Univerzita Hradec Králové
Fakulta informatiky a managementu
Katedra Informačních technologií

Analýzy bezpečnostních rizik smart grid sítí

Diplomová práce

Autor: Martin Holeček
Studijní obor: Informační management

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

Odborný konzultant: Ing. Vlastimil Novotný
specialista nových technologií
ČEZ a. s. Riegrovo nám. 1493/3, 500 02 Hradec Králové

Hradec Králové Duben 2016

Prohlášení:

Prohlašuji, že jsem diplomovou práci zpracoval samostatně a s použitím uvedené literatury.

V Hradci Králové dne 19.4.2016 Martin Holeček

Poděkování:

Děkuji vedoucímu diplomové práce, Mgr. Josefu Horálkovi, Ph.D. za metodické vedení práce, odborné rady a připomínky v průběhu jejího psaní. Dále chci poděkovat Ing. Vlastimilovi Novotnému za odborné konzultace a poskytnutí velmi odborných a cenných informací k problematice Smart Grid sítí a oblasti Smart Regionu Vrchlabí.

Anotace

Tato práce se zabývá aktuálním tématem sítí Smart Grid, jejichž cílem je snižování spotřeby elektrické energie a zvýšení podílu počtu zdrojů obnovitelné energie. Aktuálně je koncept testován v rámci mnoha projektů. V České republice je velmi významný a komplexní projekt Smart Region Vrchlabí.

Pro chytré chování elektrické sítě je využito automatizace prvků energetické soustavy a nasazení komunikačních technologií. Pro komunikaci je využíván mimo jiné protokol ethernet a sada protokolů TCP/IP. Tato skutečnost umožňuje přenášet útoky z datových sítí do prostředí SG. Přitom bezpečnost v SG je zásadním prvkem. Rozdíl dopadu útoku, který vyřadí z funkce webový server nebo i malou trafostanici, je zřejmý.

Cílem práce je identifikace takových hrozeb, jejich popis a analýza dopadu v SG síti. Vhodné je konkrétní útok otestovat v síťové laboratoři. Dále je cílem popsat účel, funkce a strukturu SG sítě.

Výsledkem práce je definování funkčnosti a struktury konceptu Smart Grid včetně popisu aktuálního stavu. V práci jsou definovány typy útoků shodné pro datovou i SG síť. Základní typy útoků jsou podrobně popsány. Je porovnán dopad na datovou a SG síť a navrženo opatření proti těmto útokům. Následně je vybrán útok UDP flooding a otestován v síťové laboratoři včetně funkčního opatření.

Annotation

Title: Security risk analysis of smart grid networks

This thesis is focused on the Smart Grid networks. The goal of Smart Grid is reducing electricity consumption and to increase the amount of renewable energy sources.

For these purposes is used automation of elements of electric grid. Important thing is utilization of ICT in electric grid and the use of ethernet and TCP/IP protocols. This is the reason why it is possible to use the same attacks in Smart Grid and computer data network.

The goal of thesis is identification of threats for Smart Grid, their description and analysis of the impact in the SG. One network attack also should be physically tested. Another aim is to describe the purpose, function and structure of SG network.

The result of the thesis is a definition of function and structure of the Smart Grid concept, including a description of state of art. In thesis there are defined attacks for SG, also description of these attacks and comparison of their impact in SG network and data network. There are also proposed measures against these attacks. Finally, there is a selected UDP flooding attack tested in the UHK laboratory network. Measurement has been also tested, and works properly.

Obsah

Seznam obrázků

Seznam tabulek

1 Úvod

Pojem Smart Grid je v oblasti energetiky v současné době stále novinkou. Smart Grid označuje určitou chytrou síť elektrického napětí. Jedná se o proces, kdy dochází k částečné nebo úplné automatizaci především distribučních sítí elektrického napětí. Tyto sítě jsou následně schopny reagovat například na změnu poptávky po elektrické energii. Dalším podstatným prvkem je vyšší využití zdrojů obnovitelné energie.

Smart Grid není zařízení, aplikace či síť, je to koncept využívající informační a komunikační technologie společně se sítí elektrické energie. Neexistuje jednotná fyzická realizace tohoto konceptu, jedná se o vývoj sítě a technologií za účelem definovaných cílů. (Flick a Morehouse 2011 s. 114)

Dle (Gharavi a Ghafurian 2011 s. 917) je Smart Grid energetickým systémem budoucnosti. Do SG konceptu spadá i téma Smart Metering či AMR (Automatic Meter Reading), tedy systém chytrých elektroměrů a práce s daty odběratelů.

Právě ze skutečnosti mnohotvárnosti konceptu a požadavků na něj, vzniklo v Evropě mnoho testovacích projektů SG sítí. Tyto projekty mají do jisté míry odlišné požadavky a různé pojetí realizace.

Aby bylo možné chytré chování sítě elektrického napětí uskutečnit, je potřeba její automatizace prostřednictvím komunikačních technologií. K tomu jsou využity síťové protokoly a průmyslové standardy. Na nižší vrstvě je využit protokol ethernet, na vyšší vrstvě je často nasazena rodina protokolů TCP/IP známá z datových sítí.

Elektroenergetického systému se týkají různá bezpečnostní rizika a hrozby. V případě realizace Smart Grid sítě se množství hrozeb výrazně zvyšuje. Mimo jiné jsou to právě možné hrozby pocházející z oblasti datových sítí. Tato skutečnost je založena na použitých komunikačních protokolech shodných s běžnou datovou sítí. Práce se zabývá mimo jiné právě těmito hrozbami. Jelikož literatura na toto téma není ucelená a často reflektuje pohled na koncept SG v odrazu na geografické lokace, či společnosti provozující testovací projekty, bude nedílnou součástí práce kompilát odborné literatury a článků na toto téma. Cílem práce je také popsat účel, důvod vzniku SG a aktuální stav v Evropě. Dále by již měla práce zohledňovat

především stav v České Republice a popsat funkčnost v testovacím projektu Vrchlabí. Více než vhodné je objasnit komunikační infrastrukturu a datovou komunikaci v SG síti.

Jelikož útoků na datové sítě existuje nespočet, práce by měla naznačit typy útoků dle motivů útočníka, proces, který útoku předchází a dále pak samotný útok. Následně je vhodné pro práci vybrat několik konkrétních útoků, popsat princip útoků, porovnat dopad v datové a SG síti a navrhnout opatření proti těmto útokům. Jeden z těchto útoků bude vybrán a prakticky zpracován a otestován v síťové laboratoři, stejně jako opatření proti takovému útoku.

2 Cíl práce

Cílem práce je analýza bezpečnostních hrozeb Smart Grid sítí, a to především v oblasti komunikace založené na sadě protokolů TCP/IP. Z toho vyplývá, že tyto hrozby jsou totožné s hrozbami známými v současných datových sítích. Práce by tedy měla vydefinovat typy hrozeb, analyzovat jejich podstatu a dopad v SG síti. K tomu se pojí návrh na zabezpečení proti vybraným hrozbám. Následně je cílem práce vybrat jeden typ útoku a reálně jej otestovat v síťové laboratoři, včetně opatření proti takovému útoku. Dále je více než vhodné popsat funkci a architekturu konceptu Smart Grid. Toto vyplývá z faktu, že koncept Smart Grid sítí je stále novinka v oblasti energetiky a literatura na toto téma není stále ujednocená.

Na funkčnost a cíle tohoto konceptu existují ve světě do určité míry rozdílné pohledy a názory. Toto vyplývá ze skutečnosti, že technologie Smart Grid se nachází stále ve fázi testování. Zatím nikde nedošlo k zařazení konceptu jako celku do reálného provozu na funkční celek typu kraj, provincie natož celého státu. Dále má na rozdílném chápání a očekávání od konceptu podíl skutečnost, že každý pilotní projekt, který je realizován, má odlišné cíle a odlišnou metodiku zavedení a nasazení.

Společnosti působící na území ČR v oblasti výroby, přenosu a distribuce elektrické energie patří do krizového řízení státu. Elektrárny a velké rozvodny mají klasifikaci objektů ODOS (Objekty Důležité pro Obranu Státu). Tato skutečnost vypovídá o důležitosti zabezpečení těchto sítí a jejich ochraně před případným cíleným útokem. Jelikož Smart Grid umožňuje ekologičtější výrobu a spotřebu energií, předpokládá se tedy postupné rozšiřování těchto technologií. Současně s tím bude i otázka bezpečnosti těchto sítí stále více aktuální.

3 Metodika zpracování

Práce je zaměřena na koncept Smart Grid sítí v oblasti energetiky, především na hrozby pro SG sítě, které jsou společné s hrozbami v datových sítích. Koncept Smart Grid sítí je stále novinkou a ve světě na tuto tématiku není ucelený pohled. Z tohoto důvodu se tato práce věnuje tématu z širšího aspektu. Součástí je tedy malý náhled na vývoj distribuční a přenosové soustavy, účel SG sítí, definice konceptu, popis funkčnosti, prvky SG a komunikační infrastruktury. Dále je popsán současný stav vývoje a testování konceptu SG v ČR a v Evropě. Při popisu a zpracování této části bylo využito velké množství zahraničních literárních zdrojů k této problematice. Z podstaty moderní technologie není pohled autorů na tuto problematiku jednotný. Tento fakt je dán současně situací, kdy různé pilotní projekty vznikly s odlišnými ambicemi, a testují mírně odlišné funkce SG. Tyto zdroje ze zahraničí byly kombinovány s informacemi a zdroji o současném stavu SG v ČR. Především tedy projektu v Smart Regionu Vrchlabí společnosti ČEZ, která je tvůrcem tohoto projektu. Část o komunikační infrastruktuře je podstatná pro další záměr práce a byla zpracována výhradně dle materiálů a reálně použitých technologií a postupů ve Smart Regionu Vrchlabí.

Stěžejní část práce se věnuje přímo bezpečnostním hrozbám SG sítí na úrovni komunikace s využitím protokolů TCP/IP. Tyto hrozby jsou identické s hrozbami z datových sítí. Je zde popsána jejich podobnost, náhled na postup útoku v síti a typy útoku. Dále jsou konkrétní útoky podrobně popsány. Pro útoky jsou porovnány dopady v datových a SG sítích a je navrženo opatření před těmito hrozbami, nebo aspoň minimalizace dopadu takovéto hrozby. Pro zpracování této části bylo využito vysoce odborné literatury v oblasti bezpečnosti sítí. Dopady útoků v SG síti byly konzultovány s Ing. Novotným ze společnosti ČEZ zabývajícím se SG sítěmi v projektu Vrchlabí.

Dále je vybraný typ DoS útoku názorně demonstrován v síťové laboratoři UHK. Typ útoku a způsob provedení byl pečlivě promyšlen a sestaven s ohledem na typizaci reálné topologie SG sítě ve Vrchlabí. Útok cílí na část sítě nutnou pro řízení sítě nízkého napětí pomocí komunikačního terminálu. V této části topologie již nejsou redundantní spoje ani prvky, proto je vhodným kandidátem pro takový

typ útoku. Následně je tedy zdokumentována funkčnost tohoto útoku a otestováno navržené opatření proti tomuto útoku. Toto testování probíhalo na fyzických síťových prvcích.

Pro tvorbu práce bylo využito množství odborných literárních zdrojů ze světové literatury, ale i českých zdrojů. Dále byly využity odborné články k problematice SG z prostředí internetu, a to vždy z uznávaných zdrojů či vědeckých databází. Současně jsem při tvorbě práce uplatnil znalosti získané během studia, především z předmětu počítačových sítí 1-4 a ochrany a bezpečnosti dat a informací vedeného v mém případě kurzem Cisco CCNA Security.

4 Elektrické sítě

Elektrická energie je v dnešní době téměř všudypřítomná, její využití je mnohočetné například v domácnostech, průmyslu i zemědělství. Elektrickou energii je relativně snadné přeměnit v energii mechanickou, tepelnou nebo světelnou pomocí nejrůznějších zářičů. Dalším důvodem pro tak rozšířené používání je možnost elektrickou energii hospodárně přenášet na velké vzdálenosti, stovky, někdy až tisíce kilometrů. Tento přenos umožňuje využít zdroje výroby el. energie z oblastí vzdálených od obydlených oblastí. (Zeman, 1966, s. 3)

Elektrická energie je pro svou univerzálnost, relativně jednoduchou výrobu, možnost přepravy od zdroje k místu spotřeby a účinnou přeměnu na jiné formy energie považována za nejušlechtilejší druh energie. Například účinnost přeměny na mechanickou energii pomocí elektromotoru je přes 90%. Přeměna na tepelnou energii(tepelné spotřebiče, chladničky) má účinnost také přes 90%, přeměna na zářivou světelnou energii má účinnost do 8% v případě žárovky, v případě zářivek a výbojek je účinnost až 40%. (ČEZ, a.s. 2003 Elektřina)

4.1 Historie a vývoj

Elektrické sítě sloužící pro přenos a distribuci elektrické energie prošly obdobně jako ostatní technické směry svým specifickým vývojem.

Jednou z oblastí, která nebyla dlouhá století probádána, je elektřina. Jedno z prvních reálných použití elektrické energie se datuje od osmdesátých let 19. století , bylo jím zavádění elektrického osvětlení využívající stejnosměrného proudu. Na prosazení stejnosměrného proudu měl velký vliv T. A. Edison v roce 1879, když předvedl svoji první žárovku s vláknem z zuhelnatělých bavlněných vláken. Tento typ veřejného osvětlení postupné vytlačoval plynové a petrolejové lampy. První vybudované elektrárny firmou Edison Company generovaly stejnosměrný proud, rozvod elektřiny byl však omezen při napětí 110V pro žárovky na 1 km. To znemožňovalo využití vodních elektráren, elektrárny museli být ve středu města, co nejblíže odběrateli. (Kubín 2006 s. 19 - 21)

V roce 1883 byl již uskutečněn přenos střídavého proudu o napětí 2000 V na vzdálenost 40 km. Nadále vývoj přenosu elektrické energie byl soustřeďován výhradně na přenos střídavého napětí. V roce 1918 bylo v Čechách 227 elektrických podniků, z nichž 193 mělo vlastní zdroj energie a 34 jich elektrickou energii nakupovalo. Největší elektrárnou v té době byla elektrárna Praha Holešovice s výkonem 23,5 MW. V roce 1919 byl přijat zákon o státní podpoře při zahájení soustavné elektrizace. Cílem tohoto zákona byla spolupráce mezi státem a podniky na budování elektráren a přenosové soustavy. První generace nových elektrárenských výkonů se datuje koncem šedesátých let 20. století, například elektrárna Opatovice (1959 - 1960), jednalo se o blokový systém elektráren, kdy každý blok disponoval výkonem 50 - 55 MW. V roce 1980 bylo rozhodnuto o výstavbě jaderné elektrárny Dukovany. Toto období vývoje již utvářelo elektrifikaci tak, jak ji známe dnes. (Kubín 2006 s. 21 - 42)

4.2 Současný stav

Cílem elektrizační soustavy je přenos a rozvod elektrické energie z místa výroby až do místa spotřeby. Elektrizační soustavu tvoří obvykle soustava přenosová a rozvodná, neboli distribuční. Účelem přenosových soustav je přenos velkých výkonů mezi hlavními uzly elektrizační soustavy. Rozvodné soustavy oproti tomu dopravují elektrickou energii z napájeného uzlu do jednotlivých skupin nebo oblastí spotřebičů. Veřejné rozvodné soustavy napájejí tzv. terciální sféru (byty občanská vybavenost), jsou z nich napájeny i rozvodné sítě průmyslové, zemědělské a dopravní. (Hradílek, 2008 s. 8)

Velmi podobně je popsána struktura práce elektrické sítě, jako zažité energetické paradigma dle (HADJSAÏD, 2012 s. 1), činnost dodávky elektrické energie je složena ze čtyř základních pilířů, těmi jsou elektrárny, které generují tuto energii, přenosové soustavy, distribuční soustavy a posledním článkem činnosti elektrické soustavy je odběratel takové energie. Důležité je, že v zažitém paradigmatu je tok elektrické energie vždy jednosměrný, od elektrárny směrem k uživateli. Až v posledních letech se začalo formovat nové paradigma, které souvisí

se změnami toků energie v síti, decentralizací prvků elektrické sítě a považuje informace o původu a spotřebě elektřiny za zásadní.

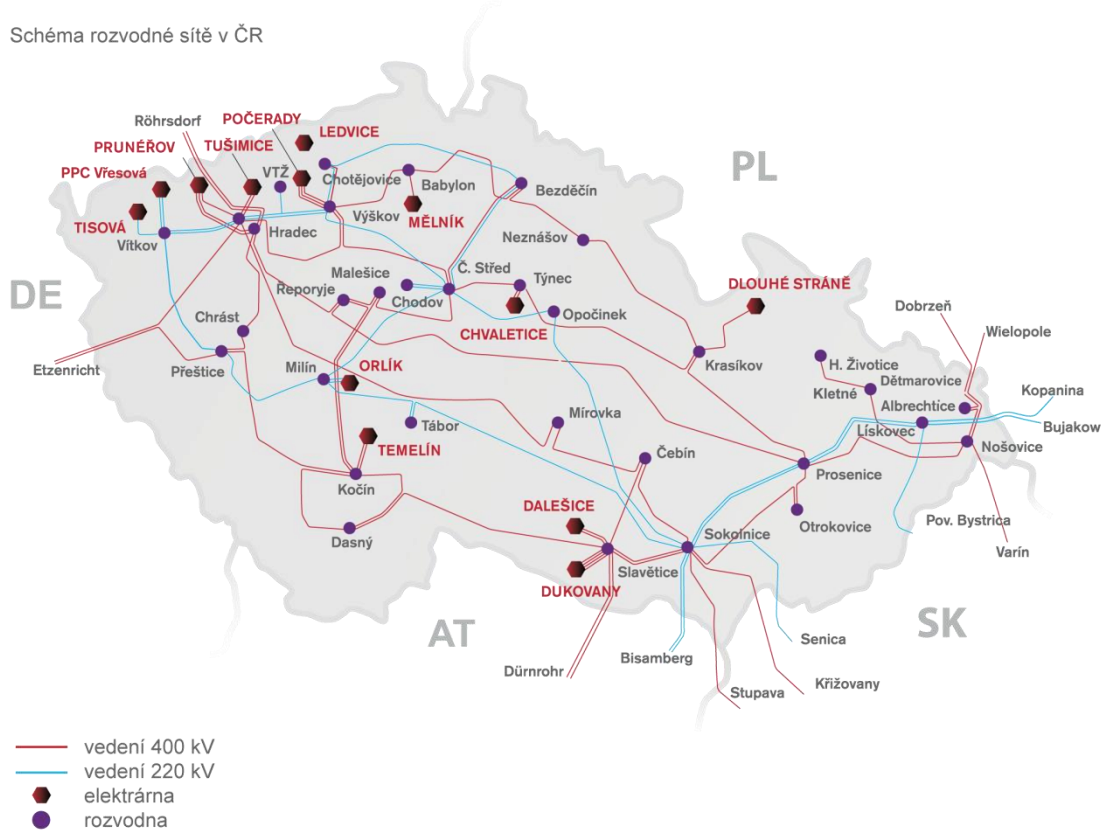
Přenosová i distribuční soustava využívají výhradně rozvody střídavého napětí, na území ČR se však vyskytují i rozvody stejnosměrného napětí, jedná se především o soustavy pro městskou trolejovou dopravu a elektrickou vlakovou dopravu. (Zeman, 1966, s. 11)

4.2.1 přenosová soustava

„Páteřní přenosová síť byla prakticky dokončena v 80. letech minulého století. V současné době ji tvoří hlavně vedení 400 kV. Trasy 220 kV, jejichž výstavba byla ukončena počátkem 70. let, dnes plní převážně úlohu záložních a doplňkových vedení. K přenosové soustavě patří 41 rozvoden se 71 transformátory pro obě základní napěťové hladiny. Historicky nejstarší soustavy 110 kV postupně v 70. letech převzaly úlohu uzlově napájených distribučních sítí. Elektroenergetická přenosová soustava 400 a 220 kV, často nazývaná „páteřní“, slouží k rozvedení výkonu z velkých elektráren do celého území České republiky a zároveň je součástí mezinárodního propojení Evropy. Napájí elektřinou distribuční soustavy, které ji dále rozvádějí až ke konečným spotřebitelům. Přeshraničními vedeními je přenosová soustava ČR napojena na soustavy všech sousedních států, a tím synchronně spolupracuje s celou elektroenergetickou soustavou kontinentální Evropy.“ (ČEPS, a.s. 2015 Technická infrastruktura)

Pro přenos vysokého výkonu na velké vzdálenosti se používá vysoké napětí z důvodů omezení ztrát výkonu na vodiči, jelikož se vodič zahřívá v závislosti k druhé mocnině procházejícího proudu, a zároveň se snižuje proud se zvyšujícím se napětím. Z toho vyplývá, že s vyšším napětím klesá zahřívání vodiče a úbytek ztrát při přenosu. V naší distribuční soustavě jsou použity linky vvn 220kV a zvn 400kV. (ČEZ, a.s. 2003 Elektřina) V zahraničí je použita i napěťová hladina ultra vysokého napětí 1000 kV, jedná se o země Rusko a Čína (ČEPS, a.s. 2015 Technická infrastruktura).

Páteřní elektroenergetická soustava ČEPS vede velmi vysoké napětí 220 kV a zvlášť vysoké napětí 400 kV. Tyto spoje spolu s dalšími prvky (elektrárny, rozvodny, transformační stanice) významnými pro přenosovou soustavu jsou vidět na obrázku 1.



Obr. 1Schéma rozvodné sítě ČR
Zdroj: ČEPS, a.s. 2015

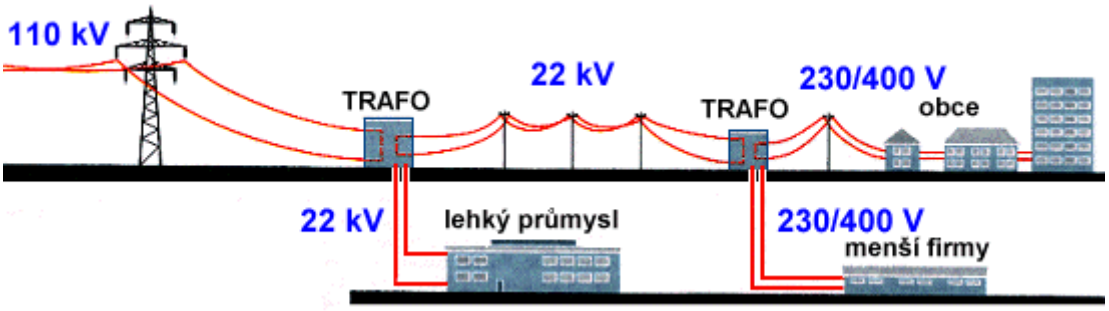
4.2.2 Distribuční síť

„V transformační stanici se velmi vysoké napětí transformuje na vysoké napětí 110 kV, část elektrické energie se přivádí do velkých podniků těžkého průmyslu a do měníren zajišťujících napájení elektrifikovaných železničních tratí. Zbývající část se distribuuje k dalším spotřebitelům (lehký průmysl, města, obce), kde se transformuje na napětí 22 kV. K poslední transformaci na nízké napětí 230V a 400 V dochází v samotných podnicích, obcích a městských čtvrtích. Do našich

domácností tak přichází elektrický proud nízkého napětí, který rozsvítí žárovku nebo pohání elektromotor vysavače.“ (ČEZ, a.s. 2003 Elektřina)

V současné době jsou hlavními hráči na trhu distribuce elektrické energie společnosti: ČEZ Distribuce, a. s., E. ON Distribuce, a.s. a PREdistribuce, a. s.. Cílem vývoje ve střednědobém horizontu je přizpůsobování zvyšující se decentralizaci výroby elektrické energie. K tomu je potřeba financování potřebných změn ve struktuře distribučních sítí. Dále je potřeba reagovat na plánovaný přechod přenosové soustavy na jednotnou hladinu napětí 400kV, tato změna by měla být provedena do roku 2040. (Elektrické sítě OTE, a.s. 2014)

Na obrázku 2 je vidět zjednodušená ukázka distribuční sítě.



Obr. 2 zjednodušená ukázka distribuční sítě
Zdroj: ČEZ, a.s. 2003 Elektřina

5 Inteligentní sítě Smart Grid

Zdroj (BORLASE, 2012 s. 16, 17) zmiňuje existenci mnoha definicí pojmu Smart Grid, i tento pojem zažil svůj boom pár let před rokem 2012, kdy v neodborných publikacích bylo pojmem Smart Grid označováno ledacos, třeba i mechanické součástky v elektrické soustavě. Dále zdroj upozorňuje na to, že neexistuje přesná definice, která by systém Smart Grid popsala ve všech ohledech, a to z jednoduchého důvodu, nejedná se o technologii, která se dá nainstalovat ze dne na den podle univerzálního postupu. Při nasazování konceptu Smart Grid je nutné postupovat individuálně s ohledem na současný stav elektrického energetického systému (zkráceně energosystém) v daném státě, ale také brát v úvahu geografické podmínky a ekonomické možnosti státu a politického systému. Následně zdroj uvádí zjednodušenou definici jak charakterizovat koncept Smart Grid, viz následující podkapitola.

Jelikož se pojetí konceptu Smart Grid liší pro různé kontinenty, tato práce reflektuje v první řadě koncept vhodný pro Evropu a stav energosystému v Evropě především v České republice. Zároveň však práce vychází z literatury a studií, které se zabývají mimo Evropu také konceptem pro USA.

