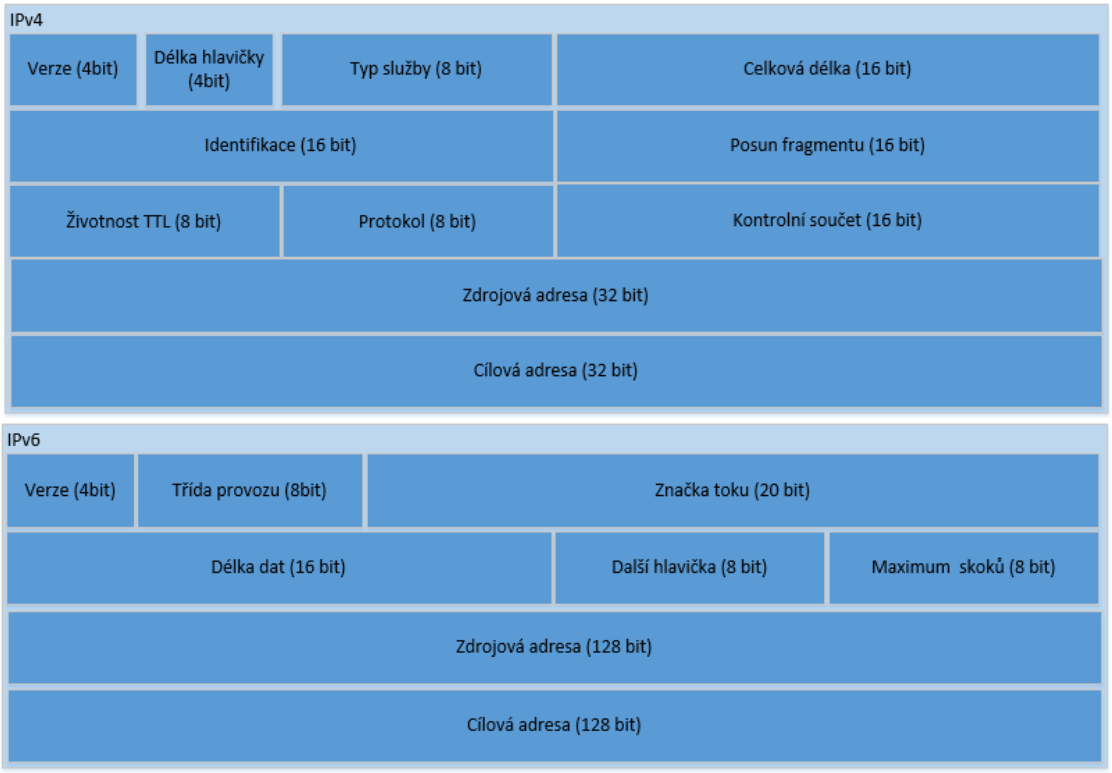
4.6 Útoky na Internet protokol

Internet protokol (IP) přináší velkou řadu výhod díky kompatibilitě s mnoha komponentami Smart gridové sítě i se stávajícími datovými sítěmi [40]. Sadu protokolů lze rozdělit do starší sady IPv4 a novější varianty IPv6. Sada protokolů TCP/IP může být dle [40] cílem různých útoků:

- Smurf útok,
- Land útok,
- SYN flood,
- Source routing,
- Podvržení DHPC serveru,
- Podvržení ICMP redirect zpráv,
- Odhalení sekvenčního čísla TCP spojení.

Důležité pro bezpečností problematiku je porozumět rozdílům mezi IPv4 a IPv6. Oba tyto protokoly sdílí řadu stejných vlastností (IPv6 je částečně odvozeno z IPv4). Díky této podobnosti lze využít a aplikovat řadu bezpečnostních opatření pro IPv4 a aplikovat je i na IPv6. Nicméně nové vlastnosti přinášejí také nová bezpečností rizika, která vyžadují nová bezpečnostní opatření, ale také nové možnosti v zabezpečení komunikace.

Při náhledu na architekturu TCP/IP je mezi IPv4 a IPv6 jediná změna, a to na síťové vrstvě. Internetový protokol funguje nad protokoly nižší vrstvy jako např. PPP, X25, Ethernet, aj. IP podporuje také různé transportní protokoly z vyšší vrstvy jako je TCP, UDP, SCTP a další. Při využití IPv6 oproti IPv4 jsou tak protokoly nad i pod síťovou vrstvou stejné. Pokud je tedy riziko útoků na vyšší vrstvě a nižší vrstvě v prostřední IPv4, existuje toto riziko i v prostředí IPv6.



Obrázek 19 - Hlavičky IP protokolů

Zdroj: [autor]

Oba tyto protokoly jsou zodpovědné za směrování datagramů přes jednu či více sítí a struktura jejich hlaviček je velmi podobná (viz obrázek 19.). Obě hlavičky obsahují údaje o verzi protokolu, QoS, délce dat, životnosti, údaje o protokolu vyšší vrstvy a zdrojovou a cílovou adresu. Díky těmto shodným vlastnostem je řada rizik známých z oblasti IPv4 podobná i v oblasti IPv6. Tyto shodné útoky jsou:

- útoky na aplikační vrstvy,
- neautorizovaný přístup,
- útoky typu main in the middle,
- odposlechy sítě,
- útoky typu DoS,
- IP spoofing,
- útoky na směrovače a jiné síťové prvky,
- útoky na fyzické a linkové vrstvy.

