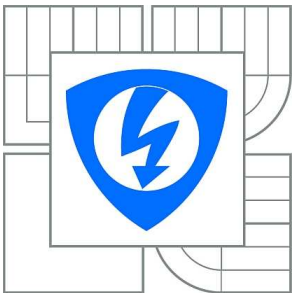
VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

BRNO UNIVERSITY OF TECHNOLOGY



FAKULTA ELEKTROTECHNIKY A KOMUNIKAČNÍCH TECHNOLOGIÍ

ÚSTAV TELEKOMUNIKACÍ

FACULTY OF ELECTRICAL ENGINEERING AND COMMUNICATION

DEPARTMENT OF TELECOMMUNICATIONS

MĚŘENÍ KVALITY ELEKTRICKÉ ENERGIE

MEASUREMENT OF ELECTRIC POWER QUALITY

BAKALÁŘSKÁ PRÁCE

BACHELOR'S THESIS

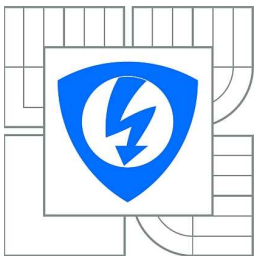
AUTOR PRÁCE — MAREK ŠENK

AUTHOR

VEDOUCÍ PRÁCE — Ing. PETR MLÝNEK

SUPERVISOR

BRNO 2010



VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

Fakulta elektrotechniky a komunikačních technologií

Ústav telekomunikací

Bakalářská práce

bakalářský studijní obor
Teleinformatika

Student: Marek Šenk ***ID:*** 106803
Ročník: 3 ***Akademický rok:*** 2009/2010

NÁZEV TÉMATU:

Měření kvality elektrické energie

POKYNY PRO VYPRACOVÁNÍ:

Nalezněte optimální způsob datové komunikace pro energetická data pro jednotlivé sítě přenosu dat s ohledem na bezpečnost a spolehlivost přenosu. Proveďte analýzu dat z měřičů kvality a vyhodnoťte možné typy zabezpečení pro jednotlivé typy dat. Realizujte sadu měření se záznamníkem kvality Fluke VR1710 a PQ monitory firmy MEgA.

DOPORUČENÁ LITERATURA:

[1] BLAŽEK, V., SKALA, P. Distribuce elektrické energie. Elektronický učební text FEKT VUT v Brně. 2003.
[2] MEgA Měřicí Energetické Aparáty: PQ monitor: MEg30, MEg31, MEg32 a MEg33. 2006. Online: <http://e-mega.cz/doc/pqmonitor_mail.pdf>.
[3] Burda.K.: Bezpečnost informačních systémů. Skripta FEKT VUT v Brně, 2005.

Termín zadání: 29.1.2010 ***Termín odevzdání:*** 2.6.2010

Vedoucí práce: Ing. Petr Mlýnek

prof. Ing. Kamil Vrba, CSc.
Předseda oborové rady

UPOZORNĚNÍ:

ABSTRAKT

Bakalářská práce na úvod objasňuje pojem kvalita elektrické energie a popisuje jednotlivé charakteristiky napětí, které kvalitu elektrické energie určují. Dále se bakalářská práce zabývá nalezením optimální datové komunikace pro energetická data pro telekomunikační sítě, GSM sítě a silnoproudé sítě technologií PLC s ohledem na bezpečnost a spolehlivost přenosu dat. Následně je provedena analýza dat pomocí programu Wireshark. Analyzovaná data byla naměřena měřiče kvality elektrické energie PQ monitor MEg 33. Podle typů analyzovaných dat byly vyhodnoceny možné typy zabezpečení pomocí programu CrypTool 2. Na závěr bakalářské práce je rozebráno měření základních charakteristik kvality elektrické energie a provedeno praktické měření se záznamníkem kvality Fluke VR1710.

Klíčová slova: Kvalita elektrické energie, datová komunikace, zabezpečení, šifrovací algoritmus, měření kvality.

ABSTRACT

Bachelor thesis introduction explains the concept of electric power quality and describes the different characteristics of voltage, which determine the electric power quality. Further bachelor thesis is engaged in finding the optimal data communications for the energy data for telecommunications networks, GSM networks and high-voltage networks PLC technology with regard to safety and reliability of data transmission. Subsequently are analyzes the data using Wireshark. Analyzed data was measured meter of power quality PQ monitor MEg 33. According to the types of analyzed data were evaluated possible types of security using CrypTool 2. At the end of this work is analyzed measuring the basic characteristics of power quality and practical measurement is made with quality recorder Fluke VR1710.

Keywords: Electric power quality, data communication, security, cryptographic algorithm, measurement of quality.

ŠENK, M. *Měření kvality elektrické energie* . Brno : Vysoké učení technické v Brně, Fakulta elektrotechniky a komunikačních technologií, 2010. 50 s. Vedoucí bakalářské práce Ing. Petr Mlýnek.

PROHLÁŠENÍ

Prohlašuji, že svou bakalářskou práci na téma „Měření kvality elektrické energie“ jsem vypracoval samostatně pod vedením vedoucího bakalářské práce a s použitím odborné literatury a dalších informačních zdrojů, které jsou všechny citovány v práci a uvedeny v seznamu literatury na konci práce.

Jako autor uvedené bakalářské práce dále prohlašuji, že v souvislosti s vytvořením této bakalářské práce jsem neporušil autorská práva třetích osob, zejména jsem nezasáhl nedovoleným způsobem do cizích autorských práv osobnostních a jsem si plně vědom následků porušení ustanovení § 11 a následujících autorského zákona č. 121/2000 Sb., včetně možných trestněprávních důsledků vyplývajících z ustanovení § 152 trestního zákona č. 140/1961 Sb.

V Brně dne ....

(podpis autora)

PODĚKOVÁNÍ

Děkuji vedoucímu práce Ing. Petru Mlýnkovi za velmi užitečnou metodickou pomoc a cenné rady při zpracování bakalářské práce.

V Brně dne ....

(podpis autora)

OBSAH

SEZNAM OBRÁZKŮ

SEZNAM TABULEK

ÚVOD

V posledních letech se v EU a tedy i v ČR pohled na kvalitu elektrické energie neustále zpřísňuje. Distribuční společnosti jsou pod přísným dohledem příslušných institucí povinny dodávat konečnému zákazníkovi elektrickou energii předepsané kvality.

Posuzovat kvalitu elektrické energie je nutné od doby, kdy elektrická energie přestala sloužit pouze pro spotřebu výrobce, ale začala se distribuovat a stala se zbožím. Rozvoj techniky přitom přinesl stále častější využívání nelineárních přístrojů a zařízení s proměnlivou provozní charakteristikou (motory, usměrňovače, zářivky, impulsní zdroje, polovodičová technika, atd.). Tyto přístroje a zařízení ale při provozu daleko více zpětně ovlivňují distribuční síť. Tyto zpětné vlivy potom mohou rušit i jiné přístroje a zařízení napájené stejnou sítí. Z tohoto důvodu je třeba kontrolovat kvalitu elektrické energie nejen ve velkých průmyslových podnicích, ale také u menších odběratelů.

Ke zjišťování a kontrole kvality elektrické energie a následnému sběru získaných dat se využívá moderních přístrojů a přenosových technologií. Získaná data lze ke sběrné stanici přenášet pomocí Ethernetu, Internetu, bezdrátových přenosů pomocí GSM resp. GPRS a v neposlední řadě pomocí technologie PLC, která používá jako přenosové médium samotnou energetickou síť. Při přenosu energetických dat je také potřeba zajistit jejich bezpečnost proti zneužití.

Cílem bakalářské práce je popsat kvalitu elektrické energie a parametrů, které kvalitu určují, tato problematika je popsána v první kapitole bakalářské práce. Dále rozebrat datové přenosy v moderních telekomunikačních sítích (Internet a Ethernet), v GSM sítích (GPRS, EDGE) a v silnoproudých sítích technologií PLC s ohledem na přenos dat z měřičů kvality elektrické energie. Poté stanovit metody zabezpečení přenášených dat v uvedených sítích a zvolit optimální způsob datové komunikace pro energetická data. Datové přenosy a zabezpečení přenášených dat v jednotlivých sítích je rozebráno ve druhé a třetí kapitole. V následující kapitole je provedena analýza dat, pomocí programu Wireshark, z měřičů kvality elektrické energie. Analyzovaná data byla naměřena měřícím přístrojem PQ monitor MEg 33. Na konci této kapitoly je provedeno vyhodnocení zabezpečení pro jednotlivé typy dat. Poslední kapitola popisuje problematiku měření kvality elektrické energie a měření konkrétních parametrů charakterizujících kvalitu elektrické energie. Nakonec je zde provedeno praktické dlouhodobé měření se záznamníkem kvality Fluke VR1710.