5.1 Definice konceptu Smart Grid

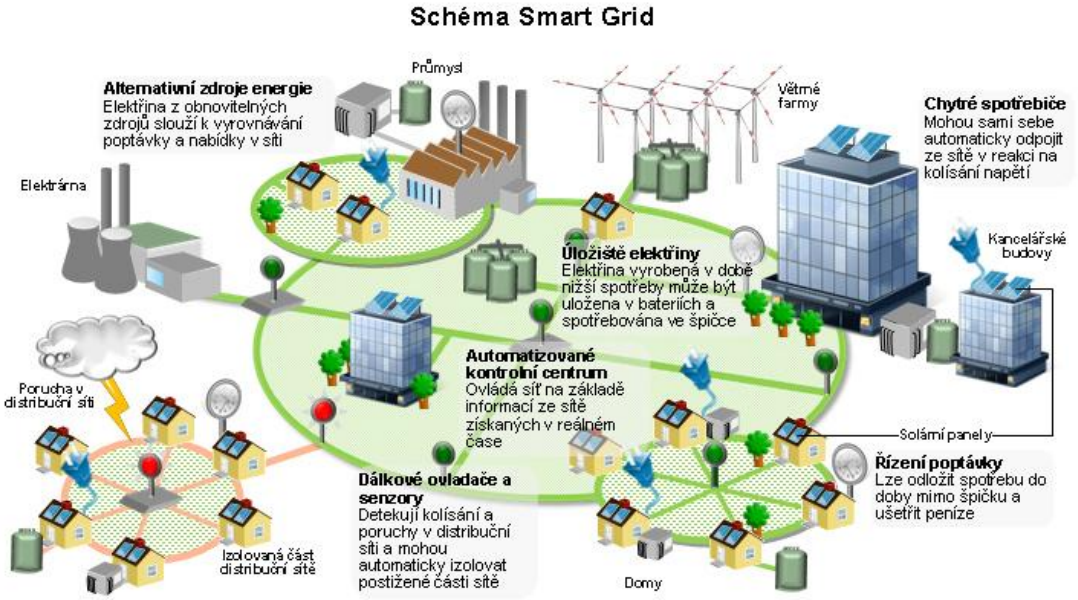
Smart Grid je integrace energosystému spolu s komunikační infrastrukturou, přičemž tato integrace je obohacena o moderní automatizaci a výpočetní technologie. Velice významná musí být synergie mezi zařízeními pro výrobu elektřiny a odběrateli. Smart Grid s sebou nese kompletní změny v poplatcích, politice, změny pro odběratele, průmysl a účastníky energosystému. (BORLASE, 2012s. 17, 18)

Dle (Begovic, 2013 s. 8) se jedná o modernizaci systému pro dodávku elektřiny, jeho monitoringu, ochrany a automatické optimalizace činností všech propojených částí tohoto systému.

Dle (Xiao, 2012 s. vii) je Smart Grid sjednocení celkového systému pro dodávku elektrické energie spolu s komunikačními sítěmi a prvky výpočetní technologie za účelem poskytování lepších služeb.

Ministerstvo energií Spojených států amerických poskytuje vlastní definici, co je to Smart Grid. Je to samoregulující systém, který umožňuje aktivní účast spotřebitelů pružně reagovat na útoky a živelné katastrofy pomocí možných úložišť energie, umožňuje zavedení nových produktů, služeb a trhu. Dále umožňuje využití a účinný provoz energie pro digitální ekonomiku. (HADJSAÏD, 2012 s. 17)

Koncept Smart Grid by měl umožnit zlepšení řízení el. energie za pomocí nejrůznějších technologií a techniky a spotřebitelů této energie. Toto by mělo účelně vést ke schopnosti zapojit vyšší počet obnovitelných zdrojů do energosystému a vzniku microgrids, jedná se o segmenty v síti s určitou schopností nezávislé funkce (ostrovní provoz) na nadřazené soustavě v případě poruchy vedení distribuční soustavy. Důležité je také zapojení občanů do řízení energetického systému. Kromě výhod s sebou však Smart Grid přináší také nástrahy v oblasti kybernetické bezpečnosti a ochraně soukromí. (STEPHENS, 2015) Na obrázku 3 je vidět ilustrační schéma struktury smart grid



Obr. 3 Schéma Smart Grid
Zdroj: ČEZ, a.s. 2013

5.2 Účel sítí a důvod vzniku

Důvodů vzniku konceptu Smart Grid je více. Důvody však vycházejí z technického a ekonomického aspektu, dále pak aspektu nařízení a regulace.

Při uvážení těchto aspektů je možno shrnout důvody vzniku a vývoje Smart Grid sítí dle (HADJSAÏD, 2012 s. 16) jako následující:

- Změna energetického paradigmatu, to zahrnuje v novém podání svobodný přístup na trh s elektrickou energií, možnost distribuovat výrobu elektřiny z obnovitelných zdrojů a nejednotnou účast mezi výrobci této čisté energie v krajině. Toto zahrnuje:
    - nediskriminovaný přístup k elektrické síti pro dodavatele
    - řízení přerušovaných dodávek elektrické energie z obnovitelných zdrojů
    - management pozorovatelnosti a odesílání informací o distribuované energii
- Dalším důvodem je stárnutí stávající elektrické soustavy.
- Potřeba připravit síť ve velkém měřítku na integraci nejvyšší bezpečnosti a ekonomických podmínek (potřeba optimalizace investic). Tato fáze potřebuje více flexibilní síť a její komponenty, včetně lepší automatizace procesů v síti.
- Inovace v rámci výpočetních a komunikačních prvků v el. síti. Rychlejší síťové a výpočetní prvky, častější úpravy cen, ochrana, senzory atd. Možnost využití Smart Meter, což je vhodný způsob, jak zapojit odběratele energie do interakce s poskytovatelem energie.
- Zvýšení spolehlivosti a kvality dodávky elektrické energie spotřebiteli.
- Potřeba reagovat na zvyšující se složitost elektrické soustavy.
- Možnost dodávky elektrické energie v tzv. ostrovním provozu.

Důvody vzniku dle uvedeného zdroje vypovídají mimo jiné i o účelu Smart Grid sítí.

Účelem sítí je vyšší efektivita přenosu elektrické energie a rychlejší zotavení po poruše v elektrické infrastruktuře. Zjednodušení tvorby cen a tarifů za elektřinu a to zejména díky tvorbě cen dle aktuálního vyráběného množství elektřiny a reakce odběratelů, respektive spotřebičů na tyto ceny pomocí chytrých

elektroměrů (Smart Metering). Tyto elektroměry umožňují čerpat energii v době, kdy je jí v síti přebytek. Například pro spotřebiče, u kterých nezáleží přesně na době provozu, například myčka, pračka, dobíjení elektromobilu atd. To umožňuje snížit množství špiček poptávky po elektřině. Dále Smart Grid sítě umožňují zapojení do sítě elektrické energie vysoké množství zdrojů obnovitelné energie. Účelem je také aktivně zapojit spotřebitele, tak aby se podíleli na optimalizaci spotřeby energie v síti. V neposlední řadě je účelem zvýšit bezpečnost, to jak pro případ zotavení po poruše, tak ochranu citlivých údajů spotřebitelů. (What is the Smart Grid, 2015)

„Podnětem pro energetiku celoevropského měřítka je SET Plan (Strategic Energy Technology Plan), jehož cílem je do roku 2020 splnit závazek EU a snížit emise skleníkových plynů o 20 % oproti úrovni z roku 1990, zvýšit podíl obnovitelných zdrojů energií v celkové spotřebě v EU na 20 % a zvýšit energetickou účinnost v Evropě o 20 % cestou komerční implementace nových konkurenceschopných energetických technologií. Pro splnění výše zmíněných cílů nastavuje SET plán dílčí cíle a aktivity v rozličných oblastech energetiky:

- průmyslové bioenergie
- zachycování, transport a ukládání CO2
- evropská přenosová a distribuční sít elektrické energie
- vodíkové pohony a palivové články
- udržitelný rozvoj jaderné energetiky
- energetická účinnost a „chytrá“ města
- rozvoj solární a větrná energie v Evropě

V rámci SET Plan začala v roce 2010 činnost **Evropské průmyslové iniciativy pro chytré sítě (EEGI)**. Tato iniciativa je tvořena distributory a technologickými společnostmi, kteří dávají důraz na rozvoj konceptu Smart Grid. EEGI se zaměřuje na demonstrační projekty po celé Evropě, jejichž cílem je vyzkoušet jednotlivé funkční celky Smart Grids. Skupina ČEZ je jediným zástupcem distributorů této iniciativy v regionu střední Evropy." (Evropský kontext: EEGI, SET Plan. *Skupina ČEZ* 2015)

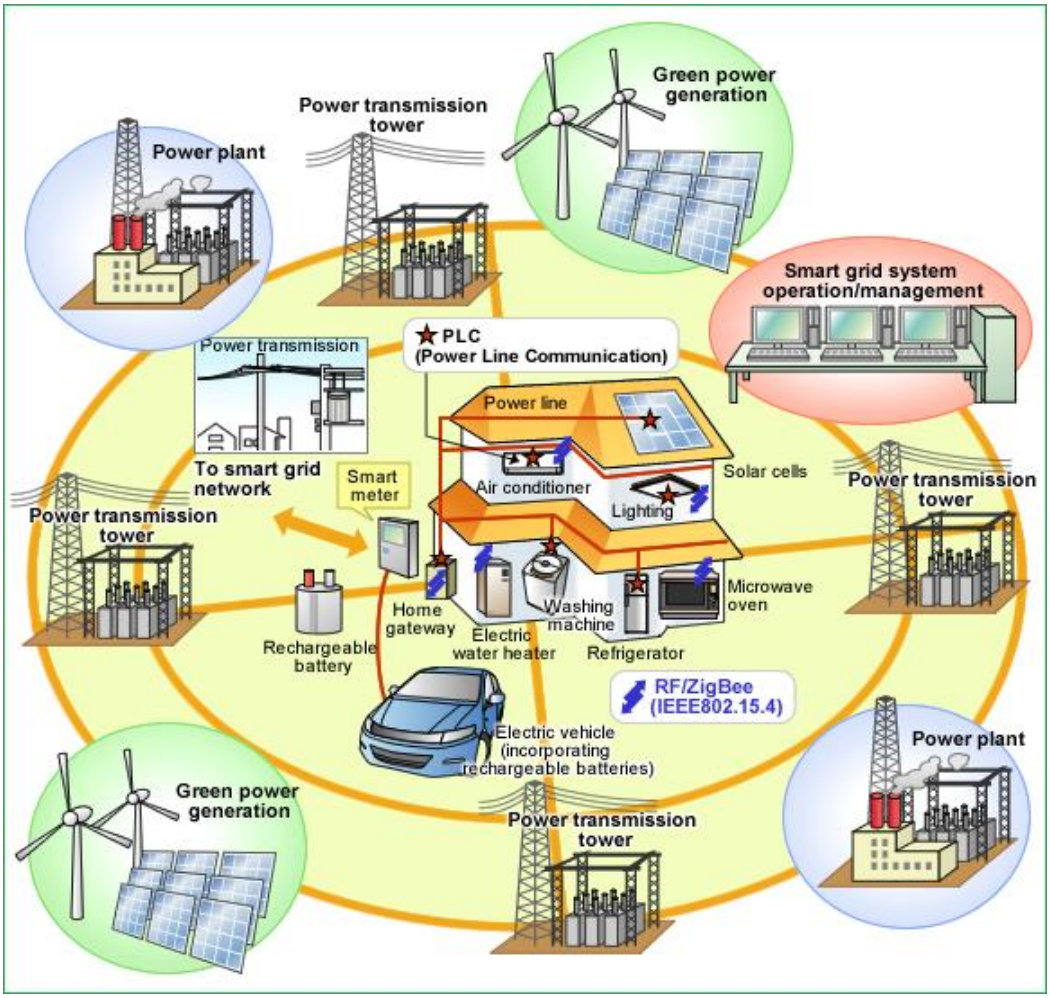
5.3 Struktura a komponenty sítí Smart Grid

Síť Smart Grid se skládá z mnoha komponentů, některé jsou identické se současnou elektrickou sítí, další komponenty ji doplňují, nebo nahrazují některé ze stávajících použitých zařízení. Mezi komponenty konceptu jako celku patří například i infrastruktura pro elektromobilitu, chápáno především jako síť dobíjecích stanic pro elektromobily. Dalšími komponenty jsou pochopitelně elektrárny, především kogenerační jednotky a lokální zdroje zelené energie, distribuční trafostanice umožňující změnu toku energie. Dále jsou to prvky automatizace, monitoringu sítě a prvky pro komunikaci v chytré síti. (Inteligentní sítě vstupují do České republiky. 2010 Skupina *ČEZ, a. s.*)

Právě prvky pro monitoring a pro komunikaci jsou zásadní pro řízení sítě a dělají elektrickou síť chytrou sítí. Spojením s dalšími komponenty a automatizací vzniká Smart Grid. Na obrázku 4 je znázorněno schéma propojení smart grid prvků a naznačena komunikace některých z nich pomocí PLC a ZigBee. Většina komunikací v SG sítích probíhá po optickém nebo metalickém vedení.

Prvky pro komunikaci a monitoring jsou především:

- Smart Meter
- Digital Grid Router
- Digital Grid Controller
- Data koncentrátor
- Server



Obr. 4 Smart Grid prvky a jejich komunikace
Zdroj: Electronics Corporation

5.3.1 Smart Meter

Jedná se o chytrý elektroměr, kromě toho co vykonává klasický elektroměr, umožňuje měřit aktuální napětí, odesílat data o spotřebě energie, měnit cenový tarif v závislosti na množství elektrické energie v síti a odběru ostatních uživatelů. To přispívá ke snižování poptávkových špiček po energii. Umožňuje spotřebiteli zobrazit údaje o jeho spotřebě, díky tomu mohou zákazníci více šetřit. Toto je zobrazováno na tzv. smart energy display, který je propojen s chytrým elektroměrem. Smart Meter umožňuje propojení s dalšími zařízeními, jako je například TV, plynoměr či vodoměr. Dále uživatel může vidět, z jakého zdroje elektrickou energii čerpal, kdy a za jakou cenu. To umožňuje odběrateli sledovat i ekologickou stopu jeho spotřeby. Odběratel může sledovat i takové rozdíly ve

spotřebě jako je vypnutá TV nebo ve standby režimu. (What is a smart meter? E.ON Company)

Smart Meter by měl umožňovat update firmware pro nové funkce, které bude potřeba zavádět během vývoje, a pro opravení chyb či nedostatků zjištěných v reálném provozu na konkrétní lokaci. Dále by měl mít unifikované komunikační rozhraní tak, aby prostřednictvím přenosu v LAN směrem k data koncentrátoru nezáleželo na výrobci nebo typu chytrého elektroměru. Tím se předejde složitému skladování všech nasazených typů elektroměrů pro různé data koncentrátory. (HADJSAÏD, 2012 s. 290)

Obvyklá komunikace mezi chytrým elektroměrem a dalšími jednotkami jako jsou např. vodoměr nebo plynoměr, probíhá nejčastěji pomocí ZigBee nebo M-BUS. ZigBee je vylepšený standard IEEE 802.15.4, umožňuje ověření zařízení, šifrování přenášených dat, směrování a přepínání. Díky tomu je mezi zařízeními využita topologie typu mesh. Největší výhoda této topologie je, že zařízení může komunikovat s jiným zařízením pomocí mezilehlých zařízení v topologii. Tímto se navíc zvyšuje dosah a spolehlivost sítě. (HO, 2014 s. 35)

5.3.2 Digital Grid Router (DGR)

DGR jsou procesorové AC/DC/AC měniče s internetovou komunikací. V digitální síti jsou tyto směrovače, řízené počítačem podobně jako směrovače v datových sítích. Jsou adresovatelné ze subsítě, propojují více sub-síťových článků skrze stávající střídavé vedení, kde každý je synchronizovaný interně, nejsou však synchronizovány s ostatními články. Umožňují výměnu energie s jinými články na předem plánovaném samo-koordinačním základě. Mohou podporovat frekvenční regulaci výměny energie z článku do článku. (NEUMAN, 2013 s. 8)

Pojem Digital Grid Router tedy označuje již spojení chytrého řídícího prvku a silového spojení. V reálném prostředí je takovýto router i s DGC součástí moderní trafostanice. Společnost ČEZ používá zvlášť označení pro prvky komunikace (Router) a automatizaci distribuční trafostanice nebo rozvodné či rozpojovací skříně. (Finální architektura technického řešení Smart Region, 2011 s. 22)

5.3.3 Digital Grid Controller (DGC)

Jedná se o regulátor digitální sítě, je to inteligentní adresovatelné zařízení, které je spojeno s každým aktivním prvkem sítě, např. tedy s generátory nebo zařízeními pro ukládání energie. DGC připravuje požadavek na přenos energie a realizuje zahajovací a konečný transfer energie, vytváří protokol o tomto přenosu z metadat, která jsou spojena s přenesenou energií. Zajišťuje autonomní provoz každého aktivního prvku uvnitř sítě. (NEUMAN, 2013 s. 8 -9)

5.3.4 Data koncentrátor

Představuje rozhraní mezí přenosem dat po elektrické nebo rádiové síti a jiným typem přenosu, často TCP/IP. Nachází se v trafostanici, kde končí informace posílané od uživatelů prostřednictvím chytrého elektroměru. Tato data mohou přicházet prostřednictvím PLC (Power Line Communication), tedy po silových vodičích. Jelikož data skrze transformátor neprojdou, je potřeba je odeslat na server jiným způsobem. Většinou pomocí LAN (Ethernet), WIFI, nebo GPRS. (FRANEK, 2012 s. 17)

Umožňuje přístup a obsluhu skupiny elektroměrů koncových klientů, tato skupina bývá označena jako cluster. Dále zajišťuje změnu protokolu, pokud je to nutné, v případě PLC vykonává dohled nad přenosovou a aplikační vrstvou. (HADJSAÏD, 2012 s. 286, 287)

5.3.5 Server

„Na konci řetězce se nachází server, který data zpracuje vhodným způsobem. Všechny nebo jen část dat je poskytnuta klientským stanicím. Zaměstnanci operátorského 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." (FRANEK, 2012 s. 17)

Zdroj (HADJSAÏD, 2012 s. 286, 287) místo serveru jmenuje jako klíčovou komponentu na konci informačního řetězce systém centrálních informací pro sběr informací a jejich zpracování.

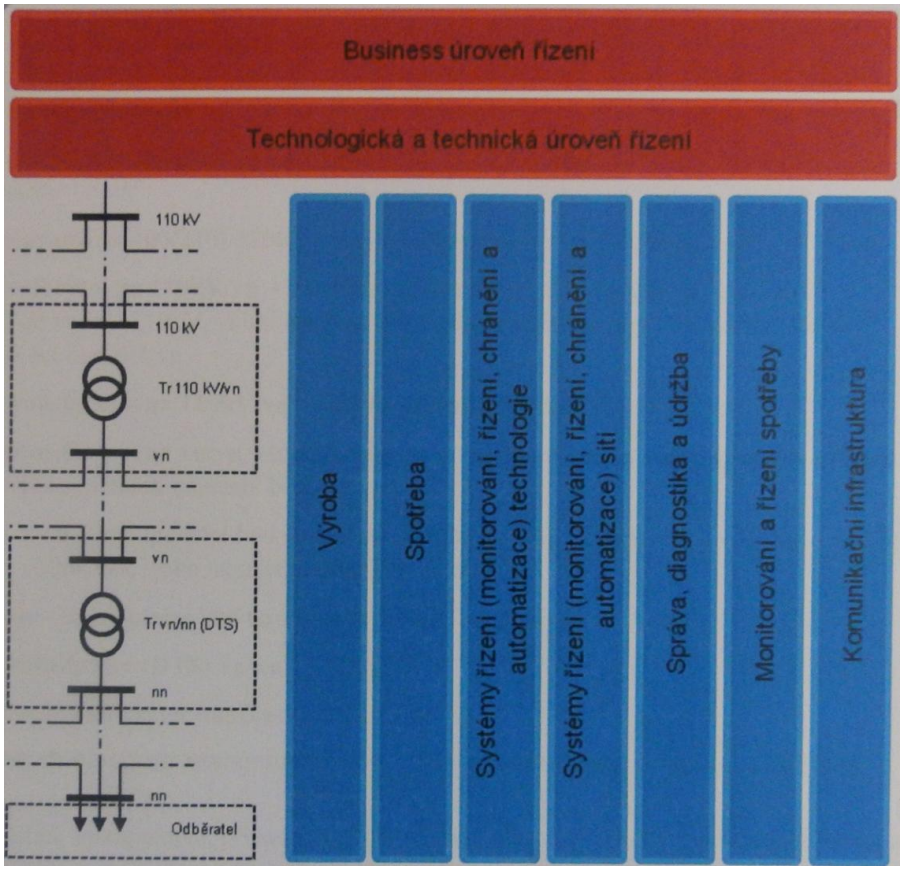
Z popisu je však zřejmé, že se jedná o identický prvek jako server. V literatuře jsou popsány různé pohledy na koncept Smart Grid. Názvosloví a členění prvků se ne málokdy liší.

5.4 Komunikační infrastruktura Smart Grid

Tato kapitola popisuje probíhající komunikační procesy a komunikační infrastrukturu ve Smart Grid a Smart Metering. Někteří autoři oddělují komunikaci v rámci Smart Grid a Smart Metering, jiní považují Smart Metering za součást SG. V této části práce jsou tyto komunikace odděleny. Popis této podkapitoly vychází především z technologických postupů užívaných v ČR společností ČEZ v pilotním projektu Smart Region Vrchlabí.

5.4.1 Vrstvený model distribuční sítě používaný společností ČEZ a. s.

Komunikační infrastruktura je jednou z osmi vrstev úplného rámce modelu distribučního systému, tento rámec je na obrázku 5. Bez komunikační struktury propojující všechny vrstvy v modelu není možné většinu funkcí konceptu Smart Grid vůbec realizovat.

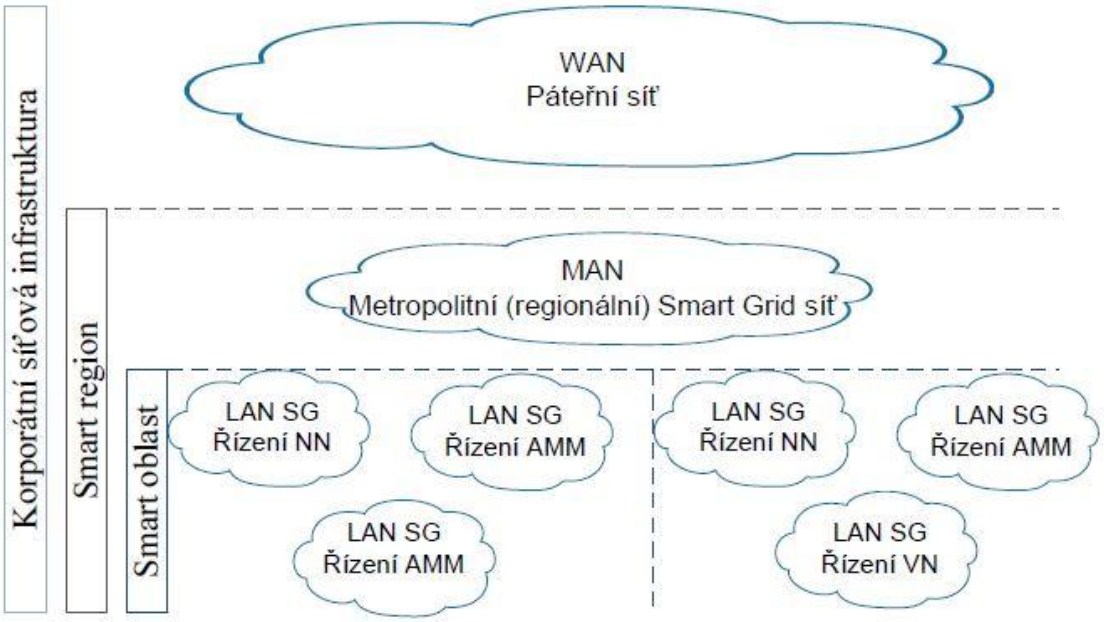


Obr. 5 Úplný rámec modelu distribučního systému
Zdroj: Finální architektura technického řešení Smart Region, 2011

Komunikační infrastruktura je typicky rozdělena do jednotlivých síťových segmentů, toto rozdělení je znázorněno na obrázku 6. Síť WAN (Wide Area Network) je zastoupena páteřní sítí ČEZ ICT Services a propojuje jednotlivé MAN SG. Tato síť využívá technologie vysokorychlostního ethernetu MPLS (MultiProtocol Label Switching), přenosové rychlosti se pohybují od jednotek až po stovky Gbit/s. Typickým přenosovým médiem je optické vlákno. Činitel pohotovosti v páteřní síti se pohybuje v rozmezí 99,9% - 99,999% (Finální architektura technického řešení Smart Region, 2011 s. 23, 24, 30, 31).

Zprostředkovává také připojení k systému SCADA. SCADA neboli Supervisory Control and Data Acquision, je základní aplikace systémů řízení, slouží například pro přístup k datům. Do systému SCADA jsou vysílány například souhrny dat zařízeními označovanými jako IED(Inteligent Electronic Device), což jsou zařízení pro automatizaci v distribuční síti. Ty mohou například ovládat trafostanice (Horálek a Soběslav 2012 s. 65-1).