IPv6 však přistupuje v některých oblastech k odlišnému řešení než v IPv4. Díky těmto řešením se změnily bezpečností hrozby platné pro IPv4 a nepřenášejí se tak na IPv6. Jednou z těchto drobných změn je rozšíření hlavičky o dvě nová pole (značku toku, odkaz na rozšiřující hlavičku). Značka toku zatím není přesně definována a tedy ani využívána. Rozšiřující hlavičky jsou však jednou z hlavních součástí IPv6 protokolu a představují tak nové cesty pro útoky, které jsou specifické již pouze pro IPv6 [42]:

- Skenování sítě metodou brutal force je obtížnější, ale možné,
- ICMPv6 útoky,
- Útoky využívající rozšíření hlavičky,
- Útoky s auto-konfigurací,
- Útoky na přechodové mechanismy,
- Útoky na mobilitu IPv6.

Původní verze IP neobsahovala žádné bezpečností mechanismy, avšak s rozvojem internetu bylo nutné komunikaci na této vrstvě zabezpečit. V současné době existují různé bezpečností mechanismy na vybraných vrstvách RM OSI, kde na úrovni síťové vrstvy jde o tzv. IPsec. V případě IPv6 byla implementace IPsecu povinná a bylo tím mylně vytvářen dojem, že je IPv6 bezpečnější než IPv4. V roce 2011 bylo vydáno RFC 6434, které ruší tuto povinnost implementace IPsec a místo toho jej pouze doporučuje, což s sebou přináší další bezpečností rizika, která by byla aplikací IPsec eliminována. [43]

5 Modely řešení vybraných rizik

V následující kapitole jsou navrženy modely řešení identifikovaných rizik z předcházející kapitoly. Navržená řešení jsou realizovatelná při současném stavu poznání v dané oblasti a popsaná rizika by měla minimalizovat. V této kapitole je kladen důraz na řešení slabin měřicích zařízení a jejich komunikace pomocí IP protokolu a následná autorizace zařízení.

5.1 Zabezpečení měřicích zařízení

V kapitole 4.1 byly identifikovány jednotlivé hrozby plynoucí z použití Internet protokolu. V této kapitole budou popsány možné bezpečností mechanismy, které poslouží k eliminaci rizik.

Mobilní komunikace

- Pro zabezpečení mobilní komunikační infrastruktury je doporučeno zřízení doplňkové služby USSD a Call Barring u SIM v elektroměrech. Tyto služby umožňují omezení některých odchozích a příchozích volání [B40]. Distributor si specifikuje telefonní čísla, která nastaví na SIM jako oprávněná a všechny ostatní hovory budou zakázány. Tímto bude útočníkovi zamezeno zneužití SIM karty v případě její krádeže. Útočník tak nebude mít finanční motivaci, pro krádež SIM.
- Zavedení evidence SIM a elektroměrů s jejich pevným přiřazením mezi sebou eliminuje riziko ukradení SIM, nebo její úmyslné přemístění do jiného elektroměru, kde by mohlo dojít k odečítání odlišné spotřeby, než je skutečná.

Zabezpečení elektroměru

- Zavedení kontroly konsistence dat zaslaných pomocí mobilní komunikace v řídícím centru. Eliminuje se tak riziko ztráty některých dat při komunikaci, v níž tento stav může způsobovat cílený útok vnějšího experta. Při podezření na útok konzistence dat následně může iniciovat výjezd posádky pracovníků energetiky na kontrolu odběrného místa.
- Zabezpečení informací o spotřebě zákazníků, aby nemohly být zneužity například k plánování krádeží v odběrných místech, jelikož informace o spotřebě nesou také informaci v které hodiny je zákazník obvykle doma. Jedná se zejména o

zabezpečení autentizovaných přístupů do vnitřní databáze Smart Grid sítě z řad vnitřních zaměstnanců energetiky.

- Zakázání změny nastavení elektroměru přes optické rozhraní elektroměru a jeho zajištění mechanickou překážkou, které je možné při odečtu pracovníkem energetiky odstranit a po odečtu znovu namontovat.
- Eliminovat veškerou komunikace s třetí stranou zakázáním zápisu dat do elektroměru a nastavením minimální periody čtení dat, čímž se eliminuje riziko útoku na modifikaci uložených dat v elektroměru a zároveň bude eliminováno riziko útoku na dostupnost elektroměru cíleným zacyklení požadavků na odečty.