1 KVALITA ELEKTRICKÉ ENERGIE

Pojem kvalita elektrické energie je často nahrazován pojmem kvalita elektřiny, ovšem nejméně sporným názvem je pojem kvalita napětí. Elektrická energie, kterou jsou napájeny spotřebiče (v domácnostech nebo firmách), není často k dispozici v ideální elektrárnami vyráběné formě. Na zhoršení její kvality nepůsobí pouze přenosové vlastnosti distribučních vedení a meteorologické vlivy, ale také provozní stavy spotřebičů připojených k elektrické síti, které se obecně nazývají „zpětné“ vlivy. Ve smluvních vztazích mezi dodavateli a odběrateli elektrické energie je tedy důležité nejen množství, ale také kvalita dodávané elektrické energie, která je definována v normě ČSN EN 50160 viz. [3]. Kvalita elektrické energie udává hlavní charakteristiky napětí v daném odběrném bodě elektrické sítě nízkého nebo vysokého napětí v normálních provozních podmínkách porovnávaných vzhledem k souboru referenčních technických parametrů. Tyto charakteristiky napětí platí pro všechny napěťové hladiny, velikost směrných hodnot je však pro různé napěťové hladiny různá. Mezi základní charakteristiky napětí patří velikost, kmitočet a odchylka napájecího napětí. Dalšími charakteristikami jsou rychlé změny napětí a flikr, krátkodobé poklesy napájecího napětí, krátkodobá a dlouhodobá přerušení napájecího napětí, nesymetrie napájecího napětí a další.

1.1 Popis charakteristik napětí

Metody vyhodnocování charakteristik napětí se stejně jako metody hodnocení kvality jiných druhů zboží obecně opírají o statistická hodnocení, kdy se vedle směrných parametrů předepisuje určitý rozsah hodnoceného souboru. Charakteristiky kvality napětí jsou definovány při ustálených provozních podmínkách.

Kmitočet napětí

Jmenovitý kmitočet napájecího napětí v ČR je 50 Hz. Střední hodnota kmitočtu základní harmonické musí být v následujících mezích:

50 Hz ± 1% (tj. 49,5…50,5 Hz) během 99,5% roku,

50 Hz + 6%, - 4% (tj. 47…52 Hz) po 100% času

Velikost napájecího napětí

Velikost napájecího napětí je udávána jmenovitým napětím sítě (U_{jm}). Normalizované jmenovité napětí pro veřejnou síť nízkého napětí je 230 V_{ef}. Je to napětí fázové mezi fázovými vodiči a vodičem středním. Normalizovaná hodnota napětí sdruženého je 400 V_{ef}. Na hladině vn se hodnotí napětí sdružená, kde jsou jmenovitá napětí U_{jm} = 3, 6, 10, 22 a 35 kV a na hladině vvn napětí fázová i napětí sdružená, kde je jmenovité napětí U_{jm} = 110 kV.

Odchylky napájecího napětí

Za normálních podmínek, s vyloučením přerušení napájení, musí být během každého týdne 95% průměrných efektivních hodnot napájecího napětí v měřících intervalech

10 min. v rozsahu $U_{jm} \pm 10\%$, tj. 207 V až 253 V pro napětí fázové a 306 V až 440 V pro napětí sdružené. V sítích vvn je stanoveno pouze nejvyšší napětí 123 kV.

Rychlé změny napětí

Rychlá změna napětí je rychlý přechod efektivní hodnoty mezi dvěma ustálenými stavy. Rychlé změny napětí jsou způsobovány zejména změnami zatížení u odběratelů nebo spínáním v síti, kdy se napětí pohybuje v dovolených tolerancích avšak jeho změny vyvolávají nepříznivé účinky u spotřebičů.

Flikr

Flikr (blikání) se může projevovat jako blikání světelných zdrojů, kdy dochází k periodickým změnám efektivní hodnoty napětí, i když se napětí nalézá v dovolených tolerancích. Flikr je charakterizován dvěma parametry a to P_{st} (krátkodobý flikr–10min) a P_{lt} (dlouhodobý flikr–2hod). V normě [3] je předepsáno, že dlouhodobá míra vjemu flikru P_{lt} musí být po 95% času týdenního měření menší než 1,0. Koeficienty P_{st} (short time) i P_{lt} (long time) jsou bezrozměrné.

Krátkodobé poklesy napájecího napětí

Krátkodobé poklesy napájecího napětí jsou obecně způsobeny poruchami ve veřejné distribuční síti nebo v instalacích odběratelů. Očekávaný počet poklesů může být během roku od několika desítek až do jednoho tisíce. Krátkodobý pokles je charakterizován svou hloubkou a dobou trvání. Většina poklesů má dobu trvání kratší než 1 sekunda a hloubku poklesu menší než 60%. V některých oblastech se mohou velmi často vyskytovat poklesy s hloubkou mezi 10% - 15% U_{jm} jako následek spínání zatížení u odběratelů.

Krátkodobá a dlouhodobá přerušení napájecího napětí

Přerušení napájecího napětí je definováno jako stav, kdy napětí klesne pod prahovou hodnotu. V normě [3] se uvádí hodnota 1% U_{jm}, v aktualizovaných provozních předpisech [10] se přechází na 5% U_{jm}. U trojfázového vývodu nastává přerušení až tehdy, když všechna tři napětí klesnou pod prahovou hodnotu a přerušení končí, jakmile alespoň jedno napětí vzroste nad prahovou hodnotu. Roční výskyt krátkodobých přerušení napájecího napětí je v rozsahu několika desítek až několika stovek. Přibližně 70% krátkodobých přerušení může mít dobu trvání menší než 1 sekunda. Roční četnost dlouhodobých (poruchových) přerušení napětí delších než 3 minuty může být menší než 10, avšak v závislosti na oblasti může dosahovat až hodnot okolo 50 [9].

Dočasná přepětí o síťovém kmitočtu

Dočasná přepětí o síťovém kmitočtu mezi živými vodiči a zemí vznikají při zemních poruchách. V uzemněných soustavách se napětí nezvýší nad $1{,}71 \times U_{jm}$. V izolovaných soustavách nebo při rezonancích může vzniknout dočasné přepětí i vyšší než $2 \times U_{jm}$. Nejčastěji vznikají dočasná přepětí při regulacích napětí v odtíženém stavu.

Přechodná přepětí mezi živými vodiče a zemí

Jedná se o časově proměnné průběhy přepětí způsobené spínacími pochody nebo atmosférickými vlivy. Spínací přepětí nejsou obvykle tak strmá jako přepětí atmosférická. Spínací přepětí mají vesměs delší dobu trvání. V normě [3] se neuvádí limitní hodnoty ani počty těchto přepětí. Nejefektivnější je zajištění koordinace izolace

u spotřebitele s koordinací izolace u distributora tj. vybudování stupňů ochrany s omezovači přepětí.

Nesymetrie napětí

V normálních provozních podmínkách sítě nn musí být v libovolném týdenním období 95% desetiminutových středních efektivních hodnot zpětné složky napájecího napětí v rozsahu do 2% složky sousledné. Pro trojfázové systémy se v normě [7] používá k výpočtu nesymetrie vztahů:

$$U_Z = \sqrt{\frac{1-\sqrt{3-6\beta}}{1+\sqrt{3-6\beta}}} \ , \tag{1.1}$$

$$\text{kde} \quad \beta = \frac{U_{12}^4 + U_{23}^4 + U_{31}^4}{\left(U_{12}^2 + U_{23}^2 + U_{31}^2\right)^2} \ . \tag{1.2}$$

Napěťová nesymetrie má vliv na snížení výkonů motorů.

Harmonická napětí

Harmonická napětí vznikají zpětným působením různých přístrojů a zařízení do distribuční soustavy, které svojí činností generují vyšší harmonické. V oblasti malých výkonů mohou být příčinou tohoto jevu počítače, televizory, síťové adaptéry apod., v oblasti vyšších výkonů součásti řízení motorů - měniče frekvence a zdroje nepřerušitelného napájení (UPS). V 50 Hz sítích používaných v ČR vznikají kmitočty o 150, 250 a 350 Hz, v menší míře ještě vyšší kmitočty, ty jsou odborně označovány jako 3., 5. nebo 7. harmonická. Činitel tvarového zkreslení THD (Total Harmonic Distortion) harmonických složek do řádu 40 včetně musí být v nn sítích menší nebo roven 8,0% U_{jm}. Celkové harmonické zkreslení THD se v normě [3] počítá dle vztahu:

$$THD = \sqrt{\sum_{n=2}^{40} \left(\frac{U_n}{U_1}\right)^2} \ , \tag{1.3}$$

kde U_1 je velikost napětí první (základní) harmonické složky napětí,

U_n je velikost napětí n-té harmonické složky napětí.