Tyto data jsou vysílána pomocí protokolu 61850 (Horálek a Soběslav 2012 s. 65-1). K páteřní síti je připojena síť MAN SG (Metropolitan Area Network Smart Grid), ta zajišťuje propojení jednotlivých LAN SG, ty reprezentují jednotlivé lokální sítě SG architektury. MAN SG se obvykle rozkládá na úrovni jednoho smart regionu (např. Vrchlabí), do tohoto regionu spadají různé LAN SG jako smart oblasti (např. Liščí Kopec). MAN SG využívá různá média, především optická a metalická. Z technologií je to nejčastěji TCP/IP a MPLS. (Finální architektura technického řešení Smart Region, 2011 s. 22, 23)



Obr. 6 Přehled jednotlivých segmentů komunikační infrastruktury
Zdroj: Horálek a Soběslav 2012

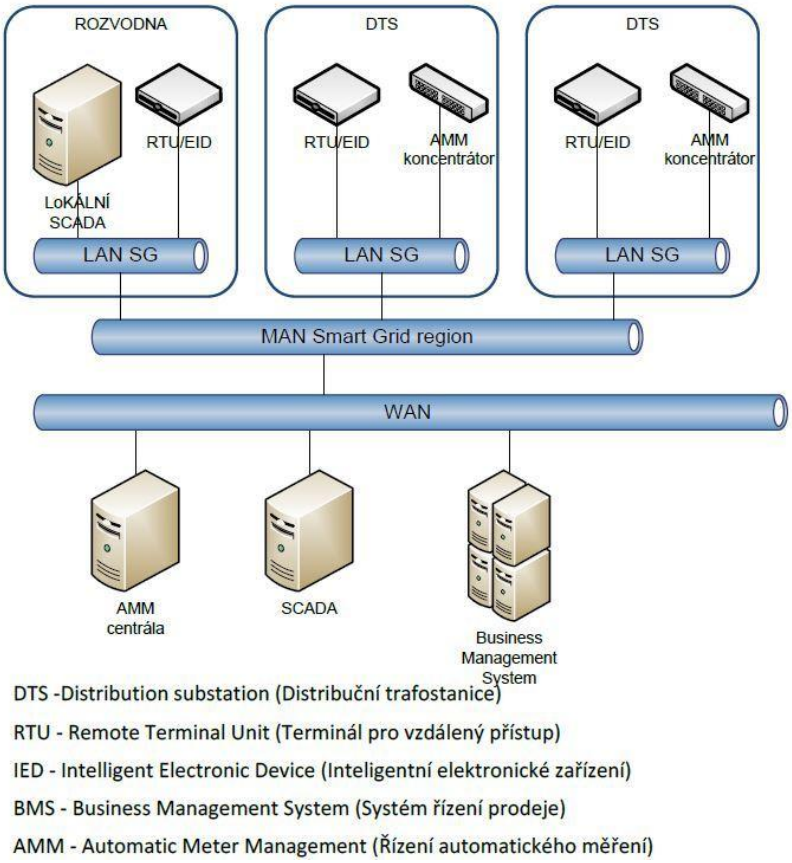
5.4.2 Hierarchická struktura komunikační infrastruktury

Tímto způsobem navržená hierarchická struktura datové sítě je velmi flexibilní a umožní snadné začlenění nových technologií a služeb. Zároveň je možné v takovéto síti použít různé přenosové technologie. I přesto je možné garantovat požadované parametry jednotlivých služeb (odezva, pohotovost, přenosová rychlost apod.). Oprávněným požadavkem je možnost využití sdílení komunikační infrastruktury tam, kde to technicko-provozní požadavky daných služeb dovolí. Jde především o vazbu mezi Smart Grid a Smart Metering.

Pro tento účel by mělo jít o sdílení komunikační infrastruktury na úrovni MAN SG v logicky oddělených VPN nebo VLAN. (Finální architektura technického řešení Smart Region, 2011 s. 23)

Pro horizontální vazbu funkce adaptace chránění (například mezi sousedními vn rozvodnami) je nutné realizovat datovou síť s rychlou a spolehlivou komunikací. Toho se zpravidla docílí tím způsobem, že je použita jednoduchá technologie (bez nutnosti složitého zpracování předávaných dat) a minimální počet mezilehlých prvků. Tyto požadavky lze splnit na úrovni LAN SG. Toto platí zpravidla pro každý systém řízení technologie, který řídí prvek pro řízení sítě, takovýto systém musí mít komunikaci k příslušnému řízení sítě. Jedná se o úrovně 110kV, vn i nn. Prakticky jde nejčastěji však o objekty vn a k nim náležící objekty nn. V LAN SG jsou často použity různé přenosové technologie, a to z důvodu, že služby a aplikace provozované na této úrovni se výrazně odlišují pozicí v síti (vn, nn). Na úrovni MAN SG lze tyto segmenty propojit díky použití standardizovaných protokolů rodiny TCP/IP. Zde již není problém vzájemně propojit technologie přenosu dat po metalickém nebo optickém vedení (Ethernet, WDM), po energetickém vedení (PDSL), anebo s využitím bezdrátového přenosu, např. GSM/GPRS nebo WiMAX. Zkratka PDSL označuje stejně jako již vysvětlená zkratka PLC datovou komunikaci v distribuční síti po napěťových rozvodech. (Finální architektura technického řešení Smart Region, 2011 s. 24, 25)

Dle Horálka a Soběslava (2012 s. 65-5) budou na komunikační infrastruktury a jednotlivé prvky energetické soustavy definovány požadavky na propustnost, latenci a spolehlivost. Přičemž propustnost znamená rychlost přenášených dat od zdroje dat do cílového zařízení. Latence je čas, který uplyne od vyslání zprávy po její přijetí. Spolehlivost je chápána jako schopnost odolávat rušivým vlivům na přenos (např. meteorologické nebo magnetické vlivy). Cílem je mít maximální propustnost, nízkou latenci a vysokou spolehlivost. Pro splnění těchto požadavků s ohledem na danou lokalitu a dostupné finanční zdroje bude navržená odpovídající technologie. Uspořádání fyzické komunikační infrastruktury v regionu SG a přístup k centrálnímu systému skrze páteřní síť je na obrázku 7.



Obr. 7 Schéma komunikační infrastruktury
Zdroj: Horálek a Soběslav 2012

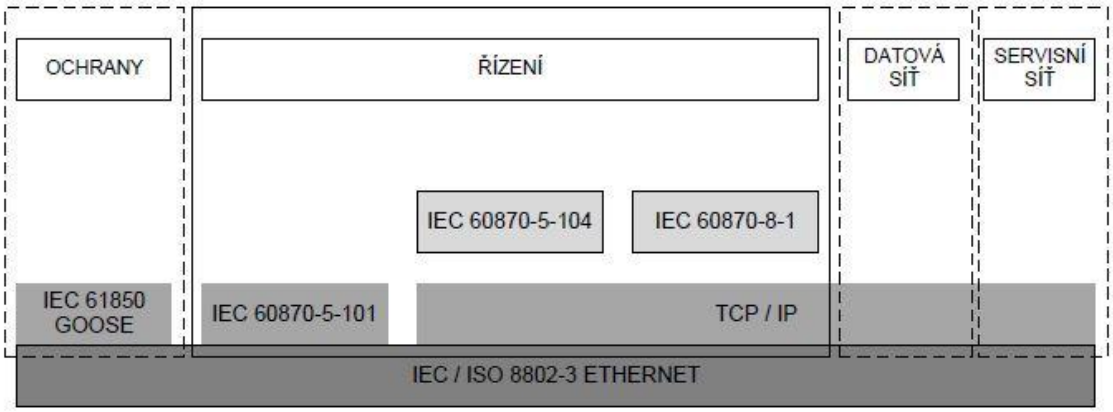
V SG lokalitě se používá pro přepínání a směrování síťových rámců a paketů přepínač (switch) a směrovač (router). Přepínač slouží pro komunikaci v lokalitě DTS a pro fyzickou komunikaci mezi lokalitami. Směrovač, tedy router řídí komunikaci směřující do MAN SG. Dále je zajištěna bezpečnost komunikace šifrováním a filtrováním. Zdroj doporučuje nad fyzickou infrastrukturou implementaci virtuálních sítí VLAN podle standardu IEEE 802.1Q. Jednotlivé VLAN jsou použity pro různé druhy komunikace, to zvyšuje bezpečnost provozu a zlepšuje kvalitu služby QoS (Quality of Service) pro dílčí komunikace. Mezi typy sítí v Smart Grid regionu patří: LAN SG, síť ochrany, povelová a přístupová síť. Základním protokolem je Ethernet, nad ním jsou použity další komunikační a aplikační protokoly. (Horálek a Soběslav 2012 s. 65-5)

„Základní VLAN sítě jsou využívány pro ochrany, tedy komunikaci GOOSE na horizontální úrovni mezi IED a zařízeními mezi různými DTS. Dále je možné ji využít pro řízení (síť určená pro předávání povelů řízeným prvkům distribuční

soustavy), sběr stavů a událostí v distribuční soustavě. Datová síť je určená pro sběr měření a odečtů z elektroměrů a dalších aktivních prvků jako jsou sondy a čidla. ICT dohledové sítě jsou určeny pro konfigurování a monitoring jednotlivých ICT zařízení." (Horálek a Soběslav 2012 s. 65-6)

Pomocí rychlých zpráv GOOSE lze například vypnout nebo zapnout spínač trafostanice vn v řádu desítek ms. (Finální architektura technického řešení Smart Region, 2011 s. 27)

Různé VLAN mohou používat různé komunikační protokoly. Na druhé vrstvě bude pro všechny sítě používán dle OSI modelu protokol Ethernet. Servisní a datová síť bude využívat standardní TCP/IP protokoly a k nim se vázající aplikační protokoly. Přehled protokolů pro sítě VLAN je vidět na obrázku 8. Pro řízení by měly být používány především protokoly IEC-60870-5 a IEC-61850-8-1. A to především z důvodů pro lepší bezpečnost protože jsou založeny na TCP/IP. (Horálek a Soběslav 2012 s. 65-6)



Obr. 8 Protokoly pro sítě VLAN
Zdroj: Horálek a Soběslav 2012

Výše uvedený popis komunikace se vztahuje především na komunikaci ve Smart Grid síti. Komunikace v oblasti Smart Metering s využitím AMM (Automated Meter Management) je považována v koncepci finální architektury Smart Region společností ČEZ za externí vrstvu. Tato vrstva je napojena formou AMM data koncentrátoru v segmentu LAN SG. Do data koncentrátoru jsou data přenášena nejčastěji formou PDSL. V některých případech také pomocí GSM/GPRS popřípadě UMTS nebo standardu IEEE 802.16 WiMAX. (Finální architektura technického řešení Smart Region, 2011 s. 36,37,38).

5.5 Současný stav Smart Grid sítí v Evropě

„Podnětem pro energetiku celoevropského měřítka je **SET Plan** (Strategic Energy Technology Plan), jehož cílem je do roku 2020 splnit závazek EU a snížit emise skleníkových plynů o 20 % oproti úrovni z roku 1990." (Evropský kontext: EEGI, SET Plan. *Skupina ČEZ* 2015)

„Lisabonská strategie přijata Evropskou radou v březnu 2000 v Lisabonu měla za cíl vytvořit z Evropské unie do roku 2010 „nejdynamičtější a nejkonkurenceschopnější ekonomiku světa založenou na znalostech, schopnou udržitelného hospodářského růstu a vytváření více kvalitních pracovních příležitostí". Lisabonská strategie byla v roce 2010 transformována do nové strategie Evropa 2020 s pěti ambiciózními cíly týkající se zaměstnanosti, inovací, vzdělávání, sociálního začleňování a změny klimatu a energetiky." (Evropský kontext: EEGI, SET Plan. *Skupina ČEZ* 2015)

Na konci této kapitoly je tabulka 1 některých zahraničních projektů a jejich vlastností, které zkoumají a testují z oblasti Smart Grid a Smart Metering. Do tabulky byl pro porovnání doplněn projekt realizovaný v regionu Vrchlabí.

5.5.1 Itálie

„Vládní nařízení na povinnou instalaci Smart Meters platí již od roku 2006. V roce 2011 by měly chytrá měřidla tvořit 95 % všech instalovaných. Doposud byly vyměněny ve 32 milionech italských domácností (cca 85 % odběratelů).

Energetická společnost Enel připravuje pilotní demonstrační projekt Smart Grids na jihu Itálie s cílem vyzkoušet aktivní řízení decentralizovaných zdrojů a spotřeby na vn úrovni distribuční sítě. Do projektu bude zapojeno cca 8 000 odběratelů a decentralizované zdroje, především FVE a VTE" (Evropský kontext: EEGI, SET Plan. *Skupina ČEZ* 2015)

Itálie je také jedním ze tří států (zbylé dva jsou Španělsko a Francie), ve kterých se realizuje komplexní výzkumný projekt ADDRESS v rámci FP7. Tento projekt má za cíl umožnit koncept aktivní poptávky elektrické energie. Toho má být docíleno přesunutím zaměření řídících mechanismů na budoucí zapojení malých a komerčních spotřebitelů do trhu silové elektřiny.

Konsorcium participujících firem zahrnuje 25 společností, činnost koordinuje společnost Enel Distribuzione. (Finální architektura technického řešení Smart Region, 2011 s. 121)

Hlavní cíle projektu ADDRESS jsou:

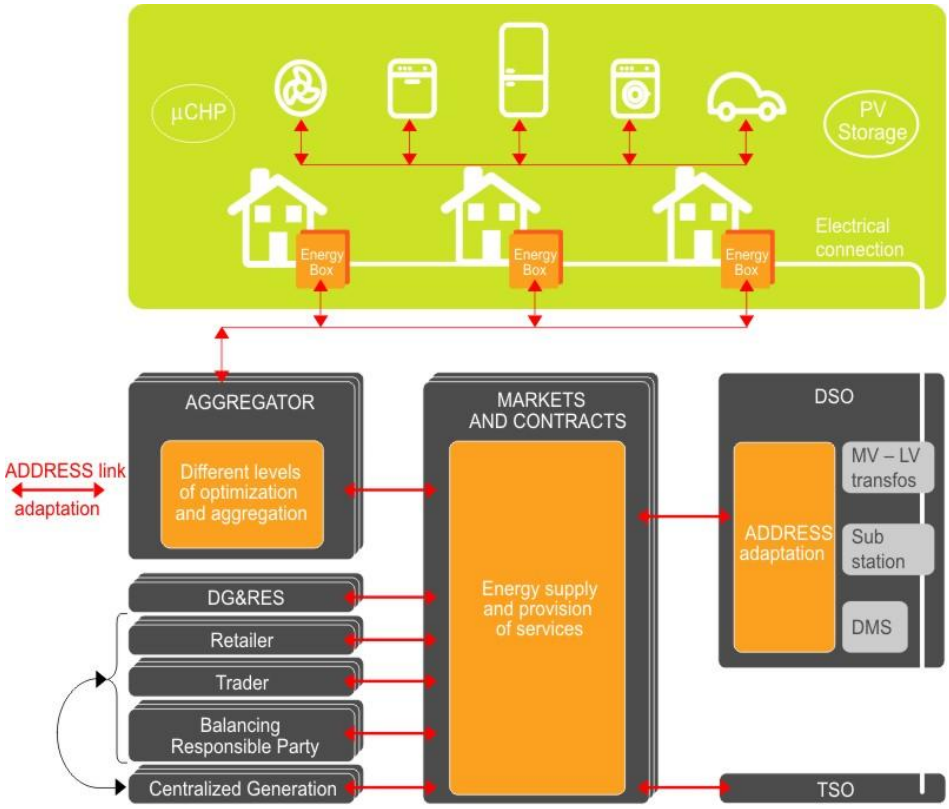
- rozvoj technických řešení na straně spotřebitele i na systémové úrovni
- vypracovat doporučení a řešení pro koncept aktivní poptávky elektřiny
- identifikovat potenciál přínosů pro účastníky energosystému
- vytvořit vhodné trhy a mechanismy k uplatnění a správě nových řídících scénářů

  (Finální architektura technického řešení Smart Region, 2011 s. 121)

5.5.2 Španělsko

Energetická firma Iberdrola spustila v roce 2010 pilotní projekt v regionu Valencie. Přes 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. (Evropský kontext: EEGI, SET Plan. *Skupina ČEZ* 2015)

Španělsko je další zemí, ve které je testován projekt ADDRESS, lokalita Castellon ve Valencii byla vybrána pro oblast specifických potřeb a vysokých teplot. Zahrnuto je 300 spotřebitelů pro řízení dodávky nízkého napětí s využitím energetického úložiště (EB - Energy Box). Cílem je ověřit využití na straně spotřebitelů, jejich ochotu se zapojit do role aktivního aktéra energosystému. Validace agregátoru a core business modelu. Dále je cílem validace navrhovaných služeb pro domácí systémy. Takovými službami jsou například: interakce zásobníku energie (EB) s vybavením domácnosti, komunikace EB a agregátoru dat nebo sběr a zpracování měřených veličin pomocí Smart Meter. Architektura projektu je na obrázku 9 . (ADDRESS Project Spain 2008)



Obr. 9 Architektura projektu ADDRESS
Zdroj: ADDRESS Project 2008

5.5.3 Německo

„Konsorcium firem a univerzity v Karlsruhe spustilo v roce 2009 pilotní projekt výstavby chytré sítě v průmyslovém regionu Karlsruhe-Stuttgart na jihu Německa pod názvem MeRegio. Do projektu se zapojí na 1 000 odběratelů z řad domácností, průmyslových podniků, výrobních a skladovacích jednotek." (Evropský kontext: EEGI, SET Plan. *Skupina ČEZ* 2015)

Cílem projektu MeRegio je především snížení emisí v testovaném regionu s využitím technologií Smart Grid. Toho má být dosaženo zapojením obnovitelných zdrojů. Projekt cílí na využívání myšlenky výroby elektřiny podle požadavků spotřebitelů a na regulaci spotřeby energie dle aktuální situace v síti. Toho má být docíleno prostřednictvím chytrých elektroměrů a dynamické tvorby cen. Cílem je testování a učení správnému chování odběratele elektrické energie v síti Smart Grid. V současnou chvíli je v testování zapojeno přes 950 odběratelů. (MeRegio - Aims of MeRegio)

„V německém Mannheimu se také realizuje pilotní projekt Smart Grid pod názvem Model City Mannheim (MoMa). Další projekty spouští i velcí provozovatelé distribučních sítí (např. E.ON, RWE). Projekty konceptu Smart Grids jsou obecně v Německu výrazně podporovány a to i na vládní úrovni." (Evropský kontext: EEGI, SET Plan. *Skupina ČEZ* 2015)

5.5.4 Francie

V březnu 2010 distribuční společnost ERDF spustila pilotní projekt Smart Grids, zahrnující na 300 tisíc domácností. Do roku 2017 by měly být nainstalovány Smart Meters ve 35 milionech francouzských domácností. ERDF spouští další rozsáhlý projekt s novou architekturou na úrovni nn i vn 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. (Evropský kontext: EEGI, SET Plan. *Skupina ČEZ* 2015)

Francie je třetím státem, kde je testován projekt ADDRESS, a to na dvou malých ostrovech Houat a Hoedic. Tyto ostrůvky se nacházejí v západní části Francie. Hlavním cílem tohoto projektu ve Francii je otestování kompletního řetězce řešení Smart Grid, podle zdroje je zde zapojeno do testování 50 - 100 odběratelů. Je zde testován obchodní model, možnosti nabídky a poptávky pro elektrickou energii, jako předmět obchodu. Dále je testováno technické ověřování poptávek, domácí chytré systémy a jejich komunikace a spolupráce s vyššími prvky v soustavě. Zjišťována je také možná výše provize pro zprostředkovatele přenosu elektrické energie. V neposlední řádě je zde testováno zařazení obnovitelných zdrojů energie do soustavy, jejich vliv na rovnováhu provozu přenosové soustavy a vliv na procesy účtování elektrické energie. (ADDRESS Project France 2008)

5.5.5 Česká Republika

Společnost ČEZ spustila v roce 2010 testování sítí Smart Grid v mikroregionu Vrchlabí. Poznatky z tohoto testování budou klíčové pro další rozvoj a nasazování Smart Grid sítí v ČR i EU. Region Vrchlabí byl vybrán pro tento

projekt záměrně, protože má vhodnou velikost, v regionu existuje dostatek obnovitelných zdrojů a projekt je prospěšný z ekologické pohledu pro blízkost Krkonošského národního parku. (Info k SR Vrchlabí. *Skupina ČEZ*)

Celý region je vhodně pokryt rozpadovými stanicemi a automatizovanými a dálkově spínanými rozvodnami vn. Ve Smart regionu je nejvýznamnější oblast Liščí kopec, tato oblast disponuje plnou automatizací i trafostanicemi a rozpojovacími skříněmi nn s dálkově ovladatelnými spínacími prvky. Všichni odběratelé v této lokalitě jsou vybaveni chytrými měřidly Smart Meter, s nimi jsou například propojeny i vodoměry. Data putují po PLC do koncentrátoru dat a odtud datovou sítí na řídící datové centrum. Dále je oblast vhodně pokryta rozpadovými stanicemi a automatikou umožňující ostrovní provoz oblasti z místní kogenerační jednotky. Rozpadové stanice a trafostanice jsou propojeny optickou datovou sítí a reagují velmi rychle, v případě poruchy na úseku dojde k propojení trafostanic a rozpojovacích skříní, tak aby byl minimalizován počet zákazníků bez dodávky elektřiny. Toto se odehraje v reálném čase a zákazník nic nepozná. Místní kogenerační jednotka vyrábí elektrickou energii pro danou oblast a současně s ní vytváří teplo, které je účelně využíváno pro obyvatele v oblasti. Kogenerační jednotka má elektrický výkon 1 560 kW a tepelný výkon 1 791 kW. Jednotka je také vybavená záložním diesel agregátem pro start ze tmy. Díky společné výrobě elektřiny a tepla dosahuje tato jednotka účinnosti 90%, pro porovnání tepelná elektrárna, která nijak nevyužívá vyrobeného tepla a vypouští jej do okolí, dosahuje účinnosti kolem 35%. Dále je v mikroregionu v rámci projektu E/MOBILITA v provozu síť dobíjecích stanic pro elektromobily. (Virtuální prohlídka ČEZ - Smart Region Vrchlabí. *Skupina ČEZ*)

Na obrázku 10 je vidět rozpojovací skříň nízkého napětí, v horní části jsou komunikační a řídící prvky (RTU, WiMAX anténa) a jejich záložní napájení. V dolní části jsou výkonové jističe ovládané řídící jednotkou (RTU).

Obr. 10 Rozpojovací skříň nn
Zdroj: Skupina ČEZ

Stát	Město	Název projektu	AMM	Komunikace	Inteligentní domácnost	Inteligentní město	Automatizace rozvoden	E-mobilita	OZE	Ostrovní provoz	Rozptýlená výroba
Holandsko	Amsterdam	Amsterdam Smart City	x	x	x	x		x	x	x	x
Španělsko	Castellon	Iberdrola	x	x			x	x			
Itálie		Enel	x	x			x	x			
Austrálie	Newington, Silverwater	EnergyAustralia	x	x	x		x	x	x		x
Portugalsko	Évora	Inovgrid	x	x	x	x		x		x	x
Španělsko	Malaga	Smartcity	x	x		x		x	x		x
Německo		MeRegio	x	x	x		x	x	x		x
USA	Ohio	gridSmart	x	x			x	x	x		
Rakousko	Salzburg	Smart grids Austria	x	x			x	x			x
ČR	Vrchlabí	Smart region	x	x	x	x	x	x		x	

Tabulka 1 přehled SG projektů a jejich oblasti zájmu
Zdroj: (Finální architektura technického řešení Smart Region, 2011 s. 124)

6 Bezpečnostní hrozby v Smart Grid sítích

Propojení průmyslové sítě a informační sítě (ICT) přináší řadu bezpečnostních rizik. Tato rizika však mají mnohem větší dopad v průmyslových sítích díky vyšší požadované pohotovosti služeb, než u ICT sítí. Dnes budované průmyslové sítě založené na TCP/IP a Ethernetu jsou paradoxně více zranitelné, než podobné systémy u ICT sítí. Tento fakt je dán tím, že výrobci průmyslových koncových zařízení, jakým jsou PLC řídící subsystémy, RTU jednotky, IED inteligentní zařízení, master servery, se soustřeďují především na správnou funkcionalitu daného prvku v rámci řídícího procesu, avšak ne vždy věnují větší pozornost integraci bezpečnostních protokolů do svých zařízení. Některým výrobcům chybí hlubší praktické zkušenosti z oblasti ICT sítí a jejich bezpečnosti. Často se také předpokládá, že průmyslová síť bude fyzicky oddělená, což samo o sobě bezpečnost do značné míry zajistí. (Finální architektura technického řešení Smart Region, 2011 s. 41)

6.1 Shodnost komunikace v SG síti s datovou sítí

Pro analýzu hrozeb je podstatná část komunikace probíhající na protokolech TCP/IP. V tuto chvíli lze použít již známé útoky z prostředí datových sítí a aplikovat je na sítě Smart Grid. Řízení prvků pomocí komunikační infrastruktury může probíhat následovně. Například řízení rozpojovací skříně nn (stejný princip může platit i pro další prvky) je možné dvěma způsoby.