5.2 Internet protokol

V kapitole 4.1 byly identifikovány jednotlivé hrozby plynoucí z použití Internet protokolu. V této kapitole budou popsány možné bezpečností mechanismy, které poslouží k eliminaci rizik. Jak již bylo popsáno v 4.1, samotným použitím novější verze protokolu IPv6 nedojde k eliminaci bezpečnostních rizik, jak je někdy mylně předpokládáno. Je proto nutné navrhnout řešení, jak případné útoky eliminovat. Mezi tyto mechanismy patří:

- Využití IPsec,
- Obrana proti skenování,
- Obrana proti DoS,
- Obrana proti MITM,
- Šifrování na aplikační vrstvě.

IPSec

Jedním z řešení je striktní implementace IPsec, který není ve výchozím stavu v IPv6 již zahrnut, ale pouze doporučen. IPsec umožnuje IP vrstvu zabezpečit pomocí dvou mechanismů [44]:

Autentizace, která nám určuje původce dat způsobem, že je možné ověřit, zda data byla skutečně odeslána uváděným odesilatelem.

Šifrování, které chrání obsah přenášených dat takovým způsobem, že jej mohou přečíst pouze určené subjekty.

Tyto mechanismy jsou aplikovány pomocí rozšířených hlaviček AH (Authentiation Header) a ESP(Encapsulating Security Payload).

AH zajišťuje pouze autentizaci a ESP zajišťuje autentizaci i šifrování dat. ESP tedy samo osobě obsahuje autentizaci. Aplikace obou mechanismů zároveň přináší jistou redundanci, proto dle RFC 4301 je ESP povinným mechanismem a AH pouze volitelným. [45]

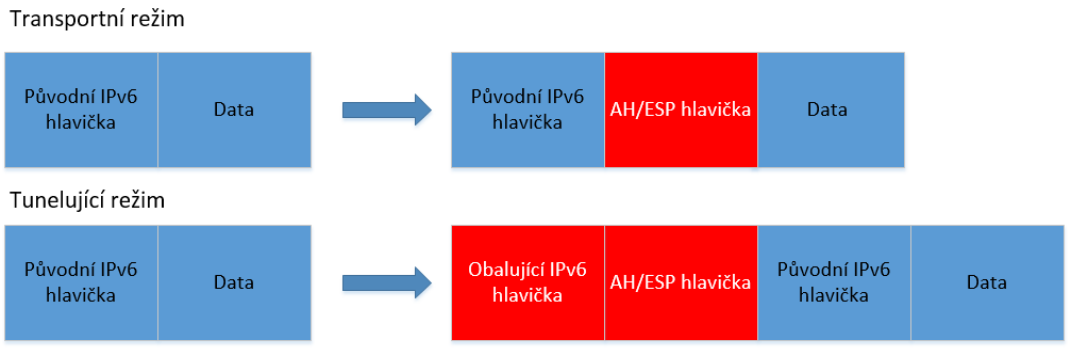
Využitím **AH** je zajištěna:

- Autentizace dat – ověření odesilatele,
- Integrita dat – ověření, zda během přenosu nedošlo ke změně dat,
- Ochrana proti replay attack – odmítnutím opakovaně zaslaného paketu.

Využitím **ESP** je zajištěna:

- Důvěrnost dat,
- Autentizace,
- Integrita dat,
- Ochrana proti replay attack.

Oba tyto mechanismy fungují ve dvou režimech, v t**ransportním režimu**, kdy AH či ESP hlavička je vložena mezi rozšiřující hlavičky, v **Tunelujícím režimu**, kdy původní datagram je zabalen jako data nového datagramu, který je opatřen novými hlavičkami (s bezpečnostními hlavičkami). Tyto režimy přenosu datagramu jsou znázorněny na obrázku č. 20.



Obrázek 20 - režimy IPsec

Zdroj:[41]

Pokud je použit transportní režim, je šifrována ta část datagramu, která následuje za hlavičkou, tedy data. Takto je zajištěno utajení pouze obsahu přenášených zpráv, případnému útočníkovi tak není zabráněno v odposlechu dat ze záhlaví datagramu, které předcházejí EPS a nejsou šifrovány. Takto lze získat data o komunikaci například adresy obou komunikujících stran. Proto je bezpečnější využít tunelujícího režimu, který šifruje celý původní datagram včetně záhlaví. Potenciální útočník tak v případě odposlechu odhalí pouze adresy bezpečnostních bran realizující bezpečnostní tunel, nikoliv však komunikující zařízení.

Obrana proti skenování

Jako obranu proti možnému skenování lze využít řady navržených mechanismů, které potenciálnímu útočníkovi značně ztíží skenování sítě. Mezi tyto mechanismy patří například:

Vhodným způsobem omezení možnosti skenování sítě je používání nepředvídatelných adresních struktur (jako je třeba eliminace číslování směrovače první, či poslední adresou z rozsahu). Ideálně by adresy měly být přidělovány zcela náhodně. Systémy Windows již náhodně generované adresy používají, ale ostatní systémy jako je GNU/Linux či Cisco vyžadují dodatečnou konfiguraci, což je důležité ve spojitosti s integrací Internetu věcí, kde je vysoký předpoklad využití právě Linuxových systémů.