Meziharmonická napětí

Ve frekvenčních pásmech mezi harmonickými složkami se vyskytují meziharmonická napětí, která nejsou zanedbatelná zvláště v provozech s frekvenčními měniči. V normě [8] je uveden kmitočtový interval mezi dvěma po sobě jdoucími mezi harmonickými spektrálními čarami o velikosti 5 Hz. V normě jsou také definovány metody seskupování meziharmonických napětí do skupin. Rozlišuje se zde skupina harmonických, skupina meziharmonických a vycentrovaná skupina meziharmonických. Pro hodnoty meziharmonických napětí nejsou zatím definovány směrné hodnoty.

Úrovně napětí signálů v napájecím napětí

Distribuční síť je také využívána k přenosu informací. V rámci normy [3] se jedná o systémy pracující v pásmu kmitočtů do 2 kHz, ovšem nelze také zapomínat na systémy PLC (Power Line Communication), které pracují na frekvencích přes 100 kHz. U nás se běžně používá tzv. systém hromadného dálkového ovládání (HDO), který nejčastěji pracuje s kmitočtem 216,67 Hz. Pro hodnocení vlivu signálu HDO na kvalitu napětí se používají mezi harmonické složky 210 Hz, 215 Hz, 220 Hz a 225 Hz, z nichž se používají průměrné hodnoty za dobu 3 s. Norma předepisuje, že 99% těchto 3 s hodnot musí být při kmitočtu 216,67 Hz menší než 9% U_{jm}.

2 DATOVÁ KOMUNIKACE

Komunikace, tj. sdělování, je *přenos informace* mezi několika místy podle dohodnutých pravidel. V souvislosti se zpracováním informace je informace vyjadřována ve tvarech vhodných ke komunikaci, uchování, nebo zpracování. Pojem *Informace* vznikl ve snaze vyjádřit použitelnost určité skupiny poznatků používaných pro rozhodování v dalším postupu při nějaké činnosti. Na teoretické úrovni se problematikou informace zabývá *teorie informace*. K nejdůležitějším odvětvím teorie informace patří *teorie přenosu informace*, s níž bývá často ztotožňována. [12]

Pojmem datová komunikace lze tedy označit proces výměny dat mezi různými systémy a jejich aplikacemi. V ideálním případě probíhá datová komunikace automatizovaně a zabezpečeně, aby bylo zabráněno neoprávněným přístupům k datům.

2.1 Data

Data jsou základem pro vytváření informací. Pod pojmem data si lze představit různé údaje, hodnoty, čísla, znaky, symboly, grafy a podobně. Slouží k vyjádření (reprezentaci) skutečností formálním způsobem tak, aby je bylo možné přenášet, uchovávat, dále interpretovat či zpracovávat (např. počítačem).

2.1.1 Data v informačních a komunikačních technologiích

Data v informačních a komunikačních technologiích se dají rozdělit do dvou skupin. První skupinou jsou data strukturovaná. Jedná se o typ dat, která se vyznačují určitou pravidelností a zákonitostmi. Strukturováním je vytvořena taková organizace dat, která umožňuje efektivně ukládat, zpracovávat a vyhledávat údaje podle potřeby. Strukturovaná data vytvářejí vyhledávací klíče, což jsou klíče, které jednoznačně identifikují datový záznam, nazývají se privátní klíče (identifikační klíče). Základní typy strukturovaných dat jdou dat: textová, číselná, logická, datum a čas, zakódovaná data, údaje věcné – jméno, příjmení, věk, adresa, cena…, apod.

Druhou skupinou jsou data nestrukturovaná. Jedná se například o volný text, audio, video, grafiku, multimédia a podobně. Poskytují více dat než jen strukturované údaje. Problémem může být, že v nich lze velmi těžko vyhledávat. Tento problém je řešen tak, že nestrukturovaná dat jsou doplněna o data strukturovaná. Například obrázek bez názvu bychom jen velmi těžko hledali v určitém souboru obrázků, ovšem dáme-li mu nějaký název, čímž dojde k doplnění o data strukturovaná, vyhledání je potom velmi jednoduché.

2.2 Datová komunikace v moderních telekomunikačních sítích

Telekomunikační síť je soubor koncových zařízení, přenosových, spojovacích, signalizačních, dohledových a řídících prostředků pro zajištění požadované kvality

telekomunikačních služeb. [14]

Mezi nejznámější moderní telekomunikační sítě v dnešní době patří sítě typu Ethernet a celosvětový systém navzájem propojených počítačových sítí Internet.

2.2.1 Základní typy sítí

Telekomunikační sítě lze rozdělit do dvou základních skupin podle toho, jakým způsobem předávají data mezi koncovými uzly [14]:

- sítě se **spojováním okruhů**,
- sítě se **spojováním datových jednotek**.

Obě dvě skupiny mají své výhody, ale také i nevýhody. Kromě přepojovaných komunikačních technik existují také permanentní (pevné) okruhy, které existují stále, čímž nedochází k jejich sestavování a rušení. Velkou nevýhodou těchto permanentních okruhů je vysoká cena pronájmu pevného spoje.

2.2.2 Základy počítačových sítí

Počítačovou sítí se obecně rozumí spojení dvou a více počítačů a dalších výpočetních prostředků. Jednotlivé počítače a další prvky, z nichž se počítačová síť skládá, se nazývají uzly sítě. Jednotlivé uzly jsou mezi sebou propojeny komunikačními médii (metalické kabely, optické kabely, bezdrátově pomocí elektromagnetických vln) tak, aby byly schopny vzájemné komunikace.

Počítače připojené k síti, které nabízejí své prostředky, se nazývají *servery*. Počítače s přístupem k těmto prostředkům se označují jako *pracovní stanice* nebo *klienti*. Servery jsou většinou nejvýkonnějšími počítači v síti, protože výkon potřebují k obsluze mnoha požadavků jiných počítačů, které sdílejí jejich prostředky. Pracovní stanice nebo klienti jsou naproti tomu obvykle počítače, které jsou levnější a méně výkonné. Počítač může být zpravidla serverem nebo pracovní stanicí, avšak jen zřídka obojím (toto oddělení velmi zjednodušuje správu a administraci sítě). [1]

Velikosti sítí

Počítačové sítě lze podle své velikosti a funkce rozdělit na tří základní skupiny:

- **LAN** – Local Area Network, místní (lokální) síť. LAN je základní klasifikací kterékoli počítačové sítě. Její architektura může být jednoduchá (dva počítače spojené kabelem) až složitá (desítky až stovky propojených počítačů a různých periferních zařízení). Přenosové rychlosti u sítí LAN začínají na hodnotách desítek Mbit/s. Nejnovější technologie umožňují přenos s rychlostí jednotek Gbit/s. Mezi nejznámější typy lokálních sítí patří Ethernet, Token Ring,… Rozlišujícím faktorem sítě LAN je to, že je omezena pouze na určitou geografickou oblast, jako je třeba oddělení, jedna budova nebo několik blízkých budov a podobně. Rozsah sítě LAN bývá většinou stovky metrů až jednotky kilometrů.
- **MAN** – Metropolitan Area Network, metropolitní síť. Metropolitní sítě umožňují rozšíření působnosti lokálních sítí jejich prodloužením, zvýšením

počtu připojených stanic a zvýšením rychlosti. Propojují lokální sítě v městech či v městských aglomeracích. Rychlost MAN sítí bývá vysoká, přenosové rychlosti se pohybují ve stejných hodnotách jako u sítí LAN. Normalizovaná metropolitní síť existuje jedna: protokol Distributed Queue Dual Bus (DQDB). Spojuje vzdálenosti řádově jednotek až desítek kilometrů.

- **WAN** – Wide Area Network, rozsáhlá síť. Spojují sítě LAN a MAN po celé zemi nebo kontinentu. Bývají většinou veřejné, ale existují i soukromé WAN sítě. Přenosové rychlosti se velmi liší podle typu sítě (od desítek kbit/s až po rychlosti řádů Gbit/s). Nemají žádná geografická omezení. Pravděpodobně nejzákladnější sítí WAN je Internet.

2.2.3 Topologie sítí

Termín topologie označuje způsob, jakým jsou počítače a další zařízení v síti propojeny (kabely, bezdrátově). Konkrétní typ kabelu, který je použit, stanovuje topologii sítě. Nelze nainstalovat určitý typ kabelu za použití libovolné topologie. Třemi hlavními topologiemi v sítích jsou sběrnicová, hvězdicová a kruhová.