Zaprvé je zde možnost využití staničního počítače (RTU) s funkcemi průmyslového komunikačního standardu Modbus, Profibus a IEC 60870-5-104 Slave -komunikace s nadřazenou úrovní. Současně s tím disponuje staniční počítač rozhraním pro technologii Ethernet, nad kterou probíhá komunikace pomocí TCP/IP a dále protokolem IEC 60870-5-104. (Finální architektura technického řešení Smart Region, 2011 s. 107, 108)

Druhou možností je varianta zdrojem označovaná jako CONV (znamená konverze). Jedná se o alternativu řešení bez "inteligentního prvku" ve skříni pro řízení nn, tedy bez staničního počítače RTU. Předpokládá se vytvoření transparentního kanálu v rámci LAN/MAN, který umožní přenesení průmyslového

standardu (Modbus, Profibus) na vyšší úroveň řízení, kde bude umístěn datový koncentrátor nn, který bude realizovat RTU společně pro skříně daného segmentu nn. Na místě RTU je umístěn konvertor CONV, který zajišťuje zapouzdření průmyslové standardu do rámců TCP. Toto řešení je navrženo především z úsporných opatření. (Finální architektura technického řešení Smart Region, 2011 s. 107, 108)

Datová i servisní síť je založena na protokolech TCP/IP, stejně tak tomu je u sítě řízení vn i nn. Cílem je vytvořit komunikační infrastrukturu pro přenos zpráv definované protokolem IEC 60870-5-104. Tato síť je tvořena směrovačem na úrovni DTS, případně i přepínačem při nedostatku portů. Přístup z LAN SG do MAN Smart Region je řešen vždy skrze směrovač. Směrovače na úrovni všech DTS je vhodné propojit mezi sebou, tím vznikne záložní routovací trasa v případě výpadku nějakého mezilehlého prvku. Směrovače by měly být vybaveny dynamickým routovacím protokolem (doporučen a používán OSPF nebo MPLS). Hraniční směrovače (přechod mezi LAN SG a MAN SG) by měly používat protokol VRPP pro zajištění vysoké dostupnosti díky redundanci směrovače. (Finální architektura technického řešení Smart Region, 2011 s. 107, 108)

6.2 Důvody útoků na průmyslovou síť Smart Grid

Z důvodu vysoké obsáhlosti a rozmanitosti SG sítí je nejvhodnější dělit útoky dle úmyslu. Nejčastějšími motivy pro útoky v SG síti jsou krádeže dat, například pro obohacení, konkurenční účely nebo průzkum a útoky směrované na znepřístupnění služeb, známé jako DoS (Denial of Services). Dalším cílem útoku může být manipulace služeb. (Knapp a Samani 2013 s. 58)

6.2.1 Krádež informací

V systémech řízení SG a jemu přidružených systémech je mnoho informací, jako například osobní data zákazníků a jejich fakturační data. Dále pak informace a data o provozu sítě, nebo spotřeby jednotlivých subjektů. Tato data a informace

mohou být zneužity k různým nekalým úmyslům. Od použití konkurencí až po ozbrojené cílené útoky. (Knapp a Samani 2013 s. 58, 59)

6.2.2 Znepřístupnění služeb - Denial of Services

Jedná se o jeden z nejčastějších útoků, zároveň však patří k jedněm z nejsnáze proveditelných. V dnešních sítích s vysokou datovou propustností je však obtížnější tento útok úspěšně provést. Zpravidla je k tomu zapotřebí poměrné množství systémů, tyto systémy jsou většinou infikovány a k útoku zneužity bez vědomí majitele. Pokud útočníci mají k dispozici někdy i miliony infikovaných počítačů, mají téměř neomezené zdroje pro tento typ útoku. Tento útok je však v sítích Smart Grid velmi aktuální, protože některá přenosová média mají nízkou propustnost dat, některé systémy a průmyslové protokoly jsou jen velmi málo zabezpečené. Tato podstata dělá většinu SG sítí velmi náchylnou na DoS útok. Útočníci mohou v zájmu útoku zahltit síť velkým objemem dat, provádět náročné skenování sítě ve velkých objemech, nebo udělat něco tak jednoduchého, jako je duplikování IP adres, možností je velké množství. Podstata mnoha průmyslových protokolů, jako je Modbus, IEC 60870, IEC 61850 a další, je komunikace v reálném čase, to znamená, že stačí částečný DoS útok, který naruší správnou funkci SG sítě. (Knapp a Samani 2013 s. 59)

6.2.3 Manipulace služeb

Na rozdíl od DoS útoku jde v tomto případě o manipulaci a účelové řízení služeb, například toku el. energie, poskytování nesprávných cenových tarifů atd. Jelikož SG sítě operují v reálném čase, je velmi těžké těmto útokům předcházet. Příklad relativně jednoduchého útoku je následující. Útočník úmyslně podvrhne časovou synchronizaci GPS, tím může dosáhnout cíleného odečtu odběru elektrické energie, myšleno především cenové politiky. V případě, že má v úmyslu způsobit nestabilitu v síti, může tímto nevhodně zařazovat energetické zdroje, které jinak slouží pro vyrovnávání poptávkových špiček. Zdroj dokonce zmiňuje případ, kdy podvržením dat lze zaměnit nízké a vysoké napětí na vstupy a výstupy transformátoru. To má katastrofální následky v podobě přehřátí cívek, přivedení chladícího oleje k varu a masivní explozi transformátoru.

V následující tabulce číslo 2 jsou vybrány cíle možných útoků v SG síti, ukazatele těchto útoků a oblasti dopadu. (Knapp a Samani 2013 s. 60)

Cíl útoku	Možný ukazatel	Dopad
Transformátory	• Změny napětí/frekvence	• životnost transformátorů • bezpečnost rozvodny • bezpečnost el. vedení • řízení zátěžových situací
Systém pro management energie	• zatížení sítě • historie zatížení	• chyby řídícího systému sítě • AMM • chybná fakturace el. energie
Chytré elektroměry	• spotřeba el. energie, plynu, vody	• data ze Smart Meters • fakturační systém • informace pro zákazníka • systém poptávky po energii
Události a upozornění v SG síti	• chybné události, upozornění a další systémové zprávy	• na všechny informace, události a systém upozornění

Tabulka 2 Cíle útoků v SG síti a jejich dopady
Zdroj dat: (Knapp a Samani 2013 s. 61)

6.3 Metody útoků v Smart Grid síti

Standardní proces postupu drtivé většiny je obdobný s datovými sítěmi. Tedy průzkum a skenování, určení cesty útoku dle možnosti chyb, průnik do systému například pomocí znalosti hesla, znalosti chyby v zabezpečení systému nebo protokolu, nebo slovníkovým útokem. Dále záleží na motivu útoku, pokud jde například o krádež dat, tak taková data mohou být odcizena. Pokud jde o manipulaci prostředků, je typicky snaha změnit systémové soubory pro zachování škodlivého kódu (malware), většinou virus, nebo může jít o nasazení škodlivého softwaru, který má za cíl šířit se na další systémy v síti. V tomto případě bývá tento malware označován jako červ (worm). Například může být na systém umístěn nějaký skrytý keylogger pro získání hesla do dalších systémů nebo konzolí. Různé útoky mohou být také kombinované s fyzickými útoky, například podle informací o spotřebě elektřiny může být vytipován neobývaný objekt, který může být následně fyzicky vykraden. (Knapp a Samani 2013 s. 74, 75)

6.3.1 Průzkum SG sítě

Pasivní testování a průzkum sítě zahrnuje nepřímou interakci s potenciálním cílem útoku. Informace k průzkumu mohou být získány pomocí různých síťových nástrojů především těch softwarových pro analýzu sítě. Mohou být také však získány zcela legálně, například informace o komunikační infrastruktuře mohou být zveřejněny na webu společnosti, nebo být uvedeny v publikaci či webu třetích společností. Typický příklad je uvedení výrobce použitého zařízení v SG síti, na stránkách výrobce bývá často ke stažení technická dokumentace k produktům. Z těchto dokumentů lze vyčíst mnoho informací zneužitelných k následnému útoku. Tabulka 3 ukazuje výčet některých nástrojů vhodných pro útoky na SG sítě ale i datové sítě pro různé fáze útoku. Produkty označené hvězdičkou jsou dostupné zdarma. Během této fáze bývají shromažďovány následující informace (Flick a Morehouse 2011 s. 114):

- IP adresy a jejich rozsahy přiřazené cílům v dané síti
  IP adresy a síťová jména (hostname) prvků:
  - Web servery

- DNS servery
- E-mailové servery
- Routery
- Brány v síti
- VPN koncentrátory
- Webové aplikace poskytovatelů služeb (například web pro kontrolu termostatů)

- Vedlejší informace o síti (grafy událostí, síťové diagramy)

(Flick a Morehouse 2011 s. 116)

6.3.2 Objevování

V této fázi se jedná zejména o hledání služeb, zařízení a komponent sítě a její topologie. Svým způsobem se předchozí a tato fáze prolínají a není lehké ani žádoucí je striktně oddělovat.

Pro účely hledání objektů v síti či systému se typicky používá pingování (využívání protokolu ICMP) a skenování portů. K tomu opět nejčastěji slouží vhodné nástroje, některé z nich jsou v tabulce 3. V této fázi je také typické hledání dostupných síťových cest (routovací záznamy v routeru), domén v síti a ACL (access control lists) na routerech. Typicky z domény pro Smart Meters není možné se spojit s doménou řídicího systému v elektrárně. Skenování portů a průzkum sítě by měl být veden z každé síťové domény, to je svým způsobem náročné na útočníkův čas. (Flick a Morehouse 2011 s. 116)

6.3.3 Identifikace míst k průniku

V této fázi je vytvářen jakýsi seznam zranitelných míst systému či SG sítě. Přestože SG sítě využívají nových technologií, stále zde platí principy komunikace datových sítí a fungují zde standardní nástroje pro hledání slabých míst. Opět některé z nich ukazuje tabulka 3. Výjimku tvoří proprietární protokoly a služby. Obecně takový analyzátor nejprve zjišťuje otevřené TCP a UDP porty a na nich běžící služby, následně naslouchá komunikaci služby na tomto portu. Některé nástroje zjišťují výrobce softwaru a jeho verzi, z té následně analyzátor chyb v

zabezpečení zjistí na jaké útoky je zařízení nebo běžící služba náchylná. Může být pomocí nástrojů testováno výchozí heslo výrobce pro službu či zařízení. (Flick a Morehouse 2011 s. 114)

Fáze útoku	**Jméno softwaru**	**Odkaz**
Průzkum	Maltego	http://paterva.com/web6/products/maltego.php
	PassiveRecon*	https://addons.mozilla.org/cs/firefox/addon/passiverecon/
	Tcpdump*	www.tcpdump.org
	Wireshark*	www.wireshark.org
Objevování	Nmap*	http://nmap.org
Identifikace chyb zabezpečení	Nessus	http://www.tenable.com/products/nessus-vulnerability-scanner
	NeXpose	http://www.rapid7.com/
	OpenVAS*	www.openvas.org/
	Qualys	https://www.qualys.com/
Průnik	Core Impact	www.coresecurity.com/
	Metasploit*	www.metasploit.com/

Tabulka 3 Nástroje pro testování zabezpečení sítí
Zdroj: Flick a Morehouse 2011 s. 114

6.3.4 Průnik zabezpečením

Jedná se o využití nějaké chyby v zabezpečení, která byla zjištěna v předchozí fázi. Následující otázkou je to, co může útočník získat. Nabouraný prvek může například obsahovat citlivá data o zákaznících, nebo mít přístup k ovládání důležitých funkcí elektrárny. Pokud nás zajímá zabezpečení prvků, je vhodné dělat tyto testy průniků pomocí vhodných nástrojů z pozice správce sítě či zabezpečení. Tím je možné odhalit jaké informace nebo jaké služby jsou přístupné v chybách zabezpečení. Pokud útočník objeví chybu v zabezpečení, může ji využít k různým účelům, tedy k úniku informací, DoS útoku či ovládání a manipulaci provozovaných služeb a systémem ovládaných činností. Manipulace činnosti systému a služeb se

typicky provádí po vzdáleném připojení ke konzoli. (Flick a Morehouse 2011 s. 114)

Zde je následný popis jak může probíhat postup k vzdálenému ovládnutí systému útočníkem. (Flick a Morehouse 2011 s. 114)

1. využití chyby v zabezpečení k nasazení vzdálené konzole
2. ukradení souboru s přístupovým heslem na cílovém systému
    a. nad systémem s Windows nahrání skriptu (např. fgdump) např. pomocí TFTP, skript ukradne soubor s heslem a ověřovací soubory
    b. spuštění fgdump rovnou
    c. použití opět programu pro přenos souborů (např. TFTP) pro přenesení vygenerovaného souboru pomocí fgdump
    d. zahlazení stop po činnosti, smazání skriptu a logovacích souborů
3. použití tabulek pro reversní kryptografii, ke zjištění hesla
4. přihlášení se do systému pomocí získaného administrátorského hesla
5. pokud se správce systému přihlásí do systému například pro zjištění co se děje, útočník typicky změní heslo administrátora, pokud ho změnil první správce, bývá toto heslo uloženo v cache paměti
6. dále již útočník používá nové heslo administrátora pro přihlášení kamkoliv v doméně

6.4 Typy útoků v datové síti

V této podkapitole jsou klasifikovány útoky v datové síti do tří typů. Jedná se o tři nejčastěji klasifikovatelné skupiny útoků dle společnosti Cisco. Těmito třemi skupinami jsou průzkum sítě, neautorizovaný přístup do sítě a DoS útok. Typy útoků jsou jakýmsi postupem útoku a prozrazují záměr útočníka, je zde tedy shoda s typy a metodami útoků v SG sítích.

6.4.1 Průzkum sítě

V této fázi jsou často používány ICMP dotazy, nástroje pro analýzu síťového provozu, paketů a testování otevřených portů. Oblíbeným nástrojem je Wireshark pro analýzu síťového provozu a paketů a Nmap pro skenování portů. Další nástroje jsou opět uvedeny v tabulce 3. Nejdříve jsou typicky zjišťovány aktivní hosté v síti pomocí ICMP ECHO dotazů, na těchto hostech jsou následně testovány otevřené známé TCP a UDP porty. Tento typ útoku často předchází útoku pro získání přístupu nebo DoS útoku. Odhalení průzkumu sítě je možné pomocí instalovaných nástrojů a služeb, ty reagují například na velké množství ICMP dotazů, tyto nástroje mohou následně upozornit např. správce sítě. Jedním z takových nástrojů je Cisco ASA (Adaptive Security Appliance). (CCNA Security. 2015)

6.4.2 Neautorizovaný přístup

Důvodem pro tento útok je velmi často odcizení dat. Útok je využíván téměř vždy pro přístup do nějaké síťové komponenty nebo při útoku na hesla. Tím může být útok takzvaně hrubou silou, který je založen na slovníkovém útoku. To je sice náročné na výpočetní výkon a čas, ale jde o jednoduchý a velmi často účinný způsob. Obrana proti takovému útoku je velmi silné heslo. Dále může být heslo získáno pomocí škodlivého softwaru (např. trojský kůň), nebo odchyceno v síťové komunikaci. Toto je označováno jako man-in-the-middle attack, tedy útočník je umístěn schematicky mezi dvěma komunikujícími subjekty v síti. K takovému útoku může útočník použít například L0phtCrack, pokud přijde na heslo, zajistí si často do systému skrytý přístup pro budoucí použití. (CCNA Security. 2015)

6.4.3 DoS útok

Jedná se o útok s cílem vyčerpání výpočetního výkonu obsluhujícího prvku, nebo přerušení služby a znemožnění regulérního využití služeb jiným platným uživatelem. V datových sítích patří k jedněm z nejčastějších a nejsnáze proveditelných útoků. Útok může být například proveden generováním velmi vysokého množství dat a zahlcením datové sítě, nebo obsluhujícího výpočetního prvku v síti. Existují dva důsledky způsobené DoS útokem. Prvním je nemožnost síťového prvku nebo aplikace zpracovat úmyslně nezpracovatelná data ve špatném

formátu nebo neočekávané příkazy a interakce systémových komponent. Druhým důvodem je neschopnost systému zpracovat enormní množství vstupních dat, tímto se stává systém nebo služba nefunkční nebo extrémně pomalá. DoS útok je považován za jednu z hlavních hrozeb, například jím může být přerušena obchodní činnost závislá na síťové komunikace (CCNA Security. 2015)

V poslední době je často tento útok modifikován a pro zahlcení systému nebo sítě je používáno více koordinovaných zařízení. Tyto zařízení jsou označovány jako agenti, majitelé těchto zařízení typicky neví o tom, že z jejich zařízení je veden útok. Takový útok je označován jako DDoS (Distributed DoS). (CCNA Security. 2015)

6.5 Porovnání možných útoků, hrozeb a zabezpečení v datové a Smart Grid síti

Tato podkapitola se věnuje některým útokům společným pro datové a SG sítě. Jednotlivé útoky jsou popsány a vysvětleny. Následně je pro každý typ útoku popsán a porovnán dopad v datové a SG síti. Dopad na SG síť vychází z konzultací s Ing. Novotným společnosti ČEZ, který se věnuje problematice Smart Grid. Dále jsou navržena opatření proti těmto útokům nebo minimalizace jejich dopadu. Konkrétních útoků existuje velmi mnoho, pro práci byly vybrány typické útoky pro různé oblasti.

Je nezpochybnitelné, že útoky na SG sítě mohou mít nesrovnatelně vyšší důsledky než útoky v prostředí datových sítí a internetu.

V červenci roku 2010 byly publikovány první zprávy o rootkitu Stuxnet, určeném pro systémy SCADA společnosti Siemens používané v jaderné elektrárně v Iránu. Poprvé bylo cílem výkonné zařízení, konkrétně PLC 7 300. Infikován byl software Step-7 sloužící k přeprogramování těchto zařízení. Dle autora tedy Stuxnet není pouze novým virusem, ale začátkem nové éry malware. Tato událost mění chápání malware a jeho cílů. Vrcholem byla dosud krádež peněz, nyní jde o ničení strojů a přímé ohrožení lidských životů. (Dočkal 2012 s. 50)

Stejně tak motivů pro útok v SG síti je mnohem více než v síti datové. Na úrovni komunikace na protokolech TCP/IP je provedení útoků z velké části podobné, liší se především v cílových službách, v roli potenciálního cíle útoku

a způsobu připojení do sítě. To především z důvodu fyzického oddělení SG sítě od internetu. Pokud data směrem do řídícího centra putují skrze internet, bývá to zpravidla v zabezpečeném a šifrovaném tunelovém spojení. V tabulce 4 jsou znázorněny rozdíly v pojetí zabezpečení SG sítě a datové sítě v běžném firemním prostředí. Některá vyjádření autora jsou kontroverzní.

Komponenta v zabezpečení	**Řídící síť v oblasti energetiky (SG)**	**Běžná datová sít ve firemním prostředí**
Antivirus	Neobvyklý / těžko nasaditelný	Běžně dostupný / snadno nasaditelný
Životnost komponenty	Více jak 20 let	Nejčastěji 3 - 5 let
Outsourcing	Velmi zřídka možnost využít	Běžně a snadno použitelný
Aktualizace komponent	Specifická, podle konkrétních potřeb	Pravidelná / plánovaná
Běh v reálném čase	Bezpodmínečně nutný pro bezpečnost	Malá prodleva přijatelná
Testování zabezpečení	Zřídka (zpravidla pro operační síť)	Plánované a standardizované
Fyzické zabezpečení	Velmi variabilní dle situace a zařízení	Vysoké
Povědomí o bezpečnosti	Zvyšující se	Vysoké
Důvěrnost dat	Nízká - střední	Vysoká
Integrita dat	Vysoká	Vysoká
Dostupnost dat	24/ 7/ 365	V některých případech zpoždění akceptovatelné
Požadavek na bezztrátovost dat	Vysoký	Střední

Tabulka 4 Porovnání zabezpečení průmyslové a běžné datové sítě
Zdroj: Falk a Fries 2011 s. 172

6.5.1 Sběr důležitých informací na webu a sociálních sítích

Jak již bylo řečeno ve většině případů, předchází útokům sběr podstatných informací. Tyto informace mohou být získány na webu společností, výrobců zařízení ale také na sociálních sítích.

1) Sociální sítě byly stvořeny pro snadné vyhledávání osob a následnou komunikaci či sdílení souborů a informací. Lidé s profilem na sociální síti se velmi snadno stanou terčem sociálního inženýrství. Typickou hrozbou pro sociální sítě jsou falešné profily kolegů či obchodních partnerů s úmyslem získání cenných informací o nasazených technologiích či zabezpečení sítě. Skrze falešný profil může být útočník naveden na cílovou webovou stránku, která slouží k napadení počítače dané osoby, k tomu je použit a šířen nějaký malware. Tento malware může získat informace nebo proniknout přímo do prvků v síti. (Knapp 2014 s. 200)

Více sofistikovaný je útok, pojmenovaný jako spear-phishing. Cílenému uživateli je podstrčená webová stránka, například skrze sociální síť, kde je požadováno vyplnění formuláře. Uživatel zde dobrovolně zveřejní společnost, ve které pracuje, svoji adresu, svého nadřízeného či svoji pracovní dobu atd. Taková webová stránka se může tvářit jako doručovací služba, výhra v soutěži či jiné. (Knapp 2014 s. 201)

Opatření ad 1): V rámci ochrany sítě je potřeba zamezit úniku informací z řad zaměstnanců. Nesmí být však zapomenuto na externí dodavatele a společnosti zajišťující jakékoliv služby či servis chráněné sítě (Knapp 2014 s. 200). Opatřením je patřičné proškolení všech zaměstnanců, kteří přichází s datovou či SG sítí do styku na úrovni obsluhy, řízení či správy takové sítě. Toto může být podpořeno vhodnými smluvními podmínkami ve vztahu zaměstnavatel - zaměstnanec.

2) Veřejný web. Již v předchozí části práce bylo naznačeno, že průzkum sítě může probíhat i zcela legálně, jednou z takových cest je skládání zveřejněných informací. Například společnost vydá o své SG síti publikaci, nebo zveřejňuje články na svém webu. Pokud jsou například uvedeny i výrobci a typy zařízení použité v síti, je možné dohledat jejich specifikace na webu výrobce, ten zpravidla poskytuje stažení technické dokumentace. (Flick a Morehouse 2011 s. 114)

Toto se zpravidla týká SG sítí, u datových sítí společnosti nezveřejňují jakékoliv informace o svých datových sítích a použitých technologiích.

Naopak v oblasti veřejných datových sítí a internetu je možno dohledat spoustu dalších informací. Například na webu správce domény cz (nic.cz) je možné zjistit nemalé množství informací k doménovému jménu. Pokud nás zajímá web www.uhk.cz zjistíme tímto způsobem například kontaktní osobu (Jan Flek), tato osoba se může nadále stát předmětem sociálního inženýrství. Dále můžeme zjistit, že doména není zabezpečena technologií DNS Security. Další údaje jsou na obrázku 11.

„DNSSEC je rozšíření systému doménových jmen (DNS), které zvyšuje jeho bezpečnost. DNSSEC poskytuje uživatelům jistotu, že informace, které z DNS získal, byly poskytnuty správným zdrojem, jsou úplné a jejich integrita nebyla při přenosu narušena. DNSSEC zajistí důvěryhodnost údajů, získaných z DNS." (CZ.NIC 2016)

VYHLEDÁVÁNÍ V REGISTRU (WHOIS)

Výsledek vyhledávání **uhk.cz**.

PROHLÍŽENÍ DOMÉNOVÉHO JMÉNA

Doménové jméno	uhk.cz
Registrace od	14.06.2000
Poslední aktualizace	04.04.2012 00:52:58
Datum expirace	16.06.2016
Držitel	SB:UHK University of Hradec Králové
Administrativní kontakt	JFLEK Jan Flek
Dočasný kontakt	
Určený registrátor	REG-GENREG GENERAL REGISTRY, s.r.o. od 22.06.2004 14:05:00
Zabezpečeno pomocí DNSSEC	⛔
Stav	

Sada jmenných serverů	NSS:HKNET_UHK:1
Jmenný server	ns.hknet.cz
Jmenný server	ns2.hknet.cz
Jmenný server	nsa.ces.net
Technický kontakt	JA11-RIPE Jindrich Andrs
Určený registrátor	REG-GENREG GENERAL REGISTRY, s.r.o. od 01.06.2009 10:39:10
Stav	Je navázán na další záznam v registru

Obr. 11vyhledaný záznam v registru domén nic.cz
Zdroj: snímek z www.nic.cz

Dalšími databázemi jsou například ARIN, RIPE či APNIC. Informace se dají také získat vyhledáváním pomocí Google vyhledávače a klíčového slova „site:", Google omezí vyhledávání na danou doménu. (Harris 2008 s. 89)

Často je také možné nalézt informace o konfiguraci síťových prvku na odborných fórech. Typické jsou dotazy ohledně nastavení firewall a dalších zařízení na diskusních fórech výrobců těchto zařízení. V některých případech dokonce správci, kteří si neví rady, zveřejňují konfigurační soubory zařízení, z těch je poté možno zjistit například IP adresy dalších zařízení v síti. (McClure, Scambray a Kurtz 2007 s. 35)

Opatření ad 2): Primárním opatřením je zveřejňovat jen minimální množství informací o SG síti. V současné době je zveřejněno obvykle více informací a to z důvodu technologické novinky ve fázi vývoje a testování. Tyto informace slouží pro výukové účely a informování odborné veřejnosti. Lze tedy předpokládat sníženou dostupnost informací o používaných technologiích a infrastruktuře SG sítě při jejím reálném použití. To, co může být hrozbou pro datovou síť, v podobě veřejně poskytnutých informací u správce domény, není prozatím rizikem v oblasti SG sítí. Pokud se správce sítě radí ohledně nastavení různých zařízení na odborných fórech, je vhodné nezveřejňovat své jméno ani žádné informace vedoucí ke společnosti, pro kterou pracuje. To, že nezveřejňuje konfigurační soubory zařízení, by mělo být samozřejmostí.

Dopad sběru informací v datové síti: Z předchozího textu je zřejmé, že sbírat informace o datové síti často není složité, obzvlášť pokud se jedná o prostředí internetu. Sběr informací má informativní účel, podstatné je, že ne vždy je cílem následný útok. Tato činnost nemá žádný dopad na provoz datové sítě.

Dopad sběru informací v Smart Grid síti: Shromažďování informací o infrastruktuře SG sítě nemá v praxi žádný reálný dopad. Většinou je tato činnost nezpozorována. Odborný personál, který má na starosti bezpečnost SG sítě, má jen malou šanci zjistit, že dochází k cílenému sběru informací třetí osobou. Jedním z důvodů je, že většinou je tato činnost prováděna zcela legálně z veřejně dostupných zdrojů. Není tedy ani důvod a většinou ani příliš mnoho metod jak tomu zabránit, kromě utajování informací.

6.5.2 Průzkum a skenování sítě (traceroute, ping, skenování portů)

Jedná se o fázi útoku, kdy útočník zjišťuje topologii cílové sítě, běžící služby či aktivní prvky.

1) Průzkum pomocí traceroute, je jedním ze základních průzkumů topologie sítě. Pomocí tohoto příkazu útočník může zjistit jména a adresy prvků v síti, přes kterou paket prochází. Často je tímto způsobem odhalen aplikační firewall nebo paketový filtr (McClure, Scambray a Kurtz 2007 s. 51). Unixové systémy používají při traceroute standardně UDP. Použití paketů ICMP lze zapnout pomocí parametrů příkazu. Tracert v MS Windows používá standardně ICMP. V systémech Windows je syntaxe příkazu tracert. V unixových systémech lze nastavit i číslo portu UDP. Další možností může být použití sofistikovaného nástroje pro průzkum sítě pomocí TCP namísto UDP. V sítích Smart Grid je použití tohoto příkazu identické, velkým rozdílem však je, že žádná vstupní, respektive výstupní brána Smart Grid sítě obvykle není z prostředí internetu nijak dostupná.