Náhodné přidělování adres lze v praxi realizovat pomocí manuálního přidělování adres nebo prostřednictvím DHPCv6 serveru. Z pohledu komfortu se jeví nasazení DHCPv6 lepším řešením, avšak ne všechny implementace DHCPv6 tuto vlastnost podporují. Správa náhodných adres přináší vysoké nároky na správce sítě, a proto lze doporučit její nasazení pouze v těch částech sítě, kde je vysoké riziko útoku, či riziko vysokých škod v případě útoku.

Obrana proti DoS

Jedním z opatření proti tomuto typu útoku je regulace množství paketů procházejících, zmírní se tím účinnost tohoto útoku. Při konfiguraci firewall je nutné také neopomenout zahrnout pravidla, kdy všechny pakety z následujících adres budou zahozeny. Seznam závadných adres:

- ::/128
- ::1/128
- ff00::/8
- fe80::/10
- fec0::/10

Všechny tyto adresy mají své využití pouze v lokální síti a nesmějí být směrovány.

V případě nasazení systémů nereflektujících RFC 5095 je nutné také zakázat směrování paketu využívající směrovací hlavičku typu 0. V novějších systémech reflektujících RFC 5095 by se již tento typ paketu neměl vyskytovat. [46].

Zabránění útoku, který využívá zařízení v síti odpovídající na povržený požadavek ICMP (smurf útok), lze zabránit plošným zákazem odpovědí na ICMPv6 žádost, které jsou adresovány na multicasotovou adresu ff02::1.

Obrana proti MITM

Obranu proti MIMT útokům lze z části převzít z mechanismů používaných pro IPv4 a z části je nutné aplikovat mechanismy nové. Jednou z možností jak předejít útoku tohoto typu je využití nástroje (vzniklého specifikací RFC 3971) Secure Neighbour Discovery. SEND však vyžaduje více výpočetních prostředků kvůli provádění kryptografických operací. [47]

Útoku, využívajícího podvržené ICMPv6 Neighbour Advertisement lze zabránit sledováním vyrovnávací paměti sousedů a generováním upozornění při podezřelé změně. Pro IPv6 bylo vytvořeno nástroje **NDPMon**, který je analogií nástroje **ARPWatch** používaném pro sledování ARP cache v sítích postavených na IPv4. [48]

Síť je také vhodné zabezpečit ochranou proti nasazení falešného DHCPv6 serveru. Navrhovanou možností zmírnění nasazení falešného DHCPv6 serveru je přítomnost více serverů v sítí, také lze doporučit manuální konfiguraci klíčových síťových prvků jako je výchozí brána, aby se tak zamezilo případnému přesměrování síťového provozu na zařízení útočníka. [49]

Šifrování na aplikační vrstvě

Nadstavbovým řešením pro případ, že by útočník i přes bezpečností opatření získal námi přenášená data, popřípadě se pokusil data podvrhnout, je implementace šifrování na vyšších vrstvách RM ISO. V případě Smart gridových sítí lze doporučit u důležitých komunikačních kanálů nespoléhat pouze na šifrování na sítové vrstvě, ale aplikovat šifrovací algoritmy již na aplikační vrstvě. Útočník v případě odposlechu a v případném dešifrování dat získá pouze data šifrovaná ve vyšších vrstvách. Využitím šifrování na aplikační vrstvě lze dosáhnout větší flexibility při výběru technologií a algoritmů, velikosti klíčů, apod. Zařízení realizující přenos takto flexibilní nejsou a musejí dodržovat stanovené standarty dané nižšími vrstvami, také není nutné, aby tato zařízení dešifrovala přenášená data. Implementace kryptografických nástrojů je však nutná na koncových zařízeních, a proto je nutné vzít v potaz technologické a výpočetní omezení těchto zařízení, aby bylo možné šifrování na těchto zařízeních realizovat (např. smart měřící zařízení, apod.).

5.3 Autentizace zařízení

Jak je uvedeno v předcházejících kapitolách, v Smart Gridových sítích spolu komunikují různá zařízení ve všech úrovních dané hierarchie sítě. V kapitole 4 je popsáno bezpečností riziko, které jde napříč celou komunikační infrastrukturou a spočívá v podvržení či úpravě přenášených dat útočníkem. Typickým příkladem takovéhoto rizika nechť je například:

- Podvržení řídícího prvku do sítě Smart Grid a řízení činností podřízených smart prvků (měřicích zařízení, apod.),
- Podvržení kradeného smart měřícího zařízení u svého odběrného místa, a tedy účtování elektřiny na původního majitele.

Aby byla zajištěna vhodná autentizace zařízení a nemohlo docházet k podvržení zařízení a tedy i jím odesílaných dat, je vhodným řešením některý z modelů pro autentizaci, navržené v této práci:

- Autentizace pomocí hardwarové adresy integrované do síťové adresy IPv6,
- Autentizace pomocí veřejného klíče.