2.2.4 Ethernet

Ethernet je jeden z typů lokálních sítí. Dosahuje přenosových rychlostí od 10 Mb/s a až po nejrychlejší varianty 10 Gb/s. Je standardizován skupinou standardů IEEE 802.3x (x – rozlišuje specifikace pro různé rychlosti). Existuje mnoho standardů pro různé rychlosti a typy vedení. Nejčastěji používaným typem je 100 BASE-TX (802.3u) s rychlostí 100 Mb/s. Jako komunikační médium se používají 4 kroucené páry UTP kabelu kategorie 5. Tento standard používá kódování 4B/5B, čtveřice bitů jsou překódovány na pětici a poté zakódovány do kódu NRZI (Non Return to Zero). Jedná se o inverzní kód, což způsobí, že každá jednička způsobí změnu polarity. Každé zařízení je identifikováno pomocí hardwarových adres tzv. MAC adres. Toto adresování má zajistit přesnou identifikaci zařízení při vysílání a příjmu, aby nedocházelo ke kolizi vysílaných dat.

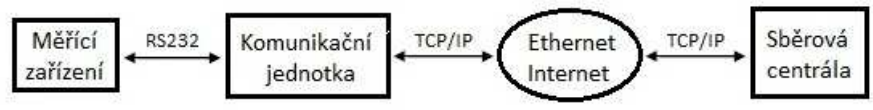
2.2.5 Internet

Internet je síťové propojení počítačů provozovaných různými subjekty, kde každý počítač, který je připojený do internetu, má svojí IP adresu a může komunikovat s ostatními počítači v síti. IP adresa je jedinečné 32 bitové číslo. Technicky je internet komplexní výtvor, jehož podsítě spojují počítače s rozdílným hardwarem a softwarem mezi sebou. Rychlost přenosu dat v síti závisí na typu a technice sítě (LAN, MAN, WAN). Komunikace v počítačových sítích probíhá na základě protokolů. Počítačový protokol je sada komunikačních pravidel, které definují postupy a parametry, které se používají při vysílání a příjmu dat.

2.2.6 Ethernet a Internet pro sběr dat

V současné době se stává velmi populární dálkový sběr dat, jako jsou např. dálkové odečty elektroměrů apod. Velkou výhodou dálkových odečtů je možnost častých odečtů nebo určení kvality el. energie bez nutnosti fyzické kontroly u elektroměrů. Nevýhodou

dálkového sběru dat můžou být neoprávněné zásahy do přenášených dat. Z tohoto důvodu je potřeba přenášená data zabezpečit. Přenos odečtených dat z elektroměru až ke sběrové centrále je zobrazen na Obr. 2.1.



Obr. 2.1: Komunikační řetězec při sběru dat přes Ethernet nebo Internet

Z elektroměru jsou pomocí měřícího zařízení kvality elektrické energie (např. PQ monitor) odečteny dat a poté přes sériovou sběrnici RS232 odeslány do komunikační jednotky. Komunikační jednotka data příjme a připraví na odeslání pomocí protokolu TCP/IP. Díky tomu lze data poslat přes Ethernet nebo Internet do sběrové centrály, kde jsou data přijata a dále zpracovávána (vyhodnocena, archivována apod.).

2.3 Datová komunikace v GSM

GSM (Globální Systém pro Mobilní komunikaci původně však francouzsky „Groupe Spécial Mobile“) je nejpopulárnější standard pro mobilní telefony na světě. Všudypřítomnost standardu GSM dělá z mezinárodního telefonování běžnou záležitost. GSM se od předchozích technologií liší tím, že signální i hovorové kanály jsou digitální, což přináší do světa telekomunikací řadu výhod. Tato technologie je označována jako druhá generace (2G) systému mobilních telefonů. Poskytovatelé GSM tak mohou zákazníkům mobilní sítě poskytnout řadu nových služeb a kvalitnější zpracování a přenos dat. U GSM je zachována zpětná kompatibilita s původními GSM telefony. Ve stejné době pokračuje GSM standard s vývojem schopností paketových dat přidaných do standardu ve verzi z roku 1997 pod zkratkou GPRS. Vyšší přenosové rychlosti dat byly představeny jako EDGE a UMTS (v tomto případě už se jedná o sítě třetí generace-3G) ve verzi z roku 1999. Z analogových systémů NMT je známá přístupová metoda FDM. V případě GSM byla metoda přístupu k médiu, zde ke kmitočtovému spektru, rozšířena o technologii TDM. Určité kmitočtové pásmo tak může využít více mobilních účastníků, než tomu bylo u analogových systémů. Kmitočtová pásma pro GSM byla s vývojem technologie postupně zvolena na kmitočtech kolem 900, 1800, 1900 MHz. Jednotlivá pásma jsou rozdělena na kanály, které mají od sebe navzájem odstup 200 kHz.

2.3.1 Základní princip GSM

GSM síť je založena na buňkovém systému, který definuje rozložení kanálů na území, které je pokryto tímto signálem. V jednotlivých buňkách jsou zvoleny určité kmitočty, které jsou pro konkrétní buňky vysílány. Možnost kanály opakovaně využívat je umožněna díky buňkovému systému.

Základní přenosovou jednotkou v GSM je burst. Rozlišujeme několik druhů, které mají rozdílnou velikost a využití jednotlivých polí. Velikost timeslotu je dána velikostí

normálového burstu, což je 156,25 bitů. Z toho 114 bitů se využívá pro přenos a realizaci spojení v GSM.

2.3.2 Datové služby v GSM

Mobilní digitální sítě byly původně vyvinuty hlavně pro přenos hlasu v digitálním tvaru. Díky tomu je pro ně relativně snadné přenášet kromě hlasu i obecná data. Z hlediska datových služeb jsou realizovány služby s přepínáním okruhů a s přepínáním datových jednotek.

Službami využívající přepínání okruhů jsou technologie CSD a HSCSD, která pracuje na podobném principu jako přenos hlasu s tím rozdílem, že přenášená informace je datového charakteru. Nevýhodou těchto technologií je blokování timeslotu a také vyšší cena, která je účtována za dobu připojení. Rozdíl mezi technologií CSD a HSCSD je v počtu obsazených timeslotů a tím dostupné přenosové kapacity. CSD a HSCSD jsou vhodné pro aplikace v reálném čase, kde je potřeba garantované šířky pásma.

Služby využívající přepínání datových jednotek jsou GPRS a EDGE. Jde o technologie založené na zasílání datových jednotek ve formě paketů. Nedochází zde k blokování timeslotů, jsou sdíleny mezi mobilními stanicemi. Pro konkrétní přenos stanice rezervuje patřičný počet timeslotů a realizuje paketový přenos. Jedná se o služby bez garance přenosové kapacity a jsou vhodné pro širší veřejnost, která využívá datové spojení k přístupu na Internet. Největším rozdílem mezi GPRS a EDGE je přenosová rychlost, která je závislá na způsobu modulace.

HSCSD (High Speed Circuit Switched Data)

HSCSD je technologie pro rychlejší přenos dat, která v sítí GSM využívá více časových intervalů. Princip je založen na přepínání okruhů a přenos přináší výrazné zrychlení. Na jednom časovém slotu jsou data přenášena buď rychlostí 9,6 kb/s, ale s pomocí zefektivnění zabezpečovacího mechanismu a omezení prostoru pro opravné bity je možno z 22,8 kb/s, připadajících na jeden interval, využívat 14,4 kb/s [15]. Maximální přenosová rychlost, kterou tato technologie dosahuje, je 64 kb/s. Ve většině případů jde o asymetrický přenos, kdy jsou ve směru od mobilní stanice přiděleny tři časové intervaly a ve směru k mobilní stanici je přidělen jeden časový interval. Tento způsob přidělování je velmi často používán a je vhodný např. pro připojení k Internetu, kdy data směřují převážně od sítě k uživateli. HSCSD rozděluje možné režimy do 18 tříd podle toho, kolik kanálů je možno v jednotlivých směrech použít.

Tab. 2.1: Některé třídy v HSCSD

Třída HSCSD		1	2	3	4	5	6	9	10	12	18
Maximální počet slotů	**Příjem**	1	2	2	3	2	3	3	4	3	8
	Vysílání	1	1	2	1	2	2	2	2	3	8
	Celkem	2	3	4	4	4	4	5	5	6	16

GPRS (General Packet Radio Service)

Jedná se o přepínanou datovou službu nabízenou GSM ve 2,5. generaci. V dnešní době je pokrytí GPRS signálem srovnatelné s GSM signálem. GPRS nabízí široké využití a jeho hlavní výhodou je sdílení timeslotů s ostatními mobilními stanicemi. Pro jeho

realizaci bylo nutné provést určité úpravy ve stávající GSM síti. Poskytuje průměrnou rychlost datových přenosů používáním TDMA kanálů v GSM síti.