Opatření ad 1): Primární ochranou v SG síti je alespoň navenek neexistující propojení mezi SG sítí a internetem. Pokud celá SG síť nemá vlastní infrastrukturu a využívá internetové spojení například pro přenos dat do řídícího centra, je nezbytné, aby data byla přenášena v šifrovaném tunelu. Pokud se nějakým způsobem útočník dostal na rozhraní SG sítě, nastupuje stejná obrana jako v datové síti, viz následující odstavec.

Průzkum sítě dokáže detekovat většina systému pro detekci průniku do sítě (NIDS - Network Intrusion Detection System) a systémy pro prevenci průniku (IPS - Intrusion Prevention System). Obrana proti traceroute může být realizována nasazením speciálního softwaru, např. RotoRouter. Ten zaznamenává všechny příchozí požadavky od traceroute a odpovídá na ně smyšlenými údaji. Vhodným řešením je také na hraničních směrovačích zahazovat veškerý provoz ICMP a UDP. Je tedy vhodné použít ACL. (McClure, Scambray a Kurtz 2007 s. 53)

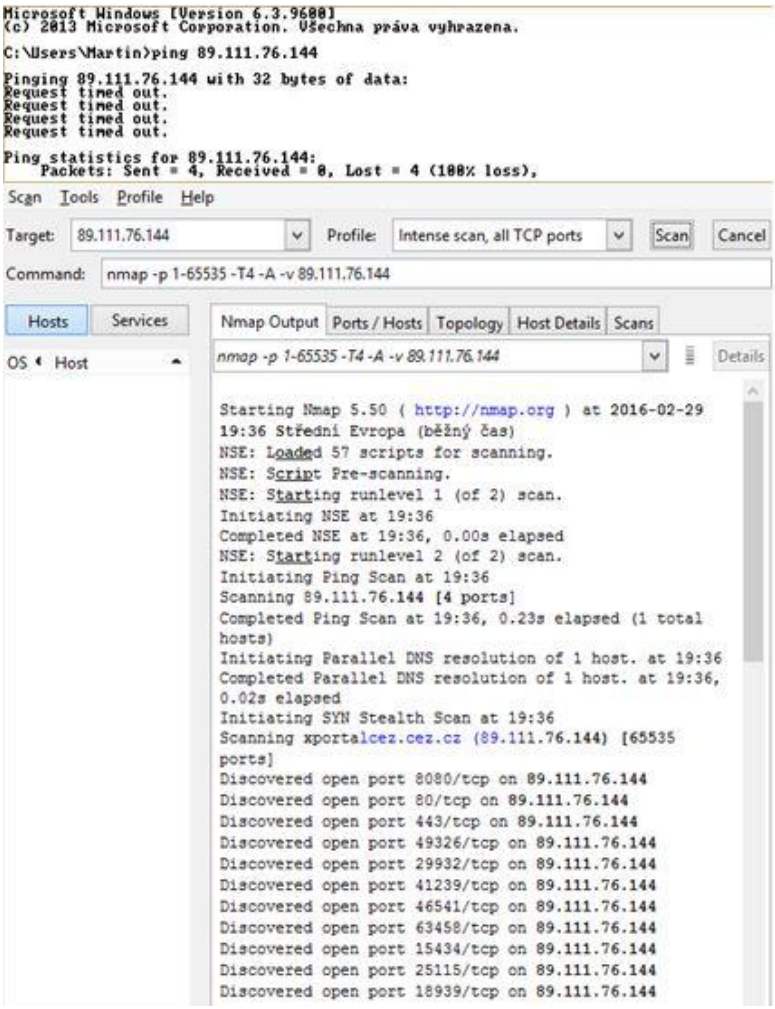
2) Hromadný ping je velmi jednoduchý a základní způsob jak v síti nalézt aktivní prvky. Tento způsob je však funkční a relativně rychlý. Ping je založen na protokolu ICMP echo, nejčastějšími zprávami jsou echo request a echo reply. Příkaz je možné používat z příkazového řádku z unixových systémů i

z MS Windows, zkušení uživatelé a útočníci používají však specializovaný SW umožňující podrobnější volby a scan založený jak na TCP i UDP. Dále tyto programy umožňují hromadné pingování ze zadaného rozsahu adres či určit port pro cílovou stanici. Těchto programů existuje celá řada, známým příkladem je Nmap, fping, SuperScan, PingSweep a další. Ukázka možného rozdílu v použití příkazového řádku či specializovaného nástroje je na obrázku 12.

Opatření ad 2): Obrana proti hromadnému pingu je obdobná s opatřením proti traceroute. I přestože v oblasti SG sítí stále platí, že by útočník vůbec neměl získat konektivitu do sítě, je nutné s takovým útokem počítat a být na něj připraven.

Opět zde platí použití IPS a NIDS a využití tvorby logů na všech zařízeních, které jsou významnými uzly v síti nebo uchovávají důležitá data. K tomu je však zapotřebí i odborný personál, který logy pravidelně vyhodnocuje a je schopný rozpoznat fázi předcházející útoku. Logování je vhodné pro monitoring provozu sítě obecně, bez logování a monitoringu nemusí firma ani poznat, že se stala terčem úspěšného útoku. (Flick a Morehouse 2011 s. 158, 159)

Zahazovat ICMP pakety je velmi dobrý krok pro prevenci. Nemusí však být dostatečný, viz obrázek 12, na kterém je znázorněno úspěšné ověření aktivního prvku, který se předtím zdál být neaktivní. V projektu Smart Grid Vrchlabí jsou data ze SG sítě přenášena do řídícího centra v HK šifrovaným tunelem, toto spojení zajišťuje společnost ČEZ ICT Services, a. s.. Tato společnost patří do skupiny ČEZ. IP adresa společnosti ČEZ v internetu je 89.111.76.144, pokud si ji zkusíme otestovat standardním (ICMP echo) příkazem ping, zjistíme, že se nevrátila odpověď ani na jeden z vyslaných paketů. Systém s touto adresou se jeví jako neaktivní. Při použití programu Nmap a intenzivním TCP skenu je zřetelné, že systém je aktivní, dále je možné zjistit například otevřené porty. Tento prvek zprávy ICMP echo nejspíš zahazuje.



Obr. 12 Porovnání ping a TCP skenu s použitím Nmap
Zdroj: vlastní tvorba

3) Skenování portů je velmi oblíbená technika pro zjištění otevřených portů a běžících služeb na cílovém prvku v síti. Útočník se připojuje na různé TCP a UDP porty oběti a zjišťuje, na kterých z nich naslouchají síťové služby. Právě síťové služby představují potenciální cestu dovnitř systému, pokud je služba špatně nastavená nebo obsahuje chybu, útočník ji může využít k získání vzdáleného přístupu. Existují různé druhy skenů, například sken úplného TCP spojení, TCP SYN sken, TCP FIN sken, Null TCP sken a další. Popis těchto skenů není účelem této práce. Skeny se zkrátka liší v záhlaví TCP segmentů. Existují i UDP skeny. Pro skenování TCP a UDP portů a hledání služeb existuje opět celá řada aplikací, mezi oblíbené patří Nmap, Strobe, Netcat či SuperScan. (McClure, Scambray a Kurtz 2007 s. 65)

Ukázka výpisu portů po intenzivním skenu TCP portů je v spodní části obrázku 12.

Opatření ad 3): Základní techniky obrany jsou identické s opatřením jedna a dva. Je vhodné správně odladit nastavení firewallu proti skenování portů. Většina moderních firewallů port sken pozná (McClure, Scambray a Kurtz 2007 s. 76). V neposlední řadě je nutné vypnout všechny nepotřebné porty.

Dopad průzkumu v datové síti: Průzkum sítě prováděný třetí osobou je zřetelným symbolem zvýšeného zájmu takové osoby o strukturu, adresy či prvky v síti. Průzkum sítě je již možné zpozorovat dle datového provozu v síti a událostí zaznamenaných do logů. Ani zde však nemusí jít vždy o předzvěst nějakého útoku na síť. I když takováto aktivita je již na síti méně obvyklá. Pokud průzkum není prováděn příliš agresivním a invazivním způsobem, pak nemá reálný dopad na funkčnost sítě.

Dopad průzkumu v Smart Grid síti: Na rozdíl od datové sítě zde žádný uživatel, který není součástí personálu pro správu SG sítě konkrétní společnosti nemá co dělat. Proto by takovému průzkumu měla být věnována patřičná pozornost. Jelikož je tento průzkum založen pouze na dotazování se prvků v síti a zjišťování běžících služeb a otevřených portů, nemá žádný negativní dopad na provoz v síti. Výjimku by mohly tvořit spoje s nízkou datovou propustností. U takových spojů by se mohla snížit přenosová rychlost a zvýšit latence spojení.

6.5.3 MAC address flooding attack

Tento typ útoku, dobře známý z datových sítí, je aktuální i pro SG sítě. Na obrázku 8 je vidět schéma používaných protokolů pro SG sítě. Základní vrstvu sítí řízení, ochrany, datové i servisní tvoří protokol ethernet. Přepínače pracující s tímto protokolem jsou tedy vystaveny útoku v SG síti stejným způsobem jako v síti datové.

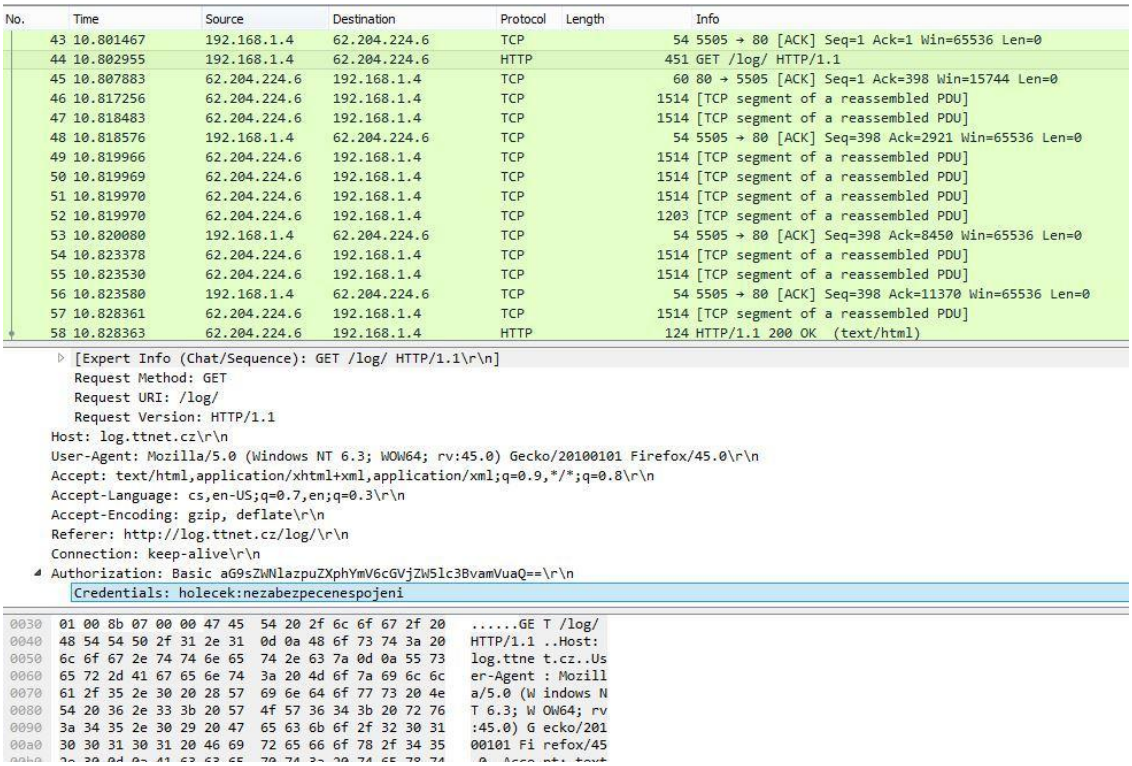
Při typickém útoku tohoto typu je switch zaplaven velkým množstvím fiktivních MAC adres. Podstata útoku je založena na přeplnění paměti přepínače těmito adresami. Standardně jsou tyto MAC adresy uchovávány v tabulce a přiřazeny k portům přepínače. Pokud je paměť přeplněna začne switch rozesílat přijaté datové rámce na všechny ostatní porty, chová se tedy jako hub. Tento stav

se nazývá „failopen state". Útočník může následně s použitím softwaru pro odchytávání paketů v promiskuitním módu získávat citlivá data. To umožňuje další útoky typu man-in-the-middle. (CiscoZine 2009)

Dopad útoku v datové síti: Útok je využíván k získání datového provozu, který není určen útočníkovi. Typickým dopadem v datové síti je tedy odchytávání paketů cizího spojení. V případě, že toto spojení není šifrované je možné ho bez problému odposlouchávat. Útočník například může zjistit přihlašovací jméno a heslo. Na obrázku 13 je vidět analýza zachycených paketů pomocí paketového analyzátoru Wireshark. Jak je vidět stačí sledovat komunikaci, následně vybrat správný paket, který obsahuje požadované údaje a ty si zobrazit. Tento příklad jsem vytvořil pro ilustraci nebezpečí nešifrovaného spojení. Použil jsem k tomu starší verzi webu mého ISP, přihlašovací jméno je: holecek, heslo jsem nastavil před pokusem na řetězec: nezabezpecenespojeni.

Proto je v dnešní době nanejvýš vhodné používat vždy zabezpečený šifrovaný přenos přihlašovacích dat. Dále je možné shromažďovat data, která jsou přenášena po síti. Útočník jednoduše sleduje komunikaci vybrané oběti. Dalším dopadem je zatěžování sítě, protože switch posílá provoz na všechny porty mimo příchozí.

Dopad útoku v Smart Grid síti: Dopad útoku v SG síti je obdobný jako v datové síti, důležité je však zmínit podstatu přenášených dat. Zde se jedná především o data o spotřebě odběratelů, stavech nejrůznějších prvků v distribuční soustavě nebo elektráren a kogeneračních jednotek. Společnost ČEZ je zodpovědná za ochranu nejen osobních ale i citlivých údajů. Dle zákona jsou hodnoty o spotřebě v konkrétních časech citlivým údajem odběratele. Existuje také reálná možnost využití odposlechu těchto dat chytrými zloději a typování si objektů s téměř nulovou spotřebou v předchozích dnech. U takových objektů je předpoklad, že je nikdo neobývá, může se jednat o letní sídla, chaty ale i běžné rodinné domy.



Obr. 13 analýza loginu a hesla z odchyceného nešifrovaného spojení
Zdroj: vlastní tvorba

Opatření: Obrana proti tomuto útoku je stejná v datové i SG síti. Princip spočívá v zabezpečení portu přepínače.

Na zařízeních Cisco se tato funkce nazývá switchport port-security. Funkce je založená na známé MAC adrese zařízení připojeného k portu přepínače. Každý port může mít asociaci pro jednu až 132 ověřených MAC adres. Přepínač může celkem těchto adres uchovávat až 1024. Adresu zařízení je možné nakonfigurovat ve třech módech, staticky, dynamicky nebo v módu označovaném jako Sticky. V módu sticky je adresa načtena dynamicky, je však zapsána do konfiguračního souboru přepínače. Dále je možné zvolit reakci po porušení bezpečnostního pravidla, těmito reakcemi jsou módy protect, restrict a shutdown. Více informací je možno zjistit v dokumentaci k Cisco přepínačům. (CiscoZine 2009)

6.5.4 Útoky na dostupnost služeb (DoS útoky)

Útoky typu Denial of Service mají velmi jednoduchý cíl a princip, jsou určeny k vyřazení služby či síťové infrastruktury z provozu. Motivů pro to může být mnoho například jen testování si schopností hackera, konkurenční boj, či útok na státní správu.

Principem DoS útoku je vyčerpání prostředků. Tím je rozuměno:

- Vyčerpání přenosového pásma, místa na disku či výpočetního výkonu procesoru
- narušení směrovacích informací
- narušení stavových informací, např. nevyžádaný reset TCP spojení

Nejčastějším cílem jsou důležité servery velkých firem, pro takové firmy může být výpadek služeb kritický. (Petrovič a Koštěnec 2012 s 20, 21)

Takovými firmami mohou být bankovní či burzovní společnosti, ale i různí poskytovatelé cloudových služeb. Právě poskytovatele těchto služeb zaručují dostupnost služby a dat zákazníka.

Dříve útoky využívaly především chyby v implementaci TCP/IP. Takovými útoky byl například Ping of Death, Smurf nebo Fraggle. Tyto útoky byly aktivně používány až do doby, dokud nebyly chyby v implementaci masivně opraveny. (McClure, Scambray a Kurtz 2007 s. 387)

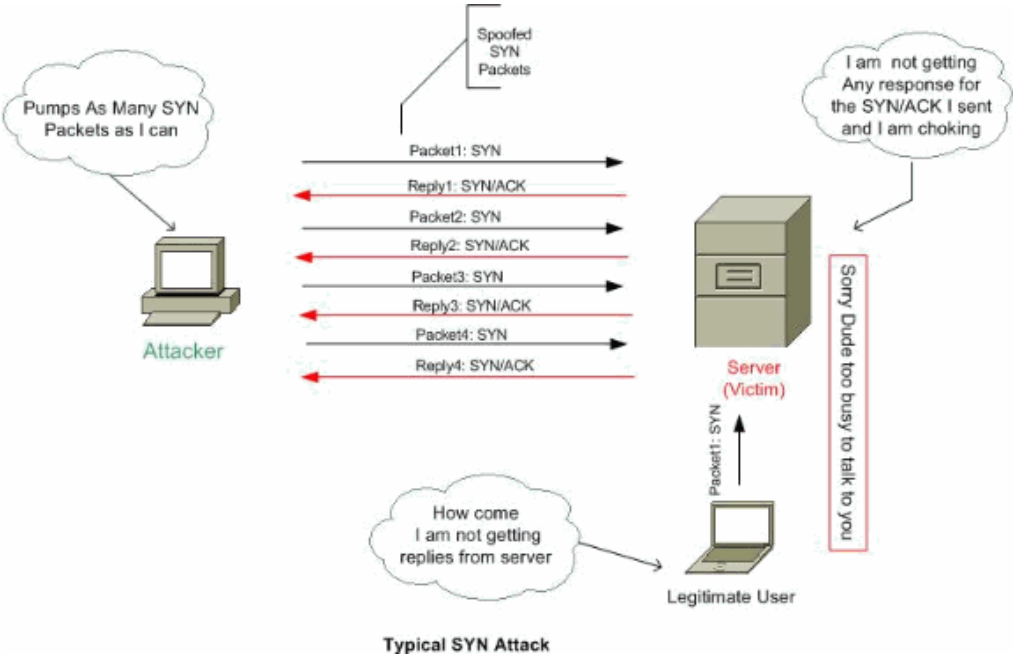
Například Ping of Death funguje následovně. Útočník odešle na cílovou adresu ICMP echo request zprávu s žádostí o odpověď, zpráva je však větší než povolená velikost 64 KB (65535 bajtů) U starších systémů toto způsobilo pád systému. Existuje také varianta, která posílala ICMP po částech ve velkých počtech, to zahltilo vstupní fronty pro skládání paketů. Výsledkem byl opět pád systému. (Petrovič a Koštěnec 2012 s. 21, 22)

Moderní variantou tohoto útoku je DDoS, tedy distribuovaný útok kterého se účastní větší množství počítačů. Velké množství počítačů dokáže zahltit prakticky jakoukoliv datovou linku. Útoky se soustřeďují nejčastěji na problematické zpracování paketů s příznakem SYN. Opravdu velikou hrozbu představují tzv. zombie sítě, tímto pojmem jsou označovány skupiny počítačů ovládaných útočníky. Tyto počítače jsou následně využívány k útokům DDoS bez vědomí uživatele. Dle autorů se v oblasti internetu nacházejí zombie sítě o velikosti až 140 tisíc počítačů. Je tedy jasné, že takové množství počítačů dokáže zahltit naprosto jakoukoliv linku či službu firmy. (McClure, Scambray a Kurtz 2007 s. 387, 388)

Dříve útočníci využívali především chyby v systému, ty již byly opraveny, je nepravděpodobné, že by tyto útoky zafungovaly v dnešní době. V současnosti jsou útoky DoS více přímočaré, jednoduše vyčerpají dostupné prostředky infrastruktury. Jedním z častých a oblíbených způsobů DoS útoku v současnosti je zaplavování SYN pakety. Tento typ útoku je ve zkratce popsán v následujícím odstavci a znázorněn na obrázku 14.

DoS útok typu záplava SYN pakety je založen na důvěryhodném prostředí IPv4 a navázání TCP spojení známého jako three-way handshake. Útočník pošle paket s příznakem SYN pro navázání spojení na cíl útoku, ovšem s podvrženou IP adresou. Cílový klient odpoví paketem SYN ACK pro navázání spojení na zdrojovou (podvrženou) adresu. Ta ovšem často vůbec neexistuje a cíl útoku se tedy poslední fáze navázání spojení paketem s příznakem ACK nedočká. Tím zůstává spojení napůl otevřené ve frontě. Doba čekání na dokončení spojení se pohybuje typicky kolem jedné minuty. Při dostatečné frekvenci je systém zahlcen těmito napůl otevřenými spojeními a znemožní komunikaci s regulérními uživateli. Důsledkem tedy bývá nefunkčnost TCP služeb (e-mail, přenos dat, www stránky atd.). (Cisco Systems 2008)

Dle McClure, Scambray a Kurtz se doba pro udržování otevřeného spojení pohybuje od 75 vteřin až do 23 minut. Navíc těchto napůl otevřených spojení dokáže většina systému obsluhovat jen několik málo desítek na rozdíl od tisíců navázaných spojení. (2007 s. 390)



Obr. 14 útok typu SYN flood, nedostupnost služeb legitimnímu uživateli
Zdroj: Cisco Systems 2008

V poslední době se však útočníci začali zajímat také o aplikační logiku a její zahlcení pomocí DDoS. Zahlcení aplikační logiky bývá mnohdy snazší než útok na síťovou infrastrukturu. Tyto útoky bývají zpravidla založeny na nepoměru výpočetní náročnosti mezi dotazem na službu, a odpovědí služby na dotaz. Následně je služba dotazována velkým množstvím dotazů, jestliže odpověď na dotaz je výpočetně mnohokrát náročnější, dojde po čase k zahlcení a složení služby. (McClure, Scambray a Kurtz 2007 s. 394)

Dopad útoku v datové síti: DoS útok je hlavním bezpečnostním rizikem, to především z důvodu poměrně snadného vedení útoku a jeho velkého dopadu. Dopad může být dočasný, nebo může vyžadovat zásah odborného personálu. Cílem útoku jsou infrastruktura a služby v síti. Důsledkem takového útoku je nedostupnost prostředků a služeb legitimním uživatelům. (OPPENHEIMER 2004 s. 75)

Typicky se jedná o obchodní sféru, u velkých firem či bankovních institucí může útok zapříčinit nemalé finanční ztráty. Kromě finančních ztrát útok může poškodit pověst firmy mezi jejími zákazníky a snižuje její důvěryhodnost.

Dopad útoku v Smart Grid síti: Úspěšný řízený DoS útok na SCADA sítě v průmyslovém sektoru by mohl znamenat naprostou katastrofu. (McClure, Scambray a Kurtz 2007 s. 388)

Dle (Flick a Morehouse 2011 s. 254, 255) jsou na DoS útok v SG síti náchylné především chytré elektroměry. To z důvodu jejich malého výpočetního výkonu, snadného zahlcení daty a následné neschopnosti monitorovat sledované údaje.

Například údaje o spotřebě nemohou být zaznamenány, protože na Smart Meter byl veden DoS útok. V takovém případě musí distributor elektřiny volit alternativní cestu k vyúčtování spotřeby odběratele. Například společnost ČEZ v takovém případě účtuje dle průměrné spotřeby za stejné období v předchozím roce.

Pokud je DoS útokem zahlcen prvek pro řízení (např. RTU pro spínání okruhu nn či vn) v SG síti, dispečink takový prvek nemůže vzdáleně ovládat a nedostává informace o el. síti. V tomto případě dispečerské stanoviště vysílá technický výjezd na místo pro fyzickou kontrolu zařízení. Důležité je si uvědomit, že prvek nemůže řídit ostatní prvky v síti, ale sám není útočníkem řízen. V kombinaci znepřístupnění informací o distribuční síti a fyzickém útoku na infrastrukturu se může jednat o velmi závažný útok.

Opatření proti DoS útokům: Opatření proti DoS útokům není nikdy jednotné a stoprocentní. Existuje však mnoho osvědčených a doporučených praktik jak rizika tohoto útoku minimalizovat tzv. best practice. Na úrovni komunikace TCP/IP je ve smart grid síti a datové síti obrana proti DoS útokům totožná.

Velmi vhodné je použití nějaké technologie pro obranu proti DoS a její zařazení do infrastruktury. Známý a osvědčený je Cisco Guard, Top Layer nebo směrovače značky Juniper. Všechny tyto technologie umí zcela zamezit či výrazně omezit běžné DoS útoky, jakými je například záplava SYN pakety. Při volbě vhodných technik je dobré vycházet z příruček výrobce síťového zařízení. V oblasti obraných technik je proslulý výrobce Cisco. Další osvědčený způsob tkví v kvalitním připojení k internetu, jedná se především o dostatečnou datovou propustnost připojovací linky. Opatření by měla být konzultována s ISP (poskytovatelem internetu) a jeho techniky. Je zbytečné mít naprosto dokonalé

opatření proti DoS, pokud se dříve zhroutí síť ISP. Je možné mít záložní připojení k internetu od dalšího poskytovatele, či vhodným způsobem s ohledem na hrozící DoS útok ISP vybírat. (McClure, Scambray a Kurtz 2007 s. 395, 396) V případě SG sítí tuto problematiku řeší infrastruktura sítě a její dostatečná optimalizace po stránce kapacity přenosů dat.