Autentizace pomocí hardwarové adresy integrované do síťové adresy IPv6

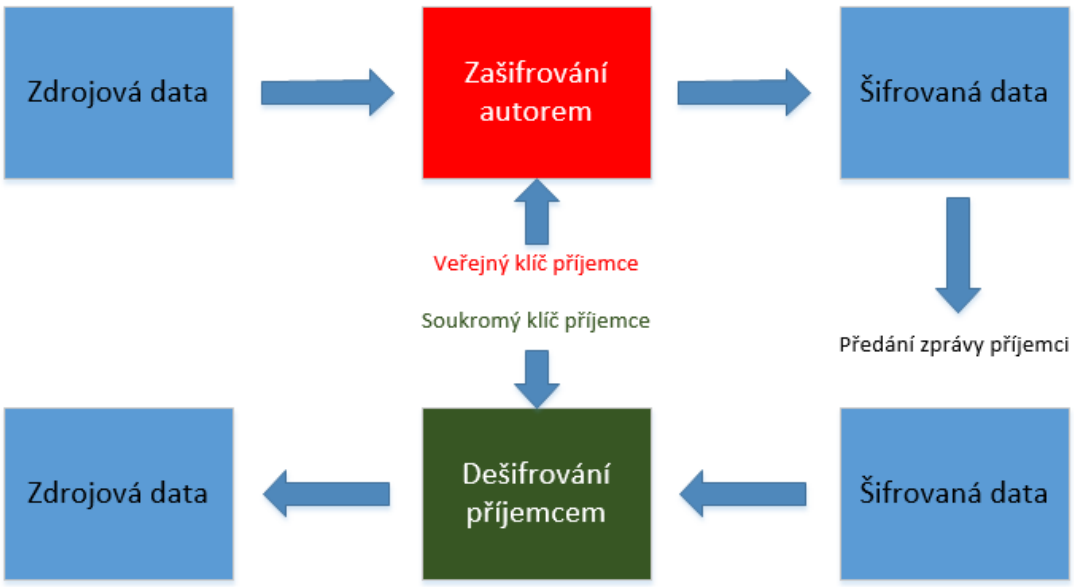
Pro proces ověření zařízení je možné použít model postavený na síťové adrese IPv6, která bude v zařízení staticky nastavena. Toto samotné řešení však neposkytne dostatečné zabezpečení, jelikož samotnou adresu je možné útočníkem podvrhnout, avšak vyžaduje to již jisté znalosti daného typu sítě, které při aplikace modelu řešení rizik u protokolu IP není tak jednoduché získat.

Doplněním identifikátoru do dané struktury IPv6 je možné zajistit ochranu pomocí vnesení náhodného prvku do adresy, a tedy i ochranu před podvržením. Jednotlivé zprávy tak budou označeny identifikátorem, který bude vypočítán pomocí algoritmu z tajného klíče. Navržený model ověření uživatele však nepředpokládá, že některá starší zařízení nejsou s IPv6 kompatibilní a také tento model řeší pouze autentizaci klientských zařízení vůči serveru, nikoli však opačně.

Koncová zařízení by tedy neověřovala server a mohla by tak odpovídat na příkazy útočníka. Jistým řešením se jeví, že by byl tento model rozšířen o generování identifikátorů serveru pro každé koncové zařízení, čímž by byla zajištěna i komunikace ze strany serveru ke klientským zařízením.

Autentizace pomocí veřejného klíče

Systém **public key infrastrukture** (dále jen PKI) představuje podle [5] vylepšení předchozího řešení. Celé PKI představuje obecné řešení pro manipulaci s certifikáty (identifikátory) včetně všech operací s nimi. Celé PKI je založeno na asymetrické kryptografii, kde je využito dvou typů klíčů, veřejného a soukromého. Tyto dva klíče jsou spolu svázané. Text zašifrovaný jedním klíčem ze dvojice lze dešifrovat pouze druhým klíčem z dané dvojice. Text zašifrovaný daným klíčem nejde stejným klíčem dešifrovat. Ale je jedno, zda klíč se použije k šifrování, nebo k dešifrování. Jeden z těchto klíčů se nazývá soukromý a druhý veřejný.



Obrázek 21 - Asymetrické šifrování

Zdroj: vytvořeno podle [50]

Příkladem asymetrických šifer, které lze použít, nechť je RSA a ECC. RSA se využívá pro šifrování nebo elektronický podpis. Tato šifra je založena na faktorizaci velkých prvočísel. ECC je algoritmus zaměřený na řešení úlohy diskrétního logaritmu v grupách na eliptických křivkách. ECC je oproti RSA bezpečnější i při použití kratšího klíče [45].

„Elektronickým podpisem se rozumí údaje v elektronické podobě, které jsou připojené k datové zprávě, nebo jsou s ní logicky spojené, a které umožňují ověření totožnosti podepsané osoby ve vztahu k datové zprávě“. [51]

Elektronický podpis je možné použít pro podepisování dat. Elektronický podpis by měl plnit následující funkce [51]:

- **Identifikace** – lze jednoznačně určit, kdo dokument podepsal,
- **Autentizace** - lze zjistit kdo je autorem daného dokumentu,
- **Integrita** – znamená, že od vytvoření elektronického podpisu nebyl podepsaný dokument změněn či poškozen,
- **Nepopiratelnost** – autor podepsaného dokumentu nemůže popřít, že dokument nevytvořil.