GPRS je technologií, které negarantuje přenosovou kapacitu, z tohoto důvodu byla do standardu přidána služba QoS (Quality of Service), která umožňuje definovat požadovanou kvalitu. Parametry, se kterými je možné sestavit požadované QoS, jsou zpoždění, propustnost, spolehlivost atd. Silným nastavení QoS je možné se přiblížit datovým technologiím CSD a HSCSD. Technologii GPRS musí podporovat, jak síť, tak mobilní stanice, pro které se vytvořila třída GPRS, která definuje použití této technologie v souvislosti s hlasovými službami. Pro GPRS byly definovány tyto třídy terminálů:

- **Třída A** – umožňuje využívat současně služby GPRS (spojování paketů) a služby hlasové (spojování okruhů), oba druhy služeb jsou ovládány nezávisle na sobě
- **Třída B** – umožňuje využívat GPRS nebo hlasové služby, ale je možné je automaticky přecházet mezi těmito dvěma režimy (lze přerušit přenos paketů při příchozím hovoru a pokračovat po skončení hovoru)
- **Třída C** – u těchto terminálů je nutné nastavení režimu (paketový nebo okruhový), při nastavení spojování paketů nelze využívat hlasové služby a naopak

Dále byla stanovena prioritní třída, která určuje prioritu jednotlivých služeb na mobilní stanici:

- **Nejvyšší priorita** – hovorové služby
- **Střední priorita** – datové služby CSD a HSCSD
- **Nejnižší priorita** – datové služby GPRS, EDGE

Kódové schéma u GPRS

GPRS nabízí několik variant datových přenosů, které se liší přenosovou kapacitou, která je dána zvolením kódového schématu (CS). Kódové schéma definuje využití jednotlivých uživatelských bitů. Jejich celkový počet je rozdělen na bity starající se o zabezpečení a bity, která přenášejí vlastní data. Kódové schéma je mobilní stanici přiděleno ze základnové stanice a jeho volba je závislá na kvalitě signálu. Rozdíl mezi kódovými schématy je v poměru počtu bitů pro zabezpečení a množství přenášených dat. V tab. 2.2 jsou uvedena jednotlivá kódová schémata se svojí přenosovou rychlostí.

Tab. 2.2: Kódová schémata pro GPRS

Třída	CS-1	CS-2	CS-3	CS-4
Přenosová rychlost	9,05 kb/s	13,4 kb/s	15,6 kb/s	21,4 kb/s

Možnosti mobilních zařízení

Mobilní stanice jsou rozděleny do tříd (multislot class) podle toho kolik timeslotů (TS) umí použít pro uplink, downlink a kolik z toho současně. Běžně GSM/GPRS/EDGE stanice umí současně používat maximálně 5 timeslotů. Nejnovější stanice třídy 32 umí použít již 6 timeslotů, ovšem toto musí podporovat i síť.

Třída (multislot class) může být rozdílná pro HSCSD, GPRS a EGPRS. Nejběžnější třídou dnes je třída 10 v konfiguraci 4+1 nebo 3+2. Daná konfigurace je zvolena podle převládajícího toku dat a mění se podle aktuální situace.

Tab. 2.3: Multislotové třídy v GPRS

Třída	1	2	3	4	5	6	7	8	9	10	11	12	32
Downlink TS	1	2	2	3	2	3	3	4	3	4	4	4	5
Uplink TS	1	1	2	1	2	2	3	1	2	2	3	4	3
Současně TS	2	3	3	4	4	4	4	5	5	5	5	5	6

Maximální přenosové rychlosti

GPRS nabízí čtyři kódová schémata CS-1 až CS-4, kdy je příslušné kódové schéma vybíráno podle aktuálního odstupu signál/rušení. Některé sítě nepodporují všechny čtyři schémata, ale pouze schéma CS-1 a CS-2. GPRS nabízí nejvyšší rychlost 80 kb/s při kódování CS-4 a konfiguraci telefonu (stanice) 4+1 (4 timesloty pro downlink a 1 pro uplink). V případě, že telefon podporuje multislot class 32 (např. novější modely telefonů) a toto podporuje i síť, pak lze teoreticky u GPRS dosáhnout rychlosti pro download 100 kb/s.

EDGE (Enhanced Data rates for Global Evolution)

EDGE je dalším vývojovým stupněm v technologii GSM po zavedení datových přenosů pomocí GPRS. Tato technologie nabízí několik metod a vylepšení umožňující dosáhnout efektivního přenosu dat a vysoké spektrální účinnosti v tomto úzkopásmovém buňkovém systému.

Hlavní vylepšení je využití modulace 8-PSK (osmistavová fázová modulace), která umožňuje přenášet tři informační bity pomocí jednoho symbolu na rádiové vrstvě. U GPRS používaná modulace GMSK dovoluje přenášet pouze jeden informační bit na jeden symbol na rádiové vrstvě.

EDGE zahrnuje dvě hlavní části:

- **EGPRS (Enhanced GPRS)** – slouží k přepínání paketů = paketový přenos
- **ECSD (Enhanced CSD)** – slouží k přepojování okruhů

EGPRS je rozšířením služby GPRS, který nabízí paketový přenos a tarifování za přenesená data nebo za měsíční paušál. ECSD je rozšířením služby HSCSD, což je služba s komutováním digitálních okruhů. HSCSD je v dnešní době méně používané z důvodu tarifování (účtování podle času a počtu kanálů), než GPRS (účtování podle přenesených dat nebo měsíční paušál a neomezená data). Stejná situace je i u ECSD a EGPRS. Většina operátorů ani ECSD v rámci EDGE neimplementuje.

EGPRS (Enhanced GPRS)

EGPRS je částí implementace EDGE a je rozšířením služby GPRS v sítích GSM. Nabízí vyšší přenosové rychlosti než GPRS a je zpětně kompatibilní s GPRS. Mobilní sítě s podporou EDGE a EGPRS jsou označovány jako sítě 2,75G.

Rozšíření EGPRS:

- nová modulace 8-PSK oproti standardní GMSK
- devět kódových a modulačních schémat oproti čtyř u GPRS
- nově přepracovaná vrstva RLC/MAC
- inkrementální redundance
- větší délka okna
- resegmentace
- retransmise

Kódové schéma u EGPRS

EGPRS používá devět kódových a modulačních schémat MCS-1 až MCS-9. Jsou vybírány v závislosti na odstupu signál/rušení tak, aby zajišťovaly co nejlepší přenos dat.

Tab. 2.4: Kódová schémata u EGPRS

Kódové schéma	MCS-1	MCS-2	MCS-3	MCS-4	MCS-5	MCS-6	MCS-7	MCS-8	MCS-9
Rychlost (kb/s)	8,8	11,2	14,8	17,6	22,4	29,6	44,8	54,4	59,2
Modulace	GMSK	GMSK	GMSK	GMSK	8-PSK	8-PSK	8-PSK	8-PSK	8-PSK

Maximální přenosové rychlosti

EGPRS dosahuje nejvyšší rychlosti maximálně 236,8 kb/s při použití kódového schématu MCS-9 a konfiguraci telefonu (stanice) 4+1 (4 timesloty pro download a 1 pro upload). V praxi se u EGPRS (EDGE) dosahuje rychlostí menších, konkrétně pro download kolem 200 kb/s a pro upload kolem 100 kb/s při konfiguraci timeslotů 3+2. K využití služby EDGE je potřeba mít mobilní telefon nebo jiné zařízení, které tuto technologii podporuje. Pokud přístroj podporuje multislot class 32 (např. novější modely telefonů) a toto podporuje i síť, pak lze teoreticky u EGPRS dosáhnout rychlosti pro download 296 kb/s.

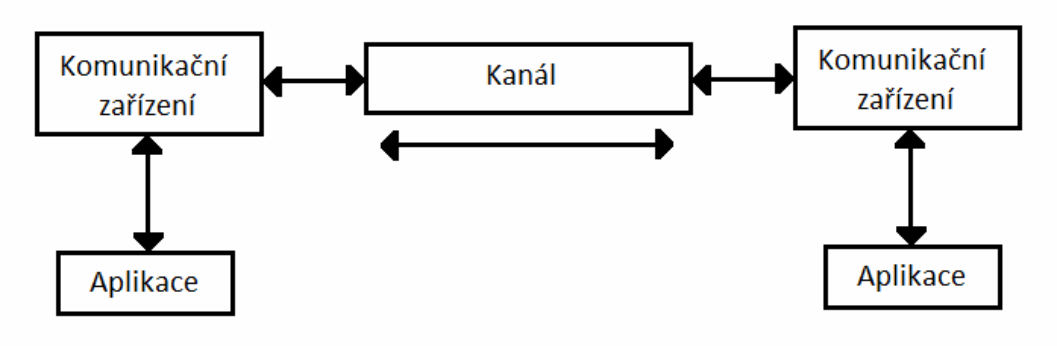
Pro sběr dat z měřičů kvality elektrické energie se jeví jako nejvhodnější technologie GPRS používající kódové schéma CS-1. GPRS je omezeno pouze dostupností signálu použitého operátora. Kódové schéma CS-1 poskytuje dostatečné zabezpečení přenášených dat vůči rušení a také proti neoprávněné manipulaci s daty, ale nenabízí příliš vysoké přenosové rychlosti. Pro sběr dat ovšem není potřeba vysokých přenosových rychlostí vzhledem k přenášeným objemům dat z měřičů kvality elektrické energie.