Mezi další obecné techniky obrany proti DoS útokům patří:

- Blokování ICMP a UDP, oba tyto protokoly nejsou při běžném provozu sítě potřeba. Zároveň oba tyto protokoly jsou často používány pro DoS útoky.
- Filtrování příchozího provozu, mnoho paketů se dá odfiltrovat ještě, než se dostanou do sítě. Jednat se může například o pakety s privátní IP adresou, takové pakety v internetu nemají vůbec co dělat.
- Vhodné je také filtrování odchozího provozu, toto slouží spíše k slušnému kodexu správce sítě. Kdyby filtroval odchozí provoz každý, k většině DoS útokům by ani nedošlo. Do internetu by ze sítě měly být puštěny pouze pakety z adres v naší síti. Tím se zabrání podvržení IP adres.
- Zakázat všesměrové vysílání, se dnes považuje za standard. Toto zabraňuje využití sítě jako zesilovač pro útok typu Smurf nebo Fraggle.
- Autentizace změn v směrovacích tabulkách, která zabrání přepsání těchto tabulek a směrování paketů jinam než je vhodné.
- V některých případech může být vhodné použití tzv. odpadního směrovače, na ten je vhodné směrovat odpadní data a nezatěžovat tak hlavní směrovač. Tento směrovač může sloužit pro další analýzu těchto dat.

Takovýchto opatření a doporučení existuje nespočet. Samozřejmostí je aktualizace všech systémů v síti, sledování zaznamenaných událostí v síti v logu a jeho vytváření. (McClure, Scambray a Kurtz 2007 s. 396, 397)

Velmi důležité pro bezpečnost SG sítí je možnost přepnout všechny prvky pro rozvod a řízení napětí všech úrovní do manuálního nastavení. Taková síť sice postrádá schopnost inteligence SG, ale je plně funkční. V takovém případě je možné prvky ovládat pouze fyzicky například v DTS. Toto řešení dává dostatek času pro vyřešení útoku a navrácení zpět k částečnému nebo plně automatickému řízení sítě.

6.5.5 IP spoofing

Ačkoliv se nejedná přímo o samostatný útok, je tato technika zahrnuta do mnoha dalších útoků. Například pro výše zmíněný DoS útok či pro prolomení zabezpečení založeném na konkrétních IP adresách (např. ACL).

Jak název útoku napovídá, jedná se o zfalšování IP adresy pro utajení útočníkovy adresy a překonání obrany založené na autentizaci IP adresy. Mezi služby náchylné k podvržení IP adres patří například NFS nebo SMB. (Petrovič a Koštěnec 2012 s. 21)

Pomocí podvržení IP adresy v paketu může útočník provádět útoky man-in-the-middle. V tomto typu útoku se může vydávat za jednu z věrohodných stran při probíhající komunikaci. Oběť tedy neví, že je vůči ní veden útok a komunikuje s útočníkem. Během takové komunikace může například poskytnout citlivá data nebo hesla. Útočník se také může vydávat za ověřeného uživatele dle IP adresy a měnit nastavení služeb v síti. (Tanase, 2003)

V případě TCP spojení je nutné ještě znát čísla navázaného spojení, sequence a acknowledgement numbers. Pokud je útočník ve stejné síti jako oběť, má to podstatně jednoduší, čísla navázaného spojení může odchytit během probíhající regulérní komunikace. V opačném případě je to velmi složité protože tyta čísla nejsou generována v moderních operačních systémech popořadě a je velmi těžké je odhadnout či spočítat. (Tanase, 2003)

Dopad útoku v datové síti: Tato technika může mít zásadní vliv na bezpečnost dat v síti. Útočník je schopen prolomit zabezpečení založené na důvěryhodnosti dle IP adresy. Tím může získat data na síti, či ovlivnit nastavení některých prvků. Dále umožňuje skrýt identitu DoS útoku, či působit DoS útoky typu Smurf či Fraggle.

Dopad útoku v Smart Grid síti: Dopady útoku v SG mohou mít kritické následky ve srovnání s datovou sítí. Pokud útočník někomu záměrně rozhodí konfiguraci, způsobí nefunkčnost např. webového či mailového serveru je to velmi nepříjemné a v mnoha případech tím způsobí finanční škody. Dopad takového útoku v SG síti je však katastrofální. Pro představu pomocí IP spoofing útoku a kombinací dalších útoků se útočník bude v síti identifikovat jako řídící stanoviště SG sítě. Následně pomocí RTU v rozpojovacích skříních vypne dodávku elektřiny například pro nemocnici. Ihned potom zahltí zařízení DoS útokem tak aby je opravdové řídící centrum nemohlo zapnout. V takovém případě bude možné zařízení zapnout až fyzicky po příjezdu techniků. Jelikož má nemocnice záložní zdroje a elektrocentrály, dá se předpokládat, že i tuto událost by zvládla, nicméně je to stále značná komplikace. Dalším případem může být vypnutí sítě semaforů, ve větším městě toto znamená dopravní kolaps. Scénářů je nepřeberné množství, ve většině případů mohou být následky kritické a někdy i životy ohrožující.

Opatření: Proti podvržení IP adres stejně jako proti většině útoků není stoprocentní obrana. Rizika se však dají minimalizovat správným nastavením zabezpečení. V první řadě je vhodná filtrace na hraničním routeru pomocí ACL, z vnější sítě nepřijímat pakety s privátní adresou. Naopak je vhodné do vnější sítě nesměrovat pakety, které mají jinou IP adresu než je v naší síti. Tím zabráníme, aby někdo v naší síti využil IP spoofing. Nejedná se sice o hrozbu, ale o morální kodex správce sítě. Dále je nutné využívat autentifikaci a šifrování přenosu dat a informací všude, kde je to možné. Například u routovacích a dalších protokolů pro provoz sítě.

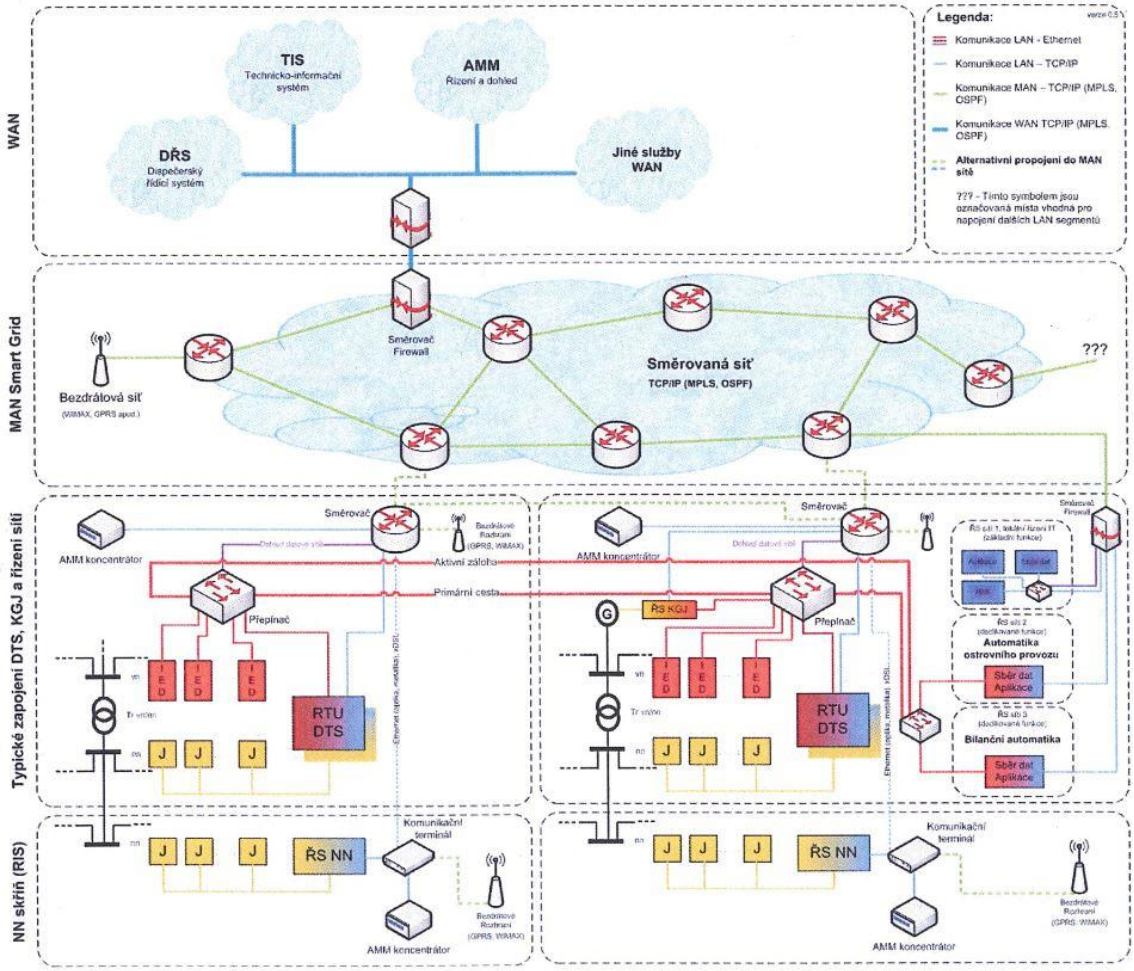
Zásadním zabezpečením proti tomuto útoku je technologie od společnosti Cisco. Jedná se o funkci nazvanou Reverse Path Forwarding. Funkce kontroluje zdrojovou IP adresu paketů a porovnává ji se směrovací tabulkou a zamítá pakety, které svoji adresou neodpovídají rozhraní.

7 Simulace DoS útoku v síťové laboratoři

Pro simulaci byl vybrán zástupce DoS útoku, který je relativně snadno proveditelný i pro nepříliš zkušeného útočníka v oblasti datových či SG sítí. Takový útok však zapříčiní nedostupnost služeb uživateli, tedy odběratelům elektrické energie, či řídícímu centru SG sítě. Proto je tento typ útoku tak nebezpečný.

Jedná se o útok UDP flooding, tedy záplava přenosové linky UDP pakety a vyčerpání přenosové kapacity linky. Útok je popsán v kapitole 6. 5. 4.

Testování bylo provedeno na topologii vycházející z obecné topologie pro SG síť společnosti ČEZ v projektu Vrchlabí. Ta je zobrazena na obrázku 15 a zároveň je součástí přílohy. V schématu je vidět velké množství redundantních prvků a linek. Proto bylo pro útok vybráno spojení v oblasti řízení sítí a to linka mezi směrovačem a komunikačním terminálem. Tento terminál má na starosti řízení sítí nízkého napětí a AMM koncentrátor, tedy sběr dat z chytrých elektroměrů. Tím je tedy vymezen dopad testovaného útoku.

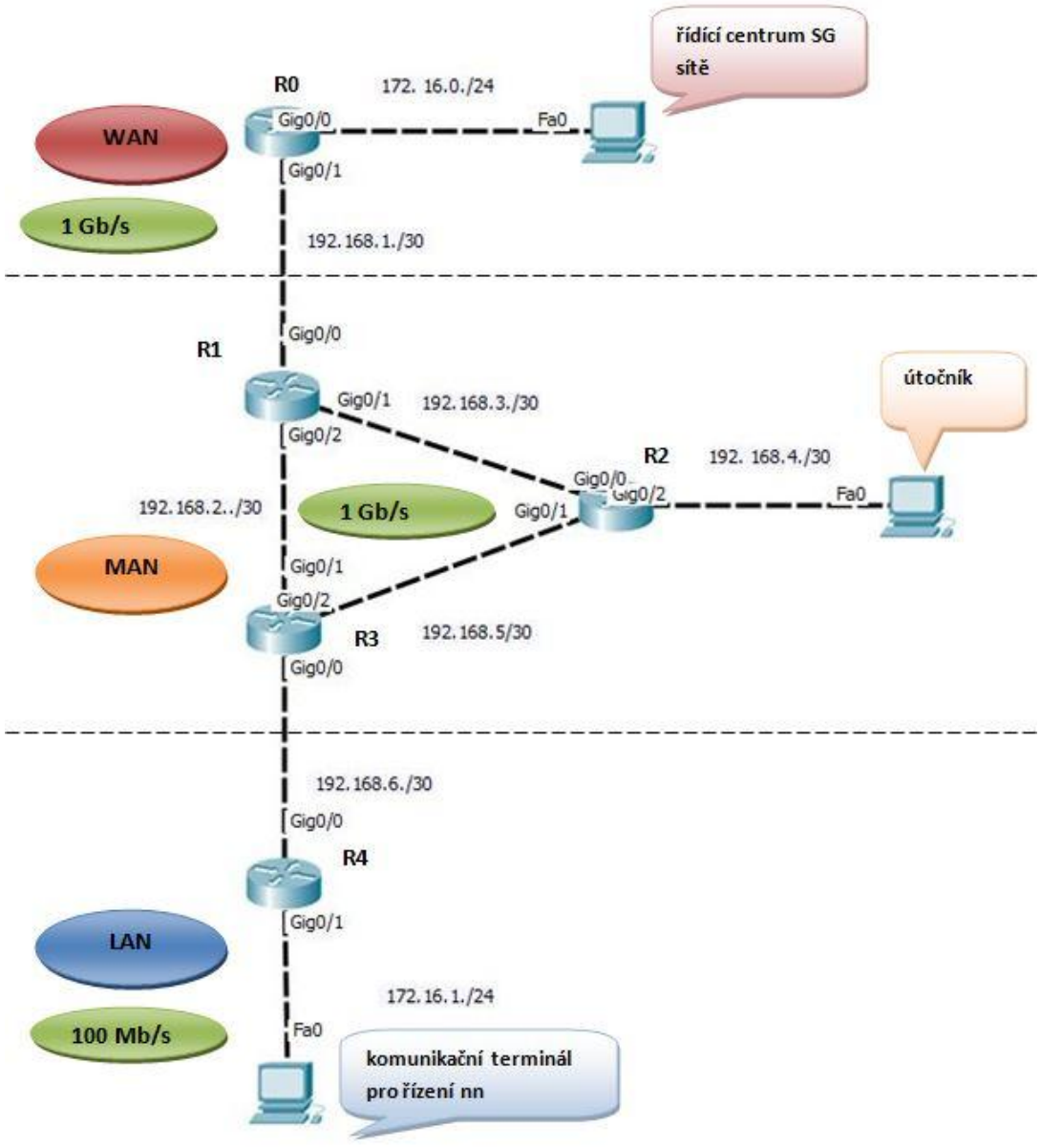


Obr. 15 Obecná topologie SG komunikační sítě
Zdroj: Finální architektura technického řešení Smart Region, 2011 s. 36

7.1 Topologie a nástroje pro testování

Zjednodušená topologie pro testování útoku obsahuje pouze spoje a prvky podstatné pro simulovaný útok. Dále jsou vyznačené adresné rozsahy, rychlosti linek jsou vždy 1Gb/s, pouze spojení na úrovni LAN, tedy mezi routerem R4 a komunikačním terminálem, má linka kapacitu 100 Mb/s. Tento fakt vychází z reality, kdy spoje v LAN segmentu mají výrazně nižší přenosové rychlosti než spoje v MAN a WAN. V praxi linky v LAN často kapacity 100 Mb/s ani nedosahují. Bohužel v současné době je testování přímo v Smart Grid síti nemožné. Proto je testování prováděno v síťové laboratoři UHK. Testovací topologie je na obrázku 16. Pro tuto úlohy byly použity routery Cisco řady 2911, dále počítače v roli řídícího centra SG sítě a komunikačního terminálu v SG síti.

Počítač je také využit jako prvek zprostředkující útočníkovi útok. Tabulka 5 obsahuje adresy zařízení. Konfigurační soubory sítě před provedením útoku jsou v příloze. Pro záplavu linky UDP pakety je využit generátor síťového provozu NetScan Tools Pro.



Obr. 16 Testovací topologie pro UDP flooding attack
Zdroj: vlastní tvorba

Název Zařízení	Rozhraní	IP adresa	Síťová maska	Výchozí brána
R0	Gi 0/0	172.16.0.1	255.255.255.0	XXX
	Gi 0/1	192.168.1.1	255.255.255.252	XXX
R1	Gi 0/0	192.168.1.2	255.255.255.252	XXX
	Gi 0/1	192.168.3.1	255.255.255.252	XXX
	Gi 0/2	192.168.2.1	255.255.255.252	XXX
R2	Gi 0/0	192.168.3.2	255.255.255.252	XXX
	Gi 0/1	192.168.5.1	255.255.255.252	XXX
	Gi 0/2	192.168.4.1	255.255.255.252	XXX
R3	Gi 0/0	192.168.6.1	255.255.255.252	XXX
	Gi 0/1	192.168.2.2	255.255.255.252	XXX
	Gi 0/2	192.168.5.2	255.255.255.252	XXX
R4	Gi 0/0	192.168.6.2	255.255.255.252	XXX
	Gi 0/1	172.16.1.1	255.255.255.0	XXX
Řídící centrum	Gig. ethernet	172.16.0.254	255.255.255.0	172.16.0.1
Útočník	Gig. ethernet	192.168.4.2	255.255.255.252	192.168.4.1
Komunikační terminál	Fast ethernet	172.16.1.254	255.255.255.0	172.16.1.1

Tabulka 5 Síťové adresy prvků topologie
Zdroj: vlastní tvorba

7.2 Provedení UDP flooding

Na obrázku 16 je vyznačeno, odkud je veden útok, umístění útočníka je systematické a představuje situaci proniknutí útočníka do infrastruktury SG sítě. Útočník může útočit schematicky z mnohem větší vzdálenosti, než sou 3 prvky, podstata vedení útoku se tím však nezmění.

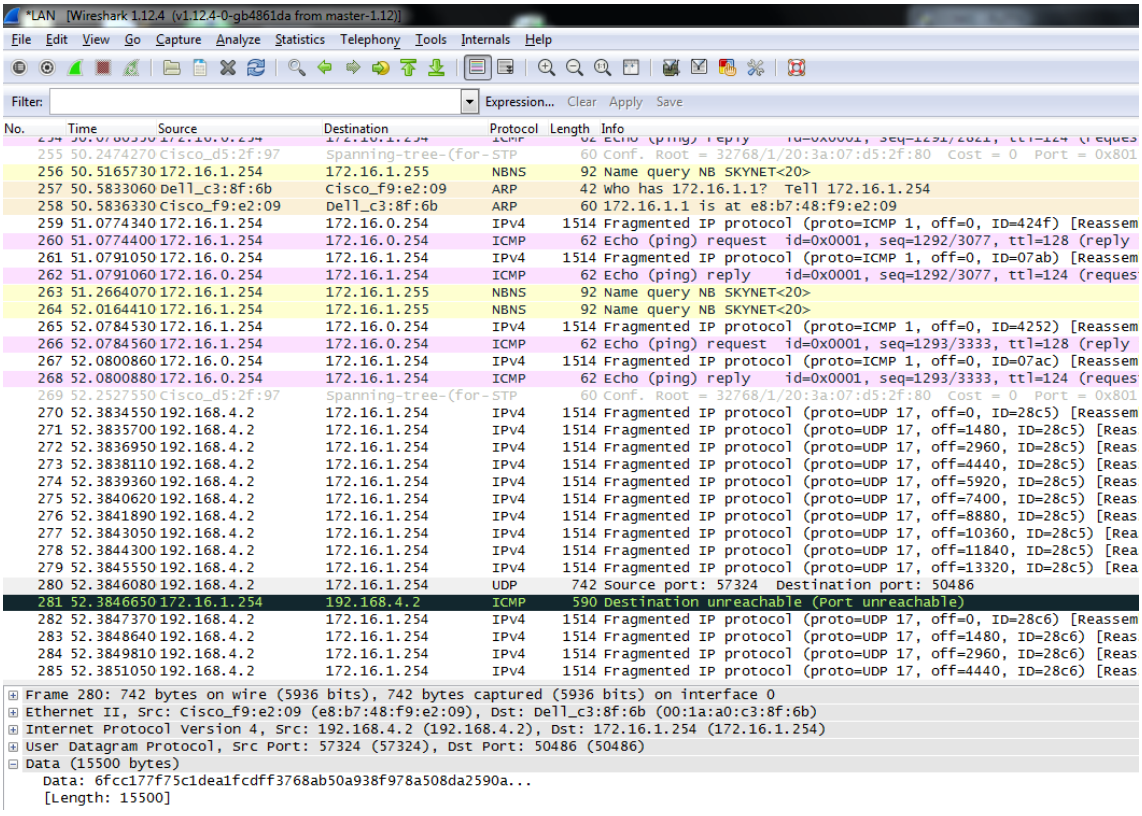
Pro útok typu vyčerpání kapacity přenosové linky je podstatná skutečnost útoku pocházejícího z oblasti MAN s cílem v LAN. V opačném případě by útok nebyl možný, neboť by útočník zahltil svoji linku, kterou je připojen, nikoliv cílovou.

Pro simulaci komunikace mezi komunikačním terminálem a řídícím centrem SG sítě bylo využito protokolu ICMP. Byly zasílány ICMP pakety o velikosti 1500 bajtů na IP adresu řídícího centra, pakety byly zasílány až do stopnutí příkazu. Pro zaznamenání odpovědi i s delší latencí, je nastavena doba čekání na 1000 ms. Pro toto nastavení je tedy využito následujícího příkazu.

```
ping -l 1500 -w 1000 -t 172.16.0.254
```

Během této komunikace útočník začal se záplavou UDP pakety na adresu komunikačního terminálu. Velikost paketu byla zvolena 15 500 bajtů. Maximální velikost paketu deklarovaná standardem IPv4 je 65 535 bajtů. Maximální MTU pro ethernetový rámec je však 1500 bajtů. To znamená, že dochází k fragmentaci UDP datagramu na více paketů. Fragmentace odesílaných UDP datagramů je vidět na obrázku 17. UDP datagramy jsou zaplněny náhodnými daty. Prodleva mezi pakety je nastavena na 100 µs. Při tomto nastavení dochází k zhruba 45% zatížení sítě MAN s přenosovou kapacitou 1Gb/s. Nastavení SW pro UDP flooding je vidět v příloze 2, stejně tak zatížení sítě.

Toto má za následek zahlcení linky v síti LAN, komunikace mezi terminálem a řídícím centrem okamžitě selhává, selhání komunikace a zahlcení pásma je vidět na obrázku 17. Výpis příkazu ping při útoku na straně terminálu je v příloze 2.



Obr. 17 Přerušení ICMP komunikace a fragmentace UDP datagramů
Zdroj: vlastní tvorba

Jestliže služba ICMP simuluje komunikaci například pro řízení sítě nízkého napětí mezi řídícím centrem a komunikačním terminálem, dopad útoku znamená přerušení takové komunikace. Komunikační terminál ztrácí spojení a stává se

neovladatelný. K takovému prvku musí být vyslán technický výjezd. V případě fyzického narušení některého z nedostupných prvků se o tom řídící centrum dozví až od výjezdu nebo telefonického kontaktu se zákazníkem.

7.3 Obrana proti UDP flooding

Velmi efektivní obrana proti tomuto typu útoku jsou správně nastavená ACL (access control list), tedy přístupové seznamy. Ty umožňují povolení či zakázání komunikace v síti založené na zdrojových či cílových adresách nebo portech. Dále umožňují stanovit pravidla založená na použitých protokolech a kombinacích všech těchto parametrů. V testovací topologii jsou použity routery Cisco řady 2911, proto je využito ACL tak, jak je umožňují tyto prvky. Pro zabezpečení je vybrán ACL rozšířený pojmenovaný. Existují také pouze standardní ACL, které nemají tolik možností voleb.

Útok je založen na velkém množství UDP paketů, proto obrana musí vycházet z této skutečnosti. Cílem je tedy zabránit šíření UDP paketů v síti. Protokol UDP není běžně v síti používán a potřebný, zvláště pokud se jedná o průmyslové sítě, kterou je i Smart Grid. Příkladem využití UDP v síti je často šíření multicastového vysílání, u kterého neprobíhá kontrola doručení dat. V praxi se může jednat například o streamování videa či audia, např. IP kamery.

Pro umístění ACL je nejvhodnější volit hraniční směrovače tak, aby oddělovali jednotlivé oblasti sítě. Zvolen je tedy Router R4, který dělí oblast LAN a MAN. Jednotlivé ACL se aplikují na konkrétní síťové rozhraní (interface) a definuje se směr kontrolovaných dat. Jelikož je cílem oddělit MAN od LAN, bude to rozhraní Gig. ethernet 0/0 a kontrolovány budou data směrem z MAN. Na tento router je tedy aplikován access control list následujícím způsobem.

Vytvoření nového rozšířeného ACL se jménem ANTIUDP:

```
R4(config)#ip access-list extended ANTIUDP
```

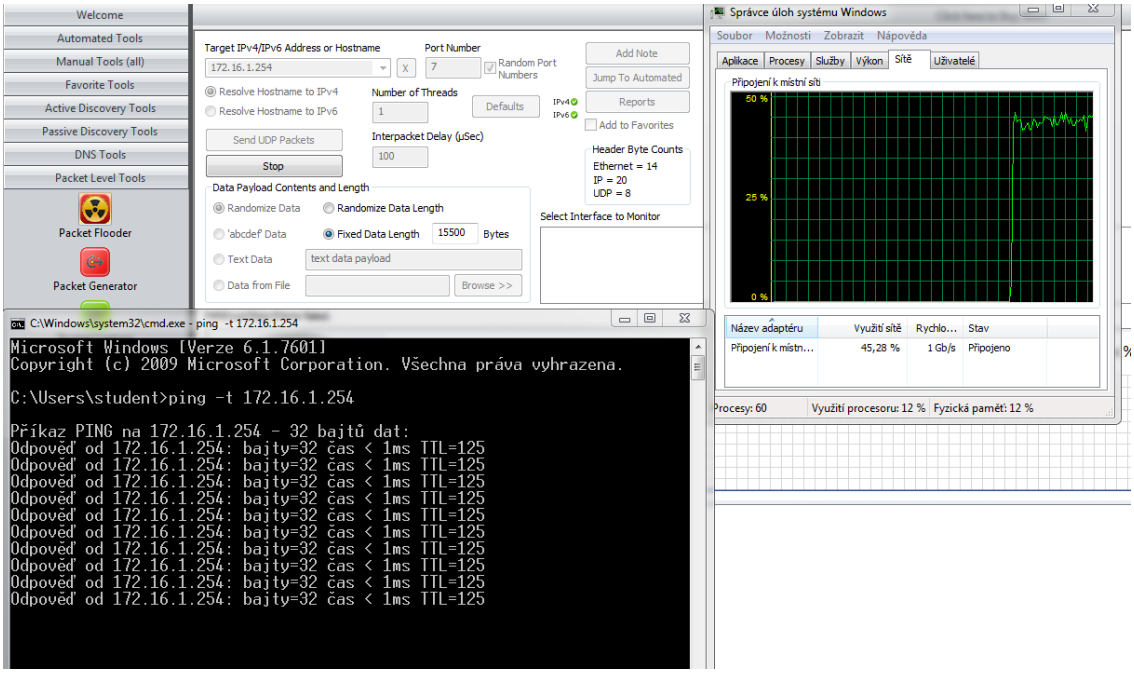
Konfigurace vytvořeného ACL, tak aby protokol UDP byl zahazován z jakékoliv sítě směřující do jakékoliv sítě. To je možné zadat pomocí klíčového slova *any* či adresou sítě a maskou ve wildcard tvaru.

```
R4(config-ext-nacl)#deny udp any any
```

Dále je nutné povolit služby a protokoly pro správný chod sítě a aplikací, které požadujeme v praxi, tedy aplikace používané pro vzdálenou správu prvků distribuční sítě a sběr dat z AMR. V tomto testovacím případě bude stačit povolit routovací protokol OSPF a protokol ICMP který slouží k ověření funkčnosti spojení.

```
R4(config-ext-nacl)#permit ospf any any
R4(config-ext-nacl)#permit icmp any any
```

Po této konfiguraci byl znovu spuštěn příkaz ping a proveden znovu stejným způsobem útok, linka mezi útočníkem a R2 byla opět vytížena kolem 43 - 46 %. Na lince ke komunikačnímu terminálu však žádné výrazné zatížení nebylo detekováno a nedošlo k přerušení komunikace mezi terminálem a řídícím centrem. Tato komunikace je zobrazena v příloze 2. Dalším důkazem stoprocentní funkčnosti opatření je ověřovací ICMP komunikace mezi útočníkem a komunikačním terminálem během útoku, viz obrázek 18.