Pro systém PKI se využívá certifikátů vystavených a používaných dle standardu X. 509. Řešení autentizace pomocí PKI představuje komplexní a standardizované řešení. Díky certifikačním autoritám lze spravovat jednotlivé části systému odděleně, což umožnuje segmentaci sítě a v případě prolomení certifikační autority pro jednu část sítě nedochází k prolomení části jiných zároveň.

Závěr

Smart Gridové sítě představují budoucnost moderních energetických sítí, do kterých je zavedena možnost obousměrné komunikace mezi zákazníkem, energetickou společností, distributory, elektrárnami a dalšími zúčastněnými stranami. Přenos informací probíhá v reálném čase, a je tak možné pružně reagovat na nejrůznější události jako jsou například: aktuální spotřeba zákazníků, na jejichž základě může řídící a dohledové centrum kvalitně řídit přenos energií, v oblasti marketingu lze online účtovat spotřebu energie, zákazník je okamžitě informován o aktuální ceně energie a může se rozhodovat, zda energii koupí. V krizovém řízení lze řídit a sledovat aktuální dodávky a případně pružně reagovat na nastalé situace.

Tento typ sítí přináší zvýšení kvality, spolehlivosti, efektivnosti a úspory prostředků v celém energetickém průmyslu, což reflektuje mezinárodní dohody a ujednání o ochraně životního prostředí a snižování produkce skleníkových plynů.

V této práci byly popsány základní principy funkčnosti Smart Gridových sítích, popsána mezinárodní a legislativní motivace pro tvorbu těchto sítí a popsány bezpečnostní hrozby a navrženy modely jejich řešení. Rozsáhlá komunikační infrastruktura a zapojení lidského faktoru do systému sítě přináší zvýšená bezpečností rizika do celé sítě. Byla ukázána analogie mezi běžnými datovými sítěmi a sítěmi typu Smart Grid, díky čemuž bylo možné aplikovat některé přístupy z běžných datových sítí, stejně tak bylo zjištěno, že rizika pro datové sítě jsou možnými riziky i pro sítě Smart Grid. Mimo běžná rizika, plynoucí z analogie s datovými sítěmi, se mohou uživatelé například pokoušet o neoprávněné odběry, či manipulace s měřicími zařízeními, teroristické organizace o vyřazení celé rozvodné sítě, přetížení elektráren či jejich bloků, apod. Všechna tato i mnohá další rizika byla popsána v rámci této práce. Pro vybraná rizika (zranitelnost IP protokolu, podvržení či změna přenášených dat) pak byly navrženy modely pro snížení či eliminaci daných rizik pomocí využití zabezpečení protokolu IPv6 s šifrováním paketů a následným šifrováním na sedmé vrstvě RM ISO/OSI. Také byl navržen model pro autentizaci jednotlivých zařízení v rámci sítě.

Zdroje

[1] HORÁLEK, Josef a Vladimír SOBĚSLAV. Technologie a požadavky na inteligentní sítě pro SmartGrid. Elektrorevue [online]. 2012, č. 65 [cit. 2016-04-01]. 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/

[2] ABB. Úvod do problematiky inteligentních sítí. [online]. [cit. 2016-04-01]. Dostupné z: http://www02.abb.com/global/czabb/czabb018.nsf/0/a5a3d03331846f55c125773d004a5ede/$file/Smart+grids_cz.pdf.

[3] ČEZ, a. s. ČEZ Smart Grids. [online]. [cit. 2016-04-01]. Dostupné z: http://www.cez.cz/cs/vyzkum-a-vzdelavani/vyzkum-a-vyvoj/subjekty-v-oblasti-vyzkumu-a-vyvoje/smart-grids.html

[4] WIKIPEDIA. Rámcová úmluva OSN o změně klimatu [online]. [cit. 2016-04-01]. Dostupné z: http://cs.wikipedia.org/wiki/Rámcová_úmluva_OSN_o_změně_klimatu

[5] MINISTERSTVO ŽIVOTNÍHO PROSTŘEDÍ. Kjótský protokol k Rámcové úmluvě OSN o změně klimatu [online]. [cit. 2016-04-01]. Dostupné z: http://www.mzp.cz/cz/kjotsky_protokol

[6] ČEZ: Evropský kontext. EEGI, SET Plan. [online]. [cit. 2016-04-01]. Dostupné z: http://www.cez.cz/cs/vyzkum-a-vzdelavani/vyzkum-a-vyvoj/subjekty-v-oblasti-vyzkumu-a-vyvoje/smart-grids.html

[7] MINISTERSTVO ŽIVOTNÍHO PROSTŘEDÍ. Klimaticko-energetický balíček [online]. [cit. 2016-04-01]. Dostupné z: http://www.mzp.cz/cz/klimaticko_energeticky_balicek

[8] MINISTERSTVO PRŮMYSLU A OBCHODU, odbor 05200. Státní energetická koncepce ČR [online]. [cit. 2016-04-01]. Dostupné z: http://www.mpo.cz/dokument5903.html

[9] ABB, ROUBAL, Jiří. 2010. Fenomén Smart Grids. [online]. [cit. 2016-04-01]. Dostupné z: http://www02.abb.com/global/czabb/czabb018.nsf/0/ce8319694ef0b683c125773d003f67a9/$file/Fenomén+Smart+Grids.pdf.