2.4 Datová komunikace v silnoproudých sítích technologií PLC

2.4.1 Technologie PLC

PLC (Power Line Communication, v překladu „komunikace po silových rozvodech“)

systémy se obecně neliší od jiných telekomunikačních systémů. V dané aplikaci (aplikace pro sběr dat z měřičů kvality elektrické energie, elektroměrů apod.) se přes uživatelské rozhraní iniciuje požadovaná služba, následně komunikační zařízení zpracuje požadavek a nakonec dojde k přenosu signálu komunikačním kanálem k cílové aplikaci (Obr. 2.2).



Obr. 2.2: Obecné schéma PLC

Přenosové médium a princip přenosu dat po síti nn

Přenosovým médiem pro PLC je energetická síť, která se skládá z přenosové a distribuční soustavy. Přenosovou soustavou se rozumí systém zařízení, která zajišťují přenos elektrické energie od elektráren k rozvodnám (pro PLC se tato část nepoužívá). Část od rozvoden k jednotlivým uživatelům se nazývá distribuční soustava.

Přenos dat po rozvodné síti je založen na principu injektování (kapacitní nebo induktivní vazbou) datového signálu namodulovaného na nosnou vyšší frekvenci do energetického vedení, a v galvanickém oddělení datového signálu na straně přijímače. Tímto způsobem lze po vedení posílat binární data. Uživatelé, kteří jsou připojeni na stejný transformátor, sdílejí dostupnou kapacitu kanálu, a proto je potřeba zajistit bezpečnost komunikace prostřednictvím šifrování dat.

Komunikaci po elektrické napájecí síti lze všestranně použít v mnoha aplikacích (kontrolní informace o stavu elektroměru, přístupové technologie k Internetu nebo spojení několika sítí LAN a MAN po vysokonapěťových vodičích).

Z hlediska použití je možné PLC systémy rozdělit na úzkopásmové a širokopásmové. Každá oblast je využita pro odlišný způsob komunikace, jsou použité různé modulační techniky, které jsou vhodné pro dané aplikace a které se liší přenosovými vlastnostmi.

Širokopásmové PLC systémy využívají kmitočtové pásmo od 2 MHz do 30 MHz a používají výrazně vyšší přenosové rychlosti, které přesahují hodnotu 2 Mb/s ve venkovních rozvodech a přes 12 Mb/s ve vnitřních rozvodech budov. Širokopásmové PLC systémy používají širokopásmové modulace typu CDMA a OFDM. OFDM je v současnosti nejvyužívanější metoda širokopásmové modulace.

Pro aplikace zajišťující přenos dat z měřičů kvality elektrické energie je používán úzkopásmový PLC systém s využitím úzkopásmové modulace, který je dále rozebrán podrobněji.

2.4.2 Úzkopásmové PLC systémy

Úzkopásmové PLC systémy jsou používány nejen pro dálkový sběr dat. Přenosové kanály s nízkou úrovní rušení poskytují malé přenosové rychlosti v úrovni stovek kilobitů za sekundu. Tyto přenosové rychlosti ovšem dostačují pro průmyslové využití. Může se jednat o sběr dat, monitorování a regulaci apod. Mezi zvláštní služby patří centrální řízení spotřeby energie.

Úzkopásmové PLC systémy pracují na frekvenčním rozsahu, který je definován CENELEC (Evropský výbor pro elektrotechnickou standardizaci) normou ČSN EN 50065, která poskytuje kmitočtový rozsah od 9 kHz do 148,5 kHz pro přenos dat po energetické síti. Kmitočtové pásmo je rozděleno do čtyř pásem [13] uvedených v Tab. 2.5.

Tab. 2.5: Rozdělení kmitočtových pásem v Evropě

Pásmo	Kmitočtový rozsah	Poznámka
	3 až 95 kHz	jen pro dodavatele el. energie
A	9 až 95 kHz	pro dodavatele el. energie a po jejich souhlasu i pro odběratel
B	95 až 125 kHz	jen pro odběratele
C	125 až 140 kHz	jen pro odběratele – vyžadován protokol o přistoupení k dohodě

Pásmo A CENELEC normy je používáno pro tzv. energetický dohled a další s tím související služby (sledování spotřeby a produkce energie, čtení z domovních elektroměrů apod.). Pásma B a C jsou využívána v aplikacích tzv. domácí automatizace (např. ovládání různých zařízení napojených na elektrickou síť, zabezpečovací úkoly apod.). Nejnižší možnou frekvenci pro přenos dat lze stanovit na 100 kHz, protože na nižších frekvencích je velká úroveň šumu od zařízení připojených k síti. Při nejvyšší frekvenci 148,5 kHz lze vidět, že šířka pásma není vysoká, čímž je ovlivněna i přenosová rychlost.

Kritéria pro rozšíření

Pro rozšíření této technologie je zapotřebí stanovit určitá kritéria, které by měly datové přenosy splňovat:

- Zajištění spolehlivé komunikace s dostatečně rychlým datovým přenosem.
- Dostatečné zabezpečení přenášených dat proti zneužití.
- Minimální nebo aspoň srovnatelné finanční náklady ve srovnání s konkurenčními technologiemi.
- Dosažení co největšího dosahu při dálkovém sběru dat.

Úzkopásmové modulace

Pro spolehlivou komunikaci přes přenosové médium je důležité zvolit vhodný způsob přenosu. Z pohledu měření kvality elektrické energie a následného sběru získaných dat jsou nejvýhodnější úzkopásmové modulace o jedné nosné. Tyto modulace jsou na napájecím vedení používány ve frekvenčním pásmu okolo 100 kHz. Dají se použít

pouze pro nízké bitové rychlosti v řádu stovek kilobitů za sekundu, což je ovšem pro přenos dat z měřičů kvality el. energie dostačující.

Rozlišujeme tyto druhy úzkopásmových modulací:

- **FSK (Frequency Shift Keying) - frekvenční klíčování** – modulace je založena na klíčování značky či mezery pomocí dvou rozdílných kmitočtů. Rozdíl klíčovacích kmitočtů je označován jako zdvih neboli shift.
- **PSK (Phase-Shift Keying) - fázové klíčování** – informace se kóduje pomocí změny fáze vysílaného signálu. Vzniká možnost použití dvou stavů, kde jsou fáze navzájem otočené o π (BPSK - Binary Phase-Shift Keying) nebo použití několik různých stavů (QPSK - Quadrature Phase Shift Keying).
- **GMSK (Gaussian Minimum Shift Keying)** – jedná se o speciální typ úzkopásmové modulace, kde jsou data vysílána ve fázi vyplývající z konstantní obálky. Při vyšších přenosových rychlostech než 2 Mb/s je signál odolný proti úzkopásmovému a impulsnímu rušení.

Přenos dat pomocí energetické sítě přináší své výhody i nevýhody. Velkou výhodou je úspora nákladů při tvorbě datové sítě, protože jako přenosového média je samozřejmostí využití současných energetických rozvodů elektrické energie, které patří celosvětově mezi nejrozšířenější síť. Není tedy nutné budovat novou síť pro datové přenosy. Rozvodná síť je využívána pro přenos energie a dat určených ke vzdálenému spotřebiči. Výhodou je také dostupnost této technologie v místech, kde nelze například realizovat bezdrátovou síť z důvodu rušení. Základní nevýhodou úzkopásmového PLC systému je praktická realizace, protože v různých zemích jsou odlišné silové rozvody a také kvůli dějům, které v napájecí síti probíhají (nejčastěji rušení způsobované el. spotřebiči). Proto je zapotřebí propracovaných technik modulací a přenosu dat. Další nevýhodou je poměrně těžké zabezpečení bezpečného přenosu dat. Rozšíření úzkopásmového PLC systému brání nejednotnost a velké množství různých specifikací (X-10, ModemTec,…). Problémem je také dosažení vyšších přenosových rychlostí, jaké jsou možné u ostatních přenosových médií.