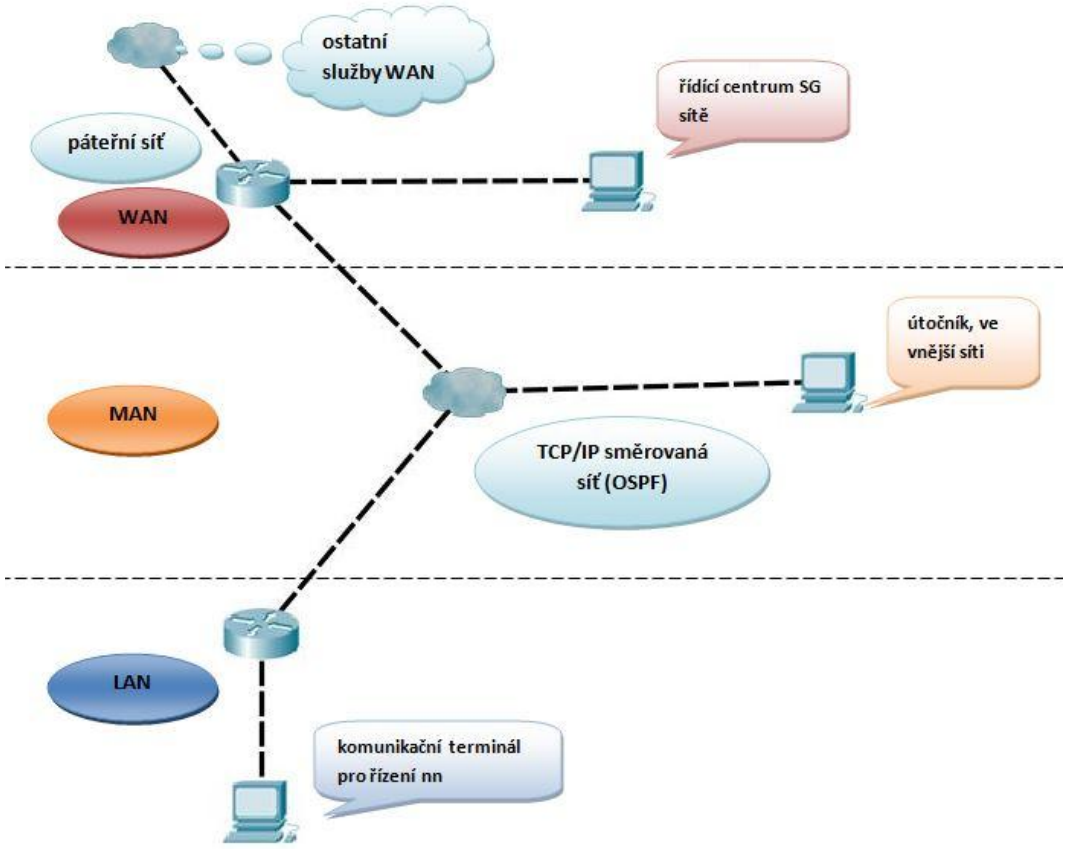


Obr. 18 Ověření funkčnosti opatření pomocí ICMP komunikace
Zdroj: vlastní tvorba

7.4 Topologie reálného útoku s využitím IP spoofing

Pro otestování útoku byl útočník přímo zařazen do síťové topologie. Aby bylo možné provést útok, musí útočník proniknout do síťové infrastruktury. Toho může být docíleno dvěma způsoby, prvním je možnost prolomení slabého zabezpečení přenosu dat skrze veřejnou síť, tedy internet. Druhou možností je fyzické napojení na komunikační infrastrukturu.

Pro reálný útok je pravděpodobnější varianta přístupu do sítě skrze vnější síť, tedy například skrze nedostatečně zabezpečené tunelové spojení. V takovém případě útočník využívá IP spoofing, tedy podvržení síťové adresy. To je nutnost neboť zařízení uvnitř topologie jsou nastaveny pro komunikaci pouze s adresami známými jako prvky SG sítě. Pakety přicházející směrem od útočníka se tedy tváří že pochází od některého z ověřených zařízení v Smart Grid síti. Zároveň tím útočník částečně skrývá svou identitu v síti. Logická topologie reálného útoku je znázorněna na obrázku 19.



Obr. 19Logická topologie reálného útoku
Zdroj: vlastní tvorba

8 Shrnutí výsledků

Ze zkoumání konceptu Smart Grid vyplývá jeho přínos především v oblasti snižování spotřeby elektrické energie a zvýšení podílu obnovitelných zdrojů. Smart Grid vzniká integrací komunikačních technologií a automatizací stávajícího energosystému. Dále přináší možnost ostrovního provozu elektrické sítě a vyšší spolehlivost dodávky elektřiny za běžných podmínek i v případě živelných katastrof. Z těchto důvodů se dá předpokládat zavádění SG sítí v budoucím období.

Současný stav SG sítí v Evropě vychází z podnětu, kterým je SET Plan (Strategic Energy Technology Plan). Ten definuje cíl snížit emise skleníkových plynů o 20% do roku 2020 oproti roku 1990. V evropských zemích vzniklo tedy velké množství testovacích projektů s mírně odlišnými cíli. Účelem všech projektů je však zavedení chytrých elektroměrů, komunikace v síti, automatizace rozvoden, snížení spotřeby či reakce na aktuální stav sítě. Ne všechny projekty však testují koncept elektromobility, chytrých domácností či ostrovního provozu. V České republice vznikl v roce 2010 pilotní projekt v mikroregionu Vrchlabí, veden společností ČEZ. Tento projekt je velmi klíčový pro další vývoj a nasazení SG sítí v ČR i EU. Celý region je pokryt rozpadovými stanicemi a dálkově spínanými rozvodnami. Nejvýznamnější oblastí je Liščí kopec, ten disponuje plnou automatizací všech rozvodných prvků včetně trafostanic a spínacích skříní nn. Dále jsou všechny domácnosti vybaveny chytrými měřidly. Oblast obsahuje vlastní kogenerační jednotku na zemní plyn, díky čemuž je umožněn ostrovní provoz nezávisle na vnější dodávce elektřiny. Tato jednotka současně produkuje i tepelnou energii, díky tomu je dosaženo využití zemního plynu s účinností 90%.

Nedílnou součástí SG sítí je komunikační infrastruktura, ta je klíčovou částí vrstveného modelu distribučního systému. Je rozdělena do síťových segmentů WAN, MAN a LAN. Těmto segmentům následně odpovídají i použité technologie pro komunikaci a přenos dat. LAN SG reprezentuje jednu oblast, přičemž MAN SG tyto oblasti propojuje a svým rozsahem odpovídá smart regionu například Vrchlabí. Jednotlivé MAN sítě se následně napojují na páteřní síť WAN. Společnost ČEZ využívá virtuální LAN sítě pro oddělení následujících sítí: řízení prvků, síť ochrany (rychlé zprávy GOOSE), datovou síť a servisní síť.

Díky logickému oddělení je možné používání různých komunikačních protokolů. Základem komunikace všech sítí je ethernetový rámec. Pro síť ochrany je následně využit protokol IEC 61850 GOOSE. Pro síť řízení je využívána v praxi nad ethernetem sada TCP/IP pro lepší bezpečnost komunikace, následně je použit IEC 60870-5-104 či IEC 60870-8-1. Datová a servisní síť využívají také TCP/IP a k nim související aplikační protokoly. Tyto skutečnosti o použitých protokolech se opírají o technické podklady studie společnosti ČEZ zhotovené přímo pro smart region Vrchlabí.

Z předchozího odstavce je tedy zřetelné použití rodiny protokolů TCP/IP a ethernet, které jsou široce aplikovány v datových sítích. Z toho vyplývá skutečnost hrozeb, které jsou známé z datových sítí a mohou být aplikovány v sítích Smart Grid. Existuje několik základních motivů pro útok na SG síť. Může se jednat o krádež dat, znepřístupnění služeb (DoS) či manipulaci služeb (ovládání prvků sítě). Z postupného výzkumu vyšlo najevo, že i způsob vedených útoků na SG síť je velmi podobný s prostředím datových sítí. V první fázi typicky útočník sbírá data, objevuje síť a její topologii, následně identifikuje místa k průniku do sítě a nakonec je veden samotný útok. Takový průnik zabezpečením s následnou krádeží dat v síti je definován v kapitole 6. 3. 4.

Zásadním rozdílem je dopad útoku na datovou a SG síť. Právě v červenci roku 2010 bylo změněno chápání útoku na SCADA systémy, jakým je i síť Smart Grid. Tato změna chápání vychází z útoku na výkonné zařízení v jaderné elektrárně v Íránu, jedná se tedy o přímé ohrožení lidských životů, nikoliv jen majetkových zdrojů. Dopad útoku na SG sítě je nesrovnatelně vyšší v porovnání s dopadem v datových sítích. Tomuto porovnání se věnuje kapitola 6. 5. . V práci jsou naznačeny možnosti přístupu k informacím, které mohou být nebezpečné. Tím mohou být zveřejněné informace na webu společností či sociálních sítích. Dále je popsáno, jakým způsobem dochází k získávání informací útočníkem a průzkumu sítě nejrůznějšími nástroji a metodami. Následně jsou již popsány konkrétní útoky jako je MAC address flooding, či DoS útoky a IP spoofing. Je popsána situace útoku MITM, odchycení paketu na nešifrovaném spojení a analýza paketového provozu s následným zjištěním přihlašovacích údajů. Pro všechny útoky je analyzován dopad v SG síti a porovnán s dopadem v datové síti.

Následně bylo navrženo opatření proti každému útoku založené na reálných zkušenostech z datových sítí. Dopady útoků v SG síti byly konzultovány s Ing. Novotným ze společnosti ČEZ, který se zabývá výhradně novými technologiemi, především konceptem Smart Grid a jeho testováním ve Vrchlabí.

Poslední částí práce je samotný útok provedený v síťové laboratoři UHK. To z důvodu, že v současné době nebylo možné testovat přímo reálnou síť SG. Síť tedy byla nakonfigurována podle vzoru obecné topologie SG sítě. Jako routovací protokol byl použit OSPF, který je využíván v projektu Vrchlabí. Pro tuto úlohu jsem vybral velmi častý útok z datových sítí, který je nebezpečný především svojí rozšířeností a nižší náročností. Útok zvládne podniknout i méně zkušený hacker. Jedná se o DoS útok typu UDP flooding. Na sestavené a nakonfigurované topologii, viz. obrázek 16, je proveden útok na komunikační terminál pro řízení sítí nn. Tento terminál je připojen linkou 100 Mb/s, ta je během útoku zcela zaplavena UDP pakety. Tím dochází k přerušení komunikace mezi terminálem pro řízení a řídícím centrem. Tato komunikace byla simulována provozem ICMP. Následně je provedeno testování navrženého opatření, které spočívá v nastavení správných ACL (access control list) na hraničním routeru mezi LAN a MAN oblastmi. Po provedeném opatření útok již neměl žádný vliv na simulovanou komunikaci. Z toho vyplývá, že na útoky využívajících principů datových sítí je možné aplikovat obranu založenou rovněž na těchto principech.

9 Závěry a doporučení

Výsledkem práce je analýza bezpečnostních hrozeb SG sítí pocházejících z oblasti datových sítí. Toto je způsobeno použitím protokolu ethernet a sady protokolů TCP/IP v oblasti SG sítí. V práci jsou definovány jednotlivé typy útoku dle provedení a podle motivu útočníka. Byl analyzován a porovnán dopad jednotlivých typů útoků v datové a SG síti. Dopad útoků na Smart Grid byl konzultován s Ing. Novotným ze společnosti ČEZ zabývajícím se konceptem SG a projektem Smart Region Vrchlabí. Dále jsou navržena opatření proti popsaným skupinám útoků. Následně je vybrán DoS útok UDP flooding, který je otestován v síťové laboratoři. Proti tomuto útoku je otestováno navržené opatření, které prokázalo svoji bezchybnou účinnost.

Jelikož pohled na koncept Smart Grid není plně ucelen, je součástí práce také definice konceptu, popis jeho funkčnosti a struktury. Dále je nedílnou součástí práce popis komunikační infrastruktury, ten už vychází z faktů testovaných v projektu Vrchlabí. Následné testování útoku reflektuje právě infrastrukturu tohoto projektu.

Byly ověřeny předpoklady, že je možné uplatnit útoky známé z datových sítí v prostředí Smart Grid. Stejně tak obrany proti nim. Na tomto se shoduje většina literatury zabývající se problematikou bezpečnosti Smart Grid. Toto vychází ze zkoumané analýzy provedení útoků a jejich dopadu. Bohužel testování útoku a obrany proti němu nebylo možné provádět přímo v SG síti.

Pro další zkoumání by bylo velmi vhodné toto testování provést přímo v prostředí fungující SG sítě při plně automatizovaném elektrorozvodném systému. Dalším směrem zkoumání by mohly být reálné dopady pro úspěšné útoky v různých prostředích. Svým způsobem by se jednalo o bezpečnostní studie pro obranu státu. Například vymezení dopadů při vyřazení světelných křižovatek ve větších městech. Dále rizika útoku a jeho dopadu na elektrárny a rozvodny.

10 Seznam použité literatury

ADDRESS Project 2008 - FP7 ENERGY. *ADDRESS Project - FP7 ENERGY* [online]. ADDRESS, 2008 [cit. 2016-02-08]. Dostupné z: http://www.addressfp7.org/index.html?topic=config/testsites_Spain

ADDRESS Project 2008 - FP7 ENERGY. *ADDRESS Project - FP7 ENERGY* [online]. ADDRESS, 2008 [cit. 2016-02-08]. Dostupné z: http://www.addressfp7.org/index.html?topic=config/testsites_France

Begovic, 2013 Miroslav M. *Electrical transmission systems and smart grids: selected entries from the Encyclopedia of sustainability science and technology*. 1. vydání. New York: Springer, 2013, vi, 324 pages. ISBN 14-614-5829-3.

BORLASE, 2012, Stuart. *Smart grids: infrastructure, technology, and solutions*. First edition. Boca Raton, FL: Taylor, 2012, xviii, 577 p. ISBN 978-143-9829-059.

CCNA Security. 2015 *Cisco Networking Academy* [online s podmíněným přístupem]. Cisco company, 2015 [cit. 2016-02-12]. Dostupné z: www.netacad.com

Cisco Systems. 2008 ASA/PIX 7.x and Later: Mitigating the Network Attacks. *Cisco Systems* [online]. San Jose, USA: Cisco Systems, 2008 [cit. 2016-03-10]. Dostupné z: http://www.cisco.com/c/en/us/support/docs/security/asa-5500-x-series-next-generation-firewalls/100830-asa-pix-netattacks.html

CiscoZine, 2009, Protecting against MAC flooding attack. *CiscoZine: Daily Reporting On Cisco Technology* [online]. CiscoZine, 2009 [cit. 2016-03-02]. Dostupné z: http://www.ciscozine.com/protecting-against-mac-flooding-attack/

CZ.NIC 2016 - O DNSSEC. *CZ.NIC* [online]. Praha: CZ.NIC, 2016 [cit. 2016-02-24]. Dostupné z: http://www.dnssec.cz/

ČEPS, a.s. 2015 - Technická infrastruktura. *ČEPS, a.s.* [online]. Praha: ČEPS, a.s., 2015, 2015 [cit. 2015-12-31]. Dostupné z: https://www.ceps.cz/CZE/Cinnosti/Technicka-infrastruktura/Stranky/Default.aspx

ČEZ, a. s. 2003 *Elektřina* [online]. ČR: 2003, 2003 [cit. 2015-12-28]. Dostupné z: http://www.cez.cz/edee/content/microsites/elektrina/elektr.htm

DOČKAL, Jaroslav. *Bezpečnostní management podnikové sítě*. Brno: Vysoká škola Karla Engliše, 2012.

Elektrické sítě OTE, a.s. 2014 *OTE, a.s.* [online]. Praha: OTE, a.s., 2014, 2015-03-18 [cit. 2016-01-02]. Dostupné z: http://www.ote-cr.cz/statistika/dlouhodoba-rovnovaha/elektricke-site/elektricke-site

Evropský kontext: EEGI, SET Plan. *Skupina ČEZ* 2015 [online]. Praha: ČEZ, a. s., 2015, 2015-12-30 [cit. 2016-01-06]. Dostupné z: http://www.cez.cz/cs/vyzkum-a-vzdelavani/vyzkum-a-vyvoj/subjekty-v-oblasti-vyzkumu-a-vyvoje/eu-verejne-zdroje-financovani/smart-grids/evropsky-kontext.html

FALK, Rainer a Steffen FRIES. 2011 Smart Grid Cyber Security – An Overview of Selected Scenarios and Their Security Implications. *PIK - Praxis der Informationsverarbeitung und Kommunikation* [online]. 2011, **34**(4), - [cit. 2016-02-15]. DOI: 10.1515/piko.2011.037. ISSN 1865-8342. Dostupné z: http://www.degruyter.com/view/j/piko.2011.34.issue-4/piko.2011.037/piko.2011.037.xml

Finální architektura technického řešení Smart Region, 2011 Draft 6. Praha: ABB s.r.o., 2011.

FLICK, Tony a Justin MOREHOUSE. 2011 *Securing the smart grid: next generation power grid security*. First edition. Boston: Syngress, 2011, xxv, 290 p. ISBN 15-974-9570-0.

FRANEK, 2012 Lešek. *DATA KONCENTRÁTOR PRO CHYTRÉ SÍTE*. BRNO, 2012. Diplomová práce. VUT Brno. Vedoucí práce Pavel Kučera.

GHARAVI, Hamid a Reza GHAFURIAN 2011 Smart Grid: The Electric Energy System of the Future. *Proceedings of the IEEE* [online]. 2011, **2011**(99), 917 - 921 [cit. 2016-03-04]. Dostupné z: https://www.ieee.org/documents/scanning0611.pdf

HADJSAÏD, 2012, Nouredine a Jean-Claude SABONNADIÈRE. *SmartGrids*. First edition. Hoboken, NJ: Wiley, 2012, xix, 358 p. ISBN 18-482-1261-5.
HARRIS, 2008 Shon. *Hacking: manuál hackera*. 1. vyd. Praha: Grada, 2008. ISBN 978-80-247-1346-5.

HO, 2014 Quang-Dung. *Wireless communications networks for the smart grid*. New York: Springer, 2014, pages 108. ISBN 978-331-9103-464.

HORÁLEK, Josef a Vladimír SOBĚSLAV, 2012. Technologie a požadavky na inteligentní sítě pro Smart Grid. *Elektro revue* [online]. 2012, 2012(6), 65-1 - 65-6 [cit. 2016-01-15]. ISSN 1213 - 1539. Dostupné z: https://www.google.cz/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&cad=rja&uact=8&ved=0ahUKEwigocHSzqvKAhUCPhQKHWAzCRsQFggfMAA&url=http%3A%2F%2Fwww.elektrorevue.cz%2Fcz%2Fdownload%2Ftechnologie-a-pozadavky-na-inteligentni-site-pro-smart-grid%2F&usg=AFQjCNEIhe4XmO12d-79JTxufUCztmHRHQ&sig2=xH7h1Na6zD2Mg05eiHwAjQ

HRADÍLEK, 2008 Zdeněk. *Elektroenergetika distribučních a průmyslových sítí*. 1. vyd. Ostrava: VŠB - Technická univerzita Ostrava, 2008, 208 s. ISBN 978-80-248-1696-8.

Info k SR Vrchlabí. *Skupina ČEZ* [online]. Praha: Skupina ČEZ [cit. 2016-01-22]. Dostupné z: http://www.cez.cz/cs/vyzkum-a-vzdelavani/vyzkum-a-vyvoj/subjekty-v-oblasti-vyzkumu-a-vyvoje/eu-verejne-zdroje-financovani/smart-grids/info-k-sr-vrchlabi.html

Inteligentní sítě vstupují do České Republiky. 2010 *ČEZ, a. s.* [online]. Praha: Skupina ČEZ, 2010, 28-4-2010 [cit. 2016-01-08]. Dostupné z: http://www.cezdistribuce.cz/cs/pro-media/tiskove-zpravy/153.html

KNAPP, Eric D a Raj SAMANI. 2013 *Applied cyber security and the smart grid: implementing security controls into the modern power infrastructure*. First edition. Amsterdam: Elsevier, Syngress, 2013, xxii, 202 pages. ISBN 978-159-7499-989.

KNAPP, Eric D. 2014 *Industrial network security: securing critical infrastructure networks for smart grid, scada, and other industrial control systems*. 2nd edition. Waltham, MA: Elsevier, 2014. ISBN 978-012-4201-149.

KUBÍN, 2006 Miroslav. *Přenosy elektrické energie ČR: v kontextu evropského vývoje*. Praha: ČEPS, 2006, 567 s.

MCCLURE, Stuart, Joel SCAMBRAY a George KURTZ, 2007 *Hacking bez záhad*. 1. vyd. Praha: Grada, 2007. ISBN 978-80-247-1502-5.

MeRegio - Aims of MeRegio. *MeRegio* [online]. Stuttgart: EnBW Vertrieb GmbH [cit. 2016-02-08]. Dostupné z: http://www.meregio.de/en/index.php?page=aim

NEUMAN, 2013 Petr. SMART/DIGITAL GRIDS - ZMĚNA ENERGETICKÉHO PARADIGMATU A JEJÍ PRAKTICKÁ APLIKACE V ES. In: *KONCEPT SMART GRIDS AND METERING*. 1. vydání. Praha: EGÚ Praha ENgineering, 2013, s. 1 - 20. ISBN 978-80-87774-06-9.

OPPENHEIMER, 2004 Priscilla. *Top-down network design*. 2nd ed. Indianapolis, IN: Cisco Press, 2004. ISBN 15-870-5152-4.

PETROVIČ, Michal a Michal KOSTĚNEC. 2012 *Bezpečnost počítačových sítí*. Plzeň: Západočeská univerzita v Plzni, 2012. ISBN 978-80-261-0117-8.

Smart Grids Renesas Electronics Europe: Efforts to Implement Smart Grids. *Renesas Electronics Europe* [online]. Tokyo Japan: Renesas Electronics Corporation [cit. 2016-01-09]. Dostupné z: http://www.renesas.eu/ecology/eco_society/smart_grid/

STEPHENS, 2015, Jennie, Elizabeth J WILSON a Tarla Rai PETERSON. *Smart grid (r)evolution: electric power struggles*. First edition. New York, NY, USA: Cambridge University Press, 2015, pages cm. ISBN 978-110-7635-296.