[10] ČEZ, a. s. Vrchlabí bude již brzy pod 3D lupou. Díky virtuální prohlídce! [online]. [cit. 2016-04-01]. Dostupné z: http://www.cez.cz/cs/pro-media/tiskove-zpravy/4800.html

[11] Jak se plete počítačová síť - základy sítí [online]. [cit. 2016-04-17]. Dostupné z: http://pctuning.tyden.cz/software/jak-zkrotit-internet/4111-jak_se_plete_pocitacova_sit-zaklady_siti

[12] Horalek, J., Sobeslav, V., Krejcar, O., Balik, L. Communications and security aspects of smart grid networks design (2014) Communications in Computer and Information Science, 465, pp. 35-46.

[13] 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.

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

[15] 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..

[16] 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. 18. DOI: 9781424428502.

[17] Referenční model ISO/OSI [online]. [cit. 2016-04-17]. Dostupné z: http://ijs2.8u.cz/index.php?option=com_content&view=article&id=13&catid=9&Itemid=119

[18] USLAR, Mathias, Michael SPECHT, Christian DANEKAS, Jorn TREFKE, Sebastian ROHJANS, José M GONZALEZ VAZQUEZ, Christine ROSINGER a Robert BLEIKER. *Standardization in smart grids: introduction to IT-related methodologies, architectures and standards*. New York: Springer, 2013. Power systems. ISBN 3642349153.

[19] HORÁLEK J.: Analysis of communication protocols for smart metering, Časopis: ARPN journal of engineering and applied sciences ISSN: 1819-6608 Datum vydání: 2015 Volume/ročník: 10 Issue/číslo: 3 Strana: 1438-1446

[20] 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

[21] 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

[22] BARAN – Vlastní dílo, Volné dílo, https://commons.wikimedia.org/w/index.php?curid=2964670

[23] MRZEON – self-made, based on Image:Tipos_fibra.jpg, CC BY-SA 3.0, https://commons.wikimedia.org/w/index.php?curid=2790879

[24] DOBKIN, Daniel M. a Bernard ABOUSSOUAN. Low power Wi-Fi for IP smart objects. GainSpan [online]. [cit. 2016-04-03]. Dostupné z: http://www.gainspan.com/docs2/Low Power_Wi-Fi_for_Smart_IP_Objects_WP_cmp.pdf

[25] NIST Priority Action Plan 2: Guidelines for Assessing Wireless Standards for Smart Grid Applications. NIST [online]. [cit. 2016-04-03]. Dostupné z: http://collaborate.nist.gov/twikisggrid/pub/SmartGrid/PAP02Objective3/NIST_PAP2_Guidelines_for_Assessing/Wireless_Standards_for_Smart_Grid_Applications_1.0.pdf

[26] PAOLINI, Monica. Empowering the smart grid with WiMAX. Energy Central [online]. 2010 [online]. [cit. 2016-04-03]. Dostupné z: http://www.energycentral.com/reference/whitepapers/103333/

[27] GSM - The Base Station Subsystem(BSS) [online]. [cit. 2016-04-17]. Dostupné z: http://www.tutorialspoint.com/gsm/gsm_base_station_subsystem.htm

[28] 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.

[29] NEW YORK TIMES: Cyberattacks on Iran — Stuxnet and Flame [online]. [cit. 2016-04-17]. Dostupné z: http://www.nytimes.com/topic/subject/cyberattacks-on-iran-stuxnet-and-flame

[30] E15: Stuxnet – virus průzkumník [online]. [cit. 2016-04-17]. Dostupné z: http://vtm.e15.cz/aktuality/stuxnet-virus-pruzkumnik

[31] WASHINGTONPOST: Cyber Incident Blamed for Nuclear Power Plant Shutdown [online]. [cit. 2016-04-17]. Dostupné z: http://www.washingtonpost.com/wp-dyn/content/article/2008/06/05/AR2008060501958.html?tid=a_inl

[32] THE HACKER NEWS: Israeli Power Grid Authority Suffers Massive Cyber Attack [online]. [cit. 2016-04-17]. Dostupné z: http://thehackernews.com/2016/01/power-grid-cyberattack.html

[33] ENISA [online]. [cit. 2016-04-17]. Dostupné z: https://www.enisa.europa.eu/

[34] NERC [online]. [cit. 2016-04-17]. Dostupné z: http://www.nerc.com/Pages/default.aspx

[35] ODCHODKOVÁ, Eliška. *Eliška Ochodková Home Page* [online] [cit. 2016-04-03]. Dostupné z: http://www.cs.vsb.cz/ochodkova

[36] HERZOG, Pete. ISECOM. Open Source Security Testing Methodology Manual New York, 2010 [online] [cit. 2016-04-03]. Dostupné z: http://www.isecom.org/mirror/OSSTMM.3.pdf