3 METODY ZABEZPEČENÍ PŘENÁŠENÁCH DAT

Data nestačí chránit pouze před jejich ztrátou, ale je nutno je také chránit před jejich zneužitím, tedy přečtením a neoprávněným zneužitím neautorizovanou osobou. Při nedůsledné ochraně se může přihodit, že dojde k neoprávněnému vniknutí do Vašeho počítače, mobilního zařízení, bankovních účtů, ke konkurenci se mohou dostat Vaše firemní plány či konstrukční řešení, mohou uniknout důvěrná data, či může dojít k porušení Zákona o ochraně osobních údajů. Jaké nepříjemnosti to může znamenat si není těžké představit. Z těchto důvodů jsou veškerá přenášená data v moderních telekomunikačních sítích, GSM sítích apod. zabezpečována pomocí různých metod a technik (šifrování, kódování apod.).

3.1 Metody zabezpečení přenášených dat v moderních telekomunikačních sítích

Pro zajišťování bezpečnosti informačních systémů je velmi důležitou vědou kryptografie. U ochran kryptografického typu je charakteristické to, že přístup k aktivům (pro majitele cenné, např. data, software,…) je umožněn na základě vyřešení nějakého matematického problému. Tyto matematické problémy jsou voleny tak, aby je útočník nemohl být schopen vyřešit v reálném čase. Uživatel však má k dispozici nějakou tajnou informaci (tj. heslo), s jejíž pomocí je schopen problém úspěšně vyřešit a tak přístup k aktivům (datům) získat. Kryptografickou ochranu tedy můžeme definovat jako technickou ochranu, která je založena na obtížnosti řešení matematických problémů. Problematikou konstrukcí kryptografických ochran se zabývá věda nazývaná kryptografie. Problematikou překonávání kryptografických ochran se zabývá věda nazývaná kryptoanalýza. Souhrn obou zmíněných věd je kryptologie. [2]

Informace v počítačových sítích je možné přenášet dvěma způsoby, jimiž jsou data v zašifrovaném stavu nebo v nezašifrovaném stavu. Nezašifrovaná data nejsou nijak zabezpečená, čímž je možné je bez problému „přečíst“ a následně změnit nebo zneužít. Pokud chceme přenášená data zašifrovat a ztížit tak možnost jejich zneužití, využijeme některý ze šifrovacích algoritmů. Šifrovací algoritmy můžeme rozdělit do dvou základních skupin, a to symetrické a nesymetrické (asymetrické).

3.1.1 Symetrické šifrovací algoritmy

Symetrické šifrovací algoritmy používají k zašifrování a dešifrování přenášených dat jediný klíč – utajený klíč. Výhodou těchto šifer je jejich nízká výpočetní náročnost, z toho vyplývá vysoká rychlost a použití pro šifrování velkého objemu dat. Nevýhodou je nutnost sdílení tajného klíče, na kterém se musí odesílatel a příjemce předem domluvit. Symetrické šifry se často používají společně s šiframi asymetrickými. Použití je takové, že otevřený text se zašifruje symetrickou šifrou s náhodně vygenerovaným klíčem. Tento symetrický klíč se zašifruje veřejným klíčem asymetrické šifry, takže dešifrovat data může pouze majitel tajného klíče dané asymetrické šifry.

Symetrické šifry se dělí na dva druhy. Prvním typem jsou proudové šifry (FISH, RC4), které zpracovávají otevřený text po jednotlivých bitech. Druhým typem jsou blokové šifry (AES, DES, RC2,…), které rozdělují otevřený text na bloky stejné velikosti a doplní vhodným způsobem poslední blok na stejnou velikost. U většiny šifer je používán blok o velikosti 64 bitů, AES používá blok o velikosti 128 bitů. Hlavní výhodou symetrického šifrování je, že je obecně velmi rychlé a dá se použít pro šifrování velkého objemu dat.

3.1.2 Asymetrické šifrovací algoritmy

Asymetrické šifry (např. RSA, ElGamal) používají dvou rozdílných klíčů k šifrování a dešifrování. Šifrovací klíč je veřejný, majitel klíče jej volně uveřejní a kdokoliv jím může šifrovat jemu určené zprávy. Dešifrovací klíč je soukromý, majitel jej drží v tajnosti a pomocí něj může tyto zprávy dešifrovat. Je zřejmé, že šifrovací a dešifrovací klíč spolu musí být matematicky spojeny, avšak nezbytnou podmínkou pro užitečnost šifry je nemožnost ze znalosti šifrovacího klíče spočítat klíč dešifrovací. Tento mechanizmus je využíván také pro elektronický podpis, čímž lze u dat prokázat jejich autora. Asymetrické algoritmy jsou velmi pomalé a prakticky nepoužitelné pro šifrování velkého objemu dat.

Pro zabezpečení přenášených dat v moderních telekomunikačních sítích z měřičů kvality elektrické energie by bylo vhodné použít symetrické blokové šifry AES (Advanced Encryption Standard). AES má pevnou velikost bloku dat 128 bitů a šifrovací klíče o velikostech 128, 192 nebo 256 bitů. Velikost klíče a bloku je nezávislá. Výhodou blokové šifry AES je vysoká rychlost šifrování a poměrně dobrá odolnost proti kryptoanalýze při zvolení dostatečně kvalitního (bezpečného) klíče.

3.2 Metody zabezpečení přenášených dat v GPRS

Přenos dat mezi mobilním terminálem a základnovou stanicí přes rádiové rozhraní znamená na jednu stranu výbornou mobilitu účastníků, ale na stranu druhou je to místo potencionálního nebezpečí. Sítě GSM/GPRS z toho důvodu používají množství bezpečnostních mechanizmů. Jde zejména o použité protokoly a formáty dat, GMSK modulace, neustálé přelaďování terminálů na různé frekvence (frequency hopping) a kanálové kódování.

Přenášená data jsou v síti GSM/GPRS chráněna při přenosu páteřní sítí a rádiovou částí sítě proti odposlechu pomocí šifrování. SGNS (Serving GPRS Support Node) a mobilní stanice používá 128 bitové náhodné číslo použité při autentizaci a privátní klíč uložený na SIM a taky v HLR (Home Location Register-domovský lokační registr) a prostřednictvím algoritmu A8 se vygeneruje šifrovací klíč. Data přenášená mezi uživatelem a sítí GPRS se šifrují pomocí algoritmu A5. Klíčem pro tento algoritmus se používá hodnota K8, která je získána výpočtem, kdy K8 je počítáno pomocí algoritmu A8, již při ověřování totožnosti uživatele. Po vypočtení K8 je tato hodnota uložena do SIM karty a při zahájení komunikace je použita jako klíč pro algoritmus A5.

K zabezpečení přenášených dat pomocí GPRS nebo EDGE také přispívá vhodná volba kódového schématu. Pro zvolení určitého kódového schématu je potřeba si určit, jak moc jsou data důležitá, tedy jaký vyžadují stupeň zabezpečení a jak rychle

potřebujeme posílaná data získat (vhodná volba přenosové rychlosti). Podle těchto parametrů zvolíme, buď schéma s vyšší přenosovou rychlostí, ale data nebudou příliš zabezpečená nebo bude rychlost přenosu pomalejší, ale data budou lépe chráněna proti neoprávněnému zásahu.

3.3 Metody zabezpečení přenášených dat v silnoproudých sítích technologií PLC

Také v silnoproudých sítích je potřeba zabezpečit přenášená data před jejich zneužitím a neoprávněným změnám. K šifrování přenášených dat se používá algoritmus DES, 3DES nebo AES. Šifrování DES (Data Encryption Standard) používá blok délky 64 bitů a šifrovací klíč má délku 56 bitů. Zesílenou variantů DES je šifrování 3DES (Triple-DES), které pracuje s trojnásobným klíčem (168 bitů). Tyto dva šifrovací algoritmy se v PLC již příliš nepoužívají.

V současné době se u PLC zařízení používá šifrování používající algoritmus AES (Advanced Encryption Standard). AES patří mezi symetrické blokové šifry. Symetrické šifrovací algoritmy používají stejný klíč pro šifrování i dešifrování. Algoritmus má pevnou velikost bloku dat (128 bitů) a šifrovací klíče o velikostech 128, 192 nebo 256 bitů. Velikost klíče a bloku je nezávislá. Výhodou blokového šifrátoru AES je větší odolnost vůči kryptoanalýze (nutné zvolit dostatečně bezpečný klíč) a vysoká rychlost šifrování.