TANASE, 2003 Matthew. IP Spoofing: An Introduction. SYMANTEC CORPORATION. *Symantec Connect* [online]. Symantec Corporation, 2003 [cit. 2016-03-18]. Dostupné z: http://www.symantec.com/connect/articles/ip-spoofing-introduction

Virtuální prohlídka ČEZ - Smart Region Vrchlabí. *Skupina ČEZ* [online]. Praha: Skupina ČEZ [cit. 2016-01-22]. Dostupné z: http://virtualniprohlidky.cez.cz/cez-vrchlabi/

What is a smart meter? *Home Energy Supplier - Gas & Electricity Suppliers - E.ON* [online]. Coventry-England: E.ON Company [cit. 2016-01-08]. Dostupné z: https://www.eonenergy.com/for-your-home/smart-meters/what-is-a-smart-meter#

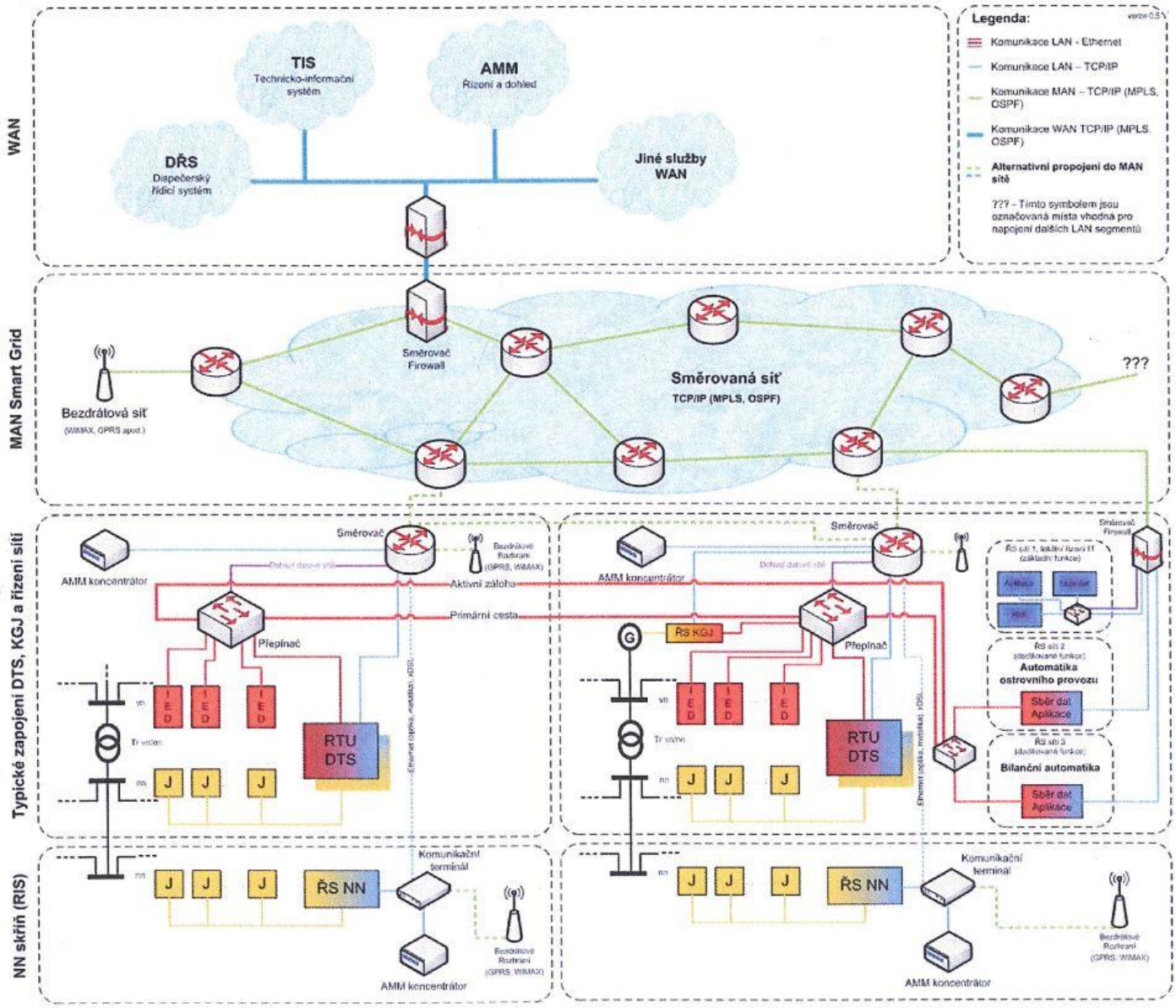
What is the Smart Grid: The Smart Grid. 2015 *SmartGrid.gov* [online]. Washington DC: U.S. Department of Energy, 2015 [cit. 2016-01-06].
Dostupné z: https://www.smartgrid.gov/the_smart_grid/smart_grid.html

Xiao 2012, Yang. *Communication and networking in smart grids*. First edition. Boca Raton, FL: CRC Press, 2012, xv, 309 p. ISBN 14-398-7873-0.

ZEMAN, 1966 Jan. *Elektrické sítě: Elektrická vedení*. 2. doplněné vydání. Praha: Československé energetické závody, 1966, s. 3 - 94.

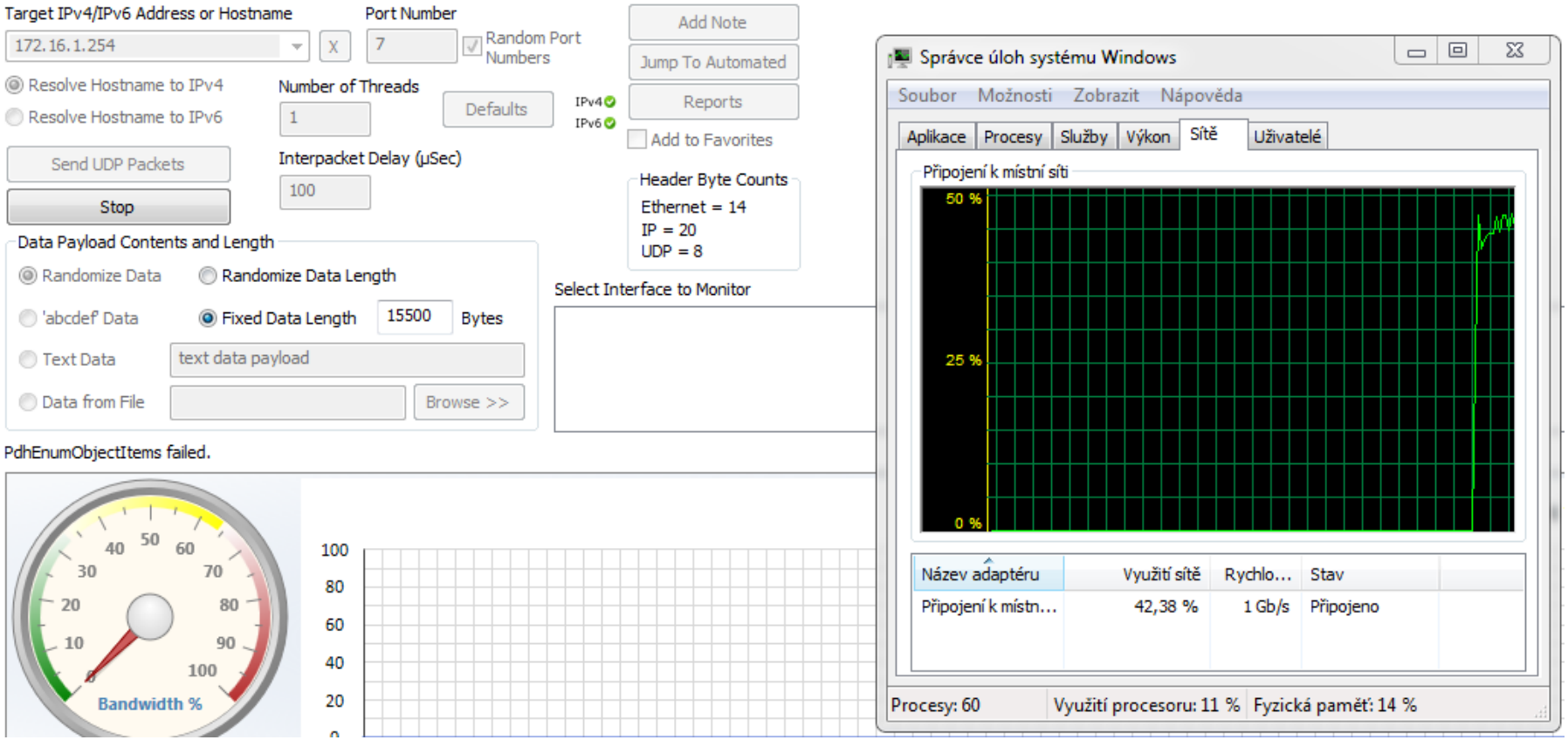
11 Přílohy

11.1 Příloha č. 1 obecná topologie komunikační sítě Smart Grid

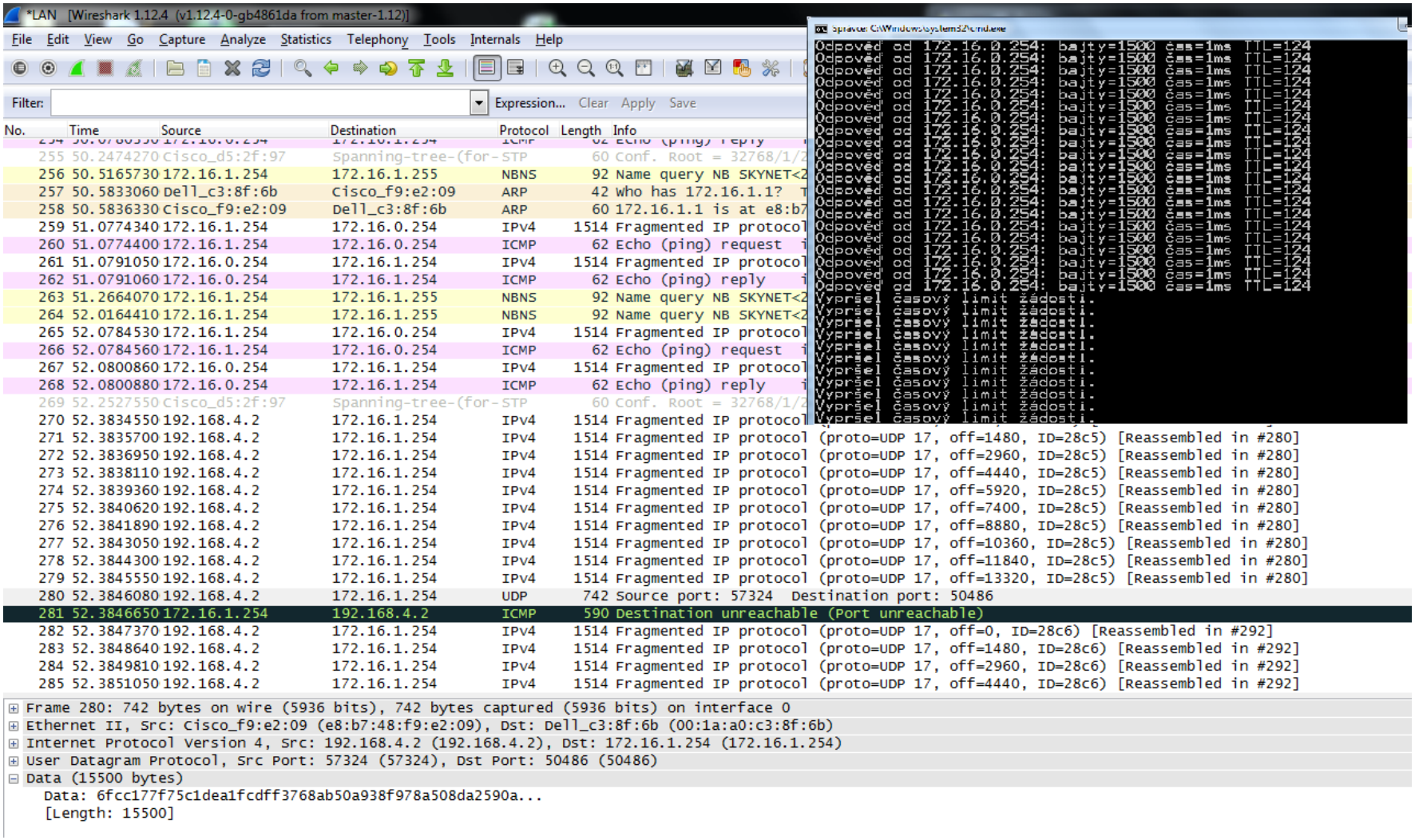


11.2 Příloha č. 2 dokumentace útoku v síti a vhodného opatření

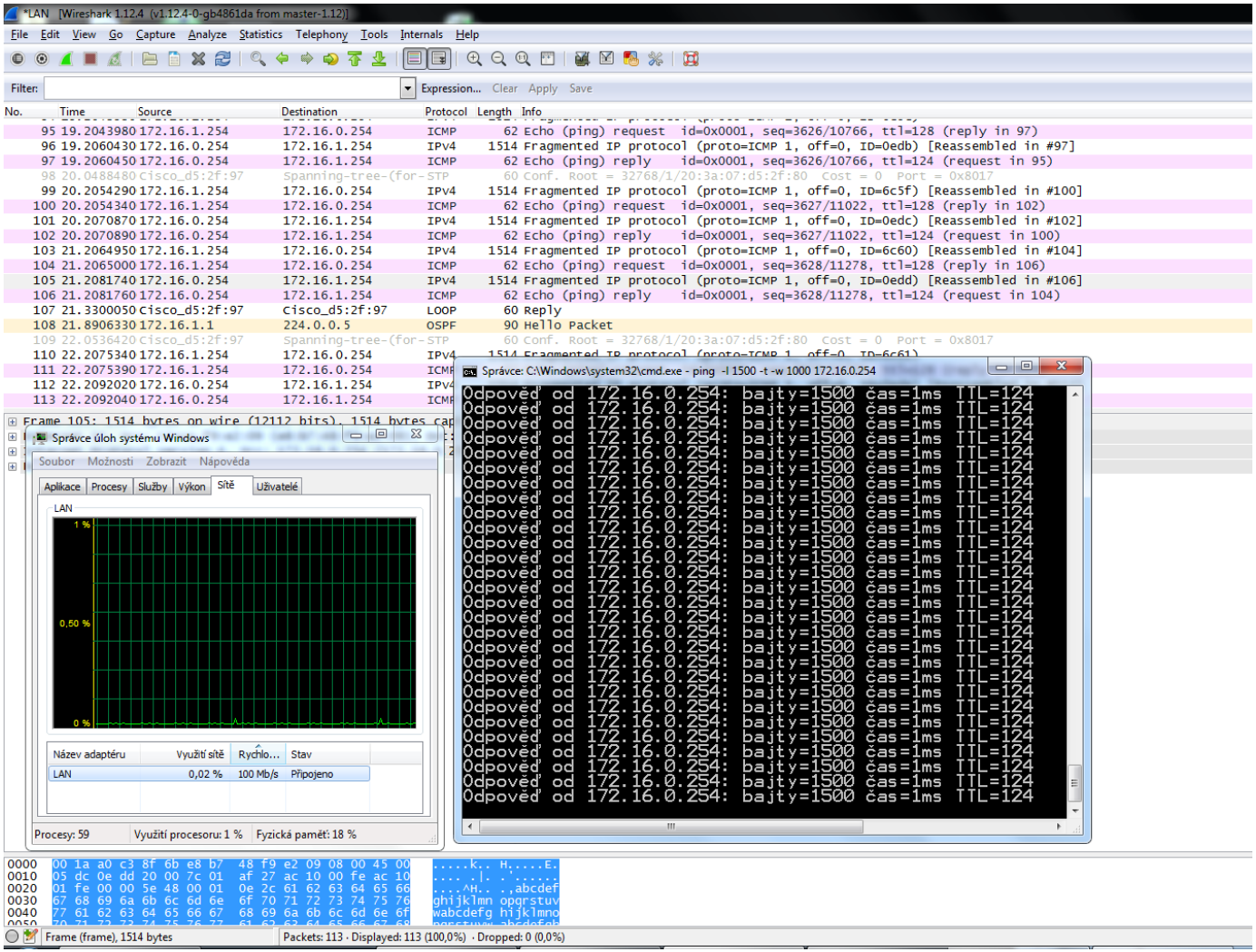
Nastavení UDP flooding a vytížení sítě v MAN



Zahlcení linky UDP datagramy a přerušení ICMP komunikace mezi terminálem, řídícím centrem



Nenarušená ICMP komunikace mezi řídícím centrem a komunikačním terminálem



11.3 Příloha č. 3 výpisy konfigurací síťových prvků

Router R0:

```
Current configuration : 1401 bytes
!
! Last configuration change at 11:55:08
UTC Wed Apr 6 2016
!
version 15.5
no service timestamps debug uptime
no service timestamps log uptime
no service password-encryption
!
hostname R0
!
boot-start-marker
boot-end-marker
!
!
!
no aaa new-model
ethernet lmi ce
!
!
!
!
!
!
no ip domain lookup
ip cef
no ipv6 cef
!
multilink bundle-name authenticated
!
!
!
!
license udi pid CISCO2911/K9 sn
FCZ16386068
!
!
!
redundancy
!
!
!
!
!
!
!
!
!
!
!
!
!
!
interface Embedded-Service-Engine0/0
 no ip address
 shutdown
!
interface GigabitEthernet0/0
 ip address 172.16.0.1 255.255.255.0
 duplex auto
 speed auto
!
interface GigabitEthernet0/1
 ip address 192.168.1.1 255.255.255.252
 duplex auto
 speed auto
!
interface GigabitEthernet0/2
 no ip address
 shutdown
 duplex auto
 speed auto
!
interface Serial0/0/0
 no ip address
 shutdown
 clock rate 2000000
!
interface Serial0/0/1
 no ip address
 shutdown
 clock rate 2000000
```

```
!
router ospf 1
 network 172.16.0.0 0.0.0.255 area 0
 network 192.168.1.0 0.0.0.3 area 0
!
ip forward-protocol nd
!
no ip http server
no ip http secure-server
ip flow-export version 9
!
!
!
!
!
control-plane
!
!
!
line con 0
 login
line aux 0
line 2
 no activation-character
 no exec
 transport preferred none
 transport output pad telnet rlogin lapb-
ta mop udptn v120 ssh
 stopbits 1
line vty 0 4
 login
 transport input none
!
scheduler allocate 20000 1000
!
end
```

Router R1:

```
Current configuration : 1589 bytes
!
! Last configuration change at 12:40:11
UTC Wed Apr 6 2016
!
version 15.5
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname R1
!
boot-start-marker
boot-end-marker
!
!
!
no aaa new-model
ethernet lmi ce
!
!
!
!
!
!
!
!
!
!
!
!
!
no ip domain lookup
ip cef
no ipv6 cef
!
multilink bundle-name authenticated
!
!
!
!
license udi pid CISCO2911/K9 sn
FCZ16386069
!
!
!
redundancy
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
interface Embedded-Service-Engine0/0
 no ip address
 shutdown
!
interface GigabitEthernet0/0
 ip address 192.168.1.2 255.255.255.252
 duplex auto
 speed auto
!
interface GigabitEthernet0/1
 ip address 192.168.3.1 255.255.255.252
 duplex auto
 speed auto
!
interface GigabitEthernet0/2
 ip address 192.168.2.1 255.255.255.252
 duplex auto
 speed auto
!
interface Serial0/0/0
 no ip address
 shutdown
 clock rate 2000000
!
interface Serial0/0/1
 no ip address
 shutdown
 clock rate 2000000
!
interface Serial0/1/0
 no ip address
 shutdown
 clock rate 2000000
!
```

```
interface Serial0/1/1
 no ip address
 shutdown
 clock rate 2000000
!
router ospf 1
 network 192.168.1.0 0.0.0.3 area 0
 network 192.168.2.0 0.0.0.3 area 0
 network 192.168.3.0 0.0.0.3 area 0
!
ip forward-protocol nd
!
no ip http server
no ip http secure-server
!
!
!
!
!
control-plane
!
!
!
line con 0
 logging synchronous
line aux 0
line 2
 no activation-character
 no exec
 transport preferred none
 transport output pad telnet rlogin lapb-ta
mop udptn v120 ssh
 stopbits 1
line vty 0 4
 login
 transport input none
!
scheduler allocate 20000 1000
!
end
```

Router R2:

```
Current configuration : 1486 bytes
!
! Last configuration change at 12:46:07
UTC Wed Apr 6 2016
!
version 15.5
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname R2
!
boot-start-marker
boot-end-marker
!
!
!
no aaa new-model
ethernet lmi ce
!
!
!
!
!
!
!
!
!
!
!
!
!
no ip domain lookup
ip cef
no ipv6 cef
!
multilink bundle-name authenticated
!
!
!
!
license udi pid CISCO2911/K9 sn
FCZ1638606A
license boot module c2900 technology-
package securityk9
!
!
!
redundancy
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
interface Embedded-Service-Engine0/0
 no ip address
 shutdown
!
interface GigabitEthernet0/0
 ip address 192.168.3.2 255.255.255.252
 duplex auto
 speed auto
!
interface GigabitEthernet0/1
 ip address 192.168.5.1 255.255.255.252
 duplex auto
 speed auto
!
interface GigabitEthernet0/2
 ip address 192.168.4.1 255.255.255.252
 duplex auto
 speed auto
!
interface Serial0/0/0
 no ip address
 shutdown
 clock rate 2000000
!
interface Serial0/0/1
 no ip address
 shutdown
 clock rate 2000000
!
router ospf 1
 network 192.168.3.0 0.0.0.3 area 0
 network 192.168.4.0 0.0.0.3 area 0
 network 192.168.5.0 0.0.0.3 area 0
!
```

```
ip forward-protocol nd
!
no ip http server
no ip http secure-server
!
!
!
!
!
control-plane
!
!
!
line con 0
line aux 0
line 2
 no activation-character
 no exec
 transport preferred none
 transport output pad telnet rlogin lapb-ta
mop udptn v120 ssh
 stopbits 1
line vty 0 4
 login
 transport input none
!
scheduler allocate 20000 1000
!
end
```

Router R3:

```
Current configuration : 1598 bytes
!
! Last configuration change at 17:07:08
UTC Fri Jan 23 2015
!
version 15.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname R3
!
boot-start-marker
boot-end-marker
!
!
!
no aaa new-model
!
!
!
!
!
!
!
!
!
!
!
no ip domain lookup
ip cef
no ipv6 cef
!
multilink bundle-name authenticated
!
!
cts logging verbose
!
!
license udi pid CISCO2911/K9 sn
FCZ16386065
!
!
!
redundancy
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
interface Embedded-Service-Engine0/0
 no ip address
 shutdown
!
interface GigabitEthernet0/0
 ip address 192.168.6.1 255.255.255.252
 duplex auto
 speed auto
!
interface GigabitEthernet0/1
 ip address 192.168.2.2 255.255.255.252
 duplex auto
 speed auto
!
interface GigabitEthernet0/2
 ip address 192.168.5.2 255.255.255.252
 duplex auto
 speed auto
!
interface Serial0/0/0
 no ip address
 shutdown
 clock rate 2000000
!
interface Serial0/0/1
 no ip address
 shutdown
 clock rate 2000000
!
interface Serial0/1/0
 no ip address
 shutdown
 clock rate 2000000
!
```

```
interface Serial0/1/1
 no ip address
 shutdown
 clock rate 2000000
!
router ospf 1
 network 192.168.2.0 0.0.0.3 area 0
 network 192.168.5.0 0.0.0.3 area 0
 network 192.168.6.0 0.0.0.3 area 0
!
ip forward-protocol nd
!
no ip http server
no ip http secure-server
!
!
!
!
!
control-plane
!
!
!
line con 0
 logging synchronous
line aux 0
line 2
 no activation-character
 no exec
 transport preferred none
 transport output pad telnet rlogin lapb-ta
mop udptn v120 ssh
 stopbits 1
line vty 0 4
 login
 transport input none
!
scheduler allocate 20000 1000
!
end
```

Router R4:

```
Current configuration : 1580 bytes
!
! Last configuration change at 16:37:56
UTC Wed Apr 6 2016
!
version 15.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname R4
!
boot-start-marker
boot-end-marker
!
!
!
no aaa new-model
!
!
!
!
!
!
!
!
!
!
!
no ip domain lookup
ip cef
no ipv6 cef
!
multilink bundle-name authenticated
!
!
cts logging verbose
!
!
license udi pid CISCO2911/K9 sn
FCZ152620DR
!
!
!
redundancy
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
interface Embedded-Service-Engine0/0
 no ip address
 shutdown
!
interface GigabitEthernet0/0
 ip address 192.168.6.2 255.255.255.252
 ip access-group ANTIUDP in
 duplex auto
 speed auto
!
interface GigabitEthernet0/1
 ip address 172.16.1.1 255.255.255.0
 duplex auto
 speed auto
!
interface GigabitEthernet0/2
 no ip address
 shutdown
 duplex auto
 speed auto
!
interface Serial0/0/0
 no ip address
 shutdown
 clock rate 2000000
!
interface Serial0/0/1
 no ip address
 shutdown
 clock rate 2000000
!
router ospf 1
 network 172.16.1.0 0.0.0.255 area 0
 network 192.168.6.0 0.0.0.3 area 0
```

```
!
ip forward-protocol nd
!
no ip http server
no ip http secure-server
!
!
ip access-list extended ANTIUDP
 deny   udp any any
 permit ospf any any
 permit icmp any any
!
!
!
!
control-plane
!
!
!
line con 0
 logging synchronous
line aux 0
line 2
 no activation-character
 no exec
 transport preferred none
 transport output pad telnet rlogin lapb-ta
mop udptn v120 ssh
 stopbits 1
line vty 0 4
 login
 transport input none
!
scheduler allocate 20000 1000
!
end
```

Univerzita Hradec Králové
Fakulta informatiky a managementu
Akademický rok: 2014/2015

Studijní program: Systémové inženýrství a informatika
Forma: Prezenční
Obor/komb.: Informační management (im2-p)

Podklad pro zadání DIPLOMOVÉ práce studenta

PŘEDKLÁDÁ:	ADRESA	OSOBNÍ ČÍSLO
Holeček Martin	Všestary 176, Všestary	I1424

TÉMA ČESKY:

Analýzy bezpečnostích rizik smart grid sítí

TÉMA ANGLICKY:

Security risk analysis of smart grid networks

VEDOUCÍ PRÁCE:

Mgr. Josef Horálek, Ph.D. - KIT

ZÁSADY PRO VYPRACOVÁNÍ:

Cílem práce bude vytvořit komparativní analýzu bezpečnostních rizik datové LAN sítě vers. smart grid sítě charakteru LAN a navrhnout opatření pro eliminaci bezpečnostních rizik. V teoretické části autor představí vybraná bezpečnostní rizika v sítích LAN a jejich implementace v sítích typu smart grid. V praktické části pak autor navrhne řešení těchto bezpečnostních rizik s využitím znalostí bezpečnosti datových sítí a úpravou standardních řešení pro smart grid.

SEZNAM DOPORUČENÉ LITERATURY:

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.

KNAPP, Eric D a Raj SAMANI. Applied cyber security and the smart grid: implementing security controls into the modern power infrastructure. Boston: Syngress, c2011, xxii, 202 pages. ISBN 978-159-7499-989.

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

KNAPP, Eric D a Michael C ECHOLS. Industrial network security: securing critical infrastructure networks for smart grid, scada, and other industrial control systems. 2nd edition. Boca Raton: CRC Press, 2011, pages cm. ISBN 978-012-4201-149.

Podpis studenta: ..... **Datum:** 8. 4. 2016

Podpis vedoucího práce: ..... **Datum:** 8. 4. 2016