[37] Guide for Assessing the Security Controls in Federal Information Systems and Organizations. Gaithersburg, 2010[online] [cit. 2016-04-03]. Dostupné z: http://csrc.nist.gov/publications/nistpubs/800-53A-rev1/sp800-53A-rev1-nal.pdf

[38] OPEN INFORMATION SYSTEM SECURITY GROUP. Information systems security assessment Framework. 2006 [online] [cit. 2016-04-03] Dostupné z: http://www.oissg.org/les/issaf0.2.1.pdf

[39] GHANSAH, Isaac. Smart Grid Cyber Security Potential Threats, Vulnerabilities And Risk [online]. Sacramento, CA, 2009 [cit. 2016-04-16]. Dostupné z: http://www.energy.ca.gov/2012publications/CEC-500-2012-047/CEC-500-2012-047.pdf

[40] 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. 2016-04-09]. ISSN 2315-4462.

[41] SATRAPA, Pavel. IPv6: internetový protokol verze 6. 3., aktualiz. a dopl. vyd. Praha: CZ.NIC, c2011, 407 s. CZ.NIC. ISBN 978-80-904248-4-5.

[42] HOGG, Scott a Eric VYNCKE. *IPv6 security: internetový protokol verze 6*. 3., aktualiz. a dopl. vyd. Indianapolis: Cisco Press, 2009, xxi, 540 s. CZ.NIC. ISBN 978-1-58705-594-2.

[43] RFC 6434. In: IETF [online]. 2011 [online] [cit. 2016-04-09]. Dostupné z: http://tools.ietf.org/html/rfc6434

[44] IPv6 Mýty a skutečnost, díl VI. - Bezpečnostní mechanizmy. LUPA. CZ [online]. 2011 [cit. 2016-04-09]. Dostupné z: http://www.lupa.cz/clanky/ipv6-myty-a-skutecnost-dil-vi-bezpecnostni-mechanizmy/

[45] ZELENKA, Josef, Jan ČAPEK, FRANCEK a Hana JANÁKOVÁ. Ochrana dat: Kryptologie. Vyd. 1. Hradec Králové: Gaudeamus, 2003. ISBN 80-704-1737-4.

[46] RFC 5095. IETF [online]. 2007 [cit. 2016-04-09]. Dostupné z: http://tools.ietf.org/html/rfc5095

[47] RFC 3971. IETF [online]. 2005 [cit. 2016-04-09]. Dostupné z: http://tools.ietf.org/html/rfc3971

[48] NDPMon. Ndpmon.sourceforge [online]. 2012 [cit. 2016-04-09]. Dostupné z: http://ndpmon.sourceforge.net/

[49] A Complete Guide on IPv6 Attack and Defense. SANS Institute InfoSec Reading Room [online]. 2011 [cit. 2016-04-09]. Dostupné z: http://www.sans.org/reading-room/whitepapers/detection/complete-guide-ipv6-attack-defense-33904

[50] NÁDENÍČEK, Petr. Pravdy o elektronickém podpisu a šifrování (1) - základní pojmy. Svět sítí [online]. 2000-2015, č. 1 [cit. 2016-04-17]. Dostupné z: http://www.svetsiti.cz/clanek.asp?cid=Pravdy-o-elektronickem-podpisu-a-sifrovani-1-zakladni-pojmy-1252003

[51] KOCMAN, Rostislav a Jakub LOHNISKÝ. Jak se bránit virům, spamu, dialerům a spyware. vyd. 1. Brno: CP Books, 2005, 148 s. ISBN 80-251-0793-0.

[52] Meregio [online]. [cit. 2016-04-23]. Dostupné z: http://www.meregio.de/en/

[53] Smart City [online]. [cit. 2016-04-23]. Dostupné z: http://www.malagavalley.com/index.php/en/energia/smartcity

[54] IEEE 802.11 WIFI [online]. [cit. 2016-04-23]. Dostupné z: https://standards.ieee.org/about/get/802/802.11.html

[55] KABELOVÁ, Alena a Libor DOSTÁLEK. Velký průvodce protokoly TCP/IP a systémem DNS. 5., aktualiz. vyd. Brno: Computer Press, 2008. ISBN 978-80-251-2236-5.

[56] IEEE 802.16 WiMAX [online]. [cit. 2016-04-23]. Dostupné z: https://standards.ieee.org/about/get/802/802.16.html

[57] IEEE 802.15 PAN WIFI [online]. [cit. 2016-04-23]. Dostupné z: https://standards.ieee.org/about/get/802/802.15.html

[58] NATHAN, Mike. Vodafone femtocells hacked, root password revealed (online). Hafl a day, USA : 2011 [online]. [cit. 2016-04-23]. Dostupné z: http://hackaday.com/2011/07/14/vodafone-femtocells-hacked-root-password-revealed/

[59] PŘIBYL, Tomáš. Zákeřný útok jménem DoS (online). CCB spol., s.r.o., Česká republika: 2006 [online]. [cit. 2016-04-23]. Dostupné z: http://www.systemonline.cz/it-security/zakerny-utok-jmenem-dos.htm