Dalšími systémy vhodnými pro zabezpečení přenášených dat (např. z měřičů kvality el. energie) v PLC je systém AMM (Automated Meter Management – Systém pro dálkové zpracování odečtů dat elektroměrů a jejich řízení) a systém AMR (Automated Meter Reading – automatické odečty elektroměrů). AMM je systém komunikace mezi centrálou a jednotlivými měřícími místy. Tato komunikace je obousměrná a zpravidla ji řídí centrála. Systém zajišťuje, že v případě neoprávněného zásahu do elektroměru nebo silového vedení je místo snadno odhaleno. Základním prvkem AMM systému je Smart Meter, který měří nejen spotřebu el. energie, ale i mnoho dalších parametrů sítě (např. okamžitá hodnota napětí, účiníku, výpadky či poklesy napětí apod.). Základní systém AMM umožňuje efektivní měření, monitorování a řízení všech měřících míst. Velký důraz je kladen na jednoduchost systému sběru dat a na dostupnost informací (rychlost přenosu dat).

4 ANALÝZA DAT A METODY ZABEZPEČENÍ

4.1 Analýza dat z měřičů kvality elektrické energie

Analyzovaná data byla naměřena pomocí měřiče kvality elektrické energie PQ monitor MEg 33. Pro analýzu dat byl následně použit software Wireshark.

V následující podkapitole je uvedeno praktické měření s měřičem kvality elektrické energie PQ monitor MEg 33. Měření je zahrnuto v této kapitole z toho důvodu, že data s naměřenými hodnotami byla použita pro analýzu pomocí Wireshark.

4.1.1 Měření s PQ monitorem MEg 33

PQ monitor MEg 33 je multifunkční měřící přístroj pro měření a dlouhodobý záznam až čtyř napětí a čtyř proudů, činných i jalových výkonů a energií v trojfázových čtyřvodičových i pětivodičových nn sítích i v sítích vn a vvn. V souladu s normou ČSN EN 50160 a dle metod mezinárodního standardu IEC 61000-4-30 analyzuje všechny parametry kvality napětí. [11]

Praktické měření bylo provedeno dlouhodobě od 21.5.2010 do 23.5.2010 na fázi, na kterou jsou napojeny zásuvky v bytě panelového domu. Interval záznamu jednotlivých měření byl nastaven na 10 minut.

Na Obr. 4.1 je zobrazena statistika naměřených údajů. Konkrétně byly měřeny hodnoty napětí, kmitočtu, flickeru a vzniklé harmonické kmity. Z naměřených údajů je patrné, že naměřené charakteristiky napětí odpovídají normě [3].

DOBA	M	Od	Do	$I_{h(THD)}$	M	E
Doba zpracování		21.5.2010 16:50:00	23.5.2010 14:40:00	U_h	M	I
VELIČINA		EN 50160	HODN.(/Mimo mez)			
Délka měření		1 týden	1d 21:50:00			
Interval záznamu		10 minut	10 min			
Frekvence 99.5 % roku		50 Hz +1% -1%	48,85 - 50,06 / 0,36%			
Frekvence 100 % roku	M	50 Hz +4% -6%	48,85 - 50,06 / 0%			
Nesymetrie 95 %	M	2,0%	Neměřeno			
VELIČINA		EN 50160	L1	L2		L3
Napětí 95 %		230V +6% -10%	222,7 - 228,5 / 0%	Neměřeno		Neměřeno
Napětí 100 %	M	230V +10% -15%	222,4 - 228,5 / 0%	Neměřeno		Neměřeno
Flicker Plt 95 %	M	1,0	0,06 - 0,15 / 0,4%	Neměřeno		Neměřeno
THD 95 %	M	8,0 %	2,00 - 2,80 / 0%	Neměřeno		Neměřeno
2.harmonická 95 %		2,0 %	Vyhovuje	Neměřeno		Neměřeno
3.harmonická 95 %	M	5,0 %	0,70 - 1,10 / 0%	Neměřeno		Neměřeno
4.harmonická 95 %		1,0 %	Vyhovuje	Neměřeno		Neměřeno
5.harmonická 95 %	M	6,0 %	1,00 - 2,30 / 0%	Neměřeno		Neměřeno
6.harmonická 95 %		0,5 %	Vyhovuje	Neměřeno		Neměřeno
7.harmonická 95 %	M	5,0 %	0,70 - 1,50 / 0%	Neměřeno		Neměřeno
8.harmonická 95 %		0,5 %	Vyhovuje	Neměřeno		Neměřeno
9.harmonická 95 %		1,5 %	Vyhovuje	Neměřeno		Neměřeno
10.harmonická 95 %		0,5 %	Vyhovuje	Neměřeno		Neměřeno
11.harmonická 95 %	M	3,5 %	0,00 - 0,40 / 0%	Neměřeno		Neměřeno
12.harmonická 95 %		0,5 %	Vyhovuje	Neměřeno		Neměřeno
13.harmonická 95 %		3,0 %	Vyhovuje	Neměřeno		Neměřeno
14.harmonická 95 %		0,5 %	Vyhovuje	Neměřeno		Neměřeno
15.harmonická 95 %		0,5 %	Vyhovuje	Neměřeno		Neměřeno
16.harmonická 95 %		0,5 %	Vyhovuje	Neměřeno		Neměřeno
17.harmonická 95 %		2,0 %	Vyhovuje	Neměřeno		Neměřeno
18.harmonická 95 %		0,5 %	Vyhovuje	Neměřeno		Neměřeno
19.harmonická 95 %		1,5 %	Vyhovuje	Neměřeno		Neměřeno
20.harmonická 95 %		0,5 %	Vyhovuje	Neměřeno		Neměřeno
21.harmonická 95 %		0,5 %	Vyhovuje	Neměřeno		Neměřeno
22.harmonická 95 %		0,5 %	Vyhovuje	Neměřeno		Neměřeno
23.harmonická 95 %		1,5 %	Vyhovuje	Neměřeno		Neměřeno
24.harmonická 95 %		0,5 %	Vyhovuje	Neměřeno		Neměřeno
25.harmonická 95 %		1,5 %	Vyhovuje	Neměřeno		Neměřeno
HDO_217 99% dne	M	9,0 %	0,0 - 1,7	Neměřeno		Neměřeno

Obr. 4.1: Statistika naměřených údajů

Z dalšího obrázku je vidět konkrétní naměřené hodnoty napětí. Průměrná hodnota napětí byla naměřena 225,9 V a maximální hodnota napětí byla naměřena 230,7 V. Tyto hodnoty jsou v toleranci s normou [3].

DOBA	Od	Do	
Doba zpracování	21.5.2010 16:50:00	23.5.2010 14:53:50	
Pro dny týdne	pondělí	neděle	
Pro hodniny dne	0	23	
NAPĚTÍ	**L 1 [V]**	**L 2 [V]**	**L 3 [V]**
Průměr	225,9	Neměřeno	Neměřeno
Maximum	230,7	Neměřeno	Neměřeno
Kdy	21.5.2010 22:38:22		
Minimum	0,3	Neměřeno	Neměřeno
Kdy	23.5.2010 14:51:36		

Obr. 4.2: Naměřené hodnoty napětí

Na posledním obrázku jsou zobrazeny naměřené hodnoty událostí na napětí. Z hodnot je patrné, že během měření došlo ke dvěma přerušení napětí. Celková doba obou přerušení byla 15 sekund. Naměřené hodnoty přerušení napětí jsou v toleranci s normou [3].

DOBA	Od	Do	
Doba zpracování	21.5.2010 16:50:00	23.5.2010 14:53:51	
HLADINY [%]	**Poklesy**	**Převýšení**	
Nastavené hranice	< 90	> 110	
STATISTIKA	**L1**	**L2**	**L3**
Počet poklesů	0	Neměřeno	Neměřeno
Počet přepětí	0	Neměřeno	Neměřeno
Počet přerušení	2	Neměřeno	Neměřeno
Počet událostí	2	Neměřeno	Neměřeno
Celková doba poklesů	0:00:00	Neměřeno	Neměřeno
Celková doba přepětí	0:00:00	Neměřeno	Neměřeno
Celková doba přerušení	0:00:15	Neměřeno	Neměřeno
Celková doba událostí	0:00:15	Neměřeno	Neměřeno
Počet přerušení >3 min	0	Neměřeno	Neměřeno
Celková doba přerušení >3 min	0:00:00	Neměřeno	Neměřeno

Obr. 4.3: Naměřené události na napětí

4.1.2 Analýza dat pomocí programu Wireshark

Program Wireshark je výkonný nástroj pro analýzu síťových protokolů, umožňující zachytávání a podrobné zkoumání dat protékajících sítí nebo zachycených a uložených na disku. Zachytávat je možno pakety procházející přes rozhraní Ethernet, IEEE 802.11, ATM, Bluetooth, USB, Token Ring, Frame Relay a mnoha dalších.

Při analýze dat se lze setkat s daty malých velikostí (jednotky kB) až po velké velikosti (jednotky MB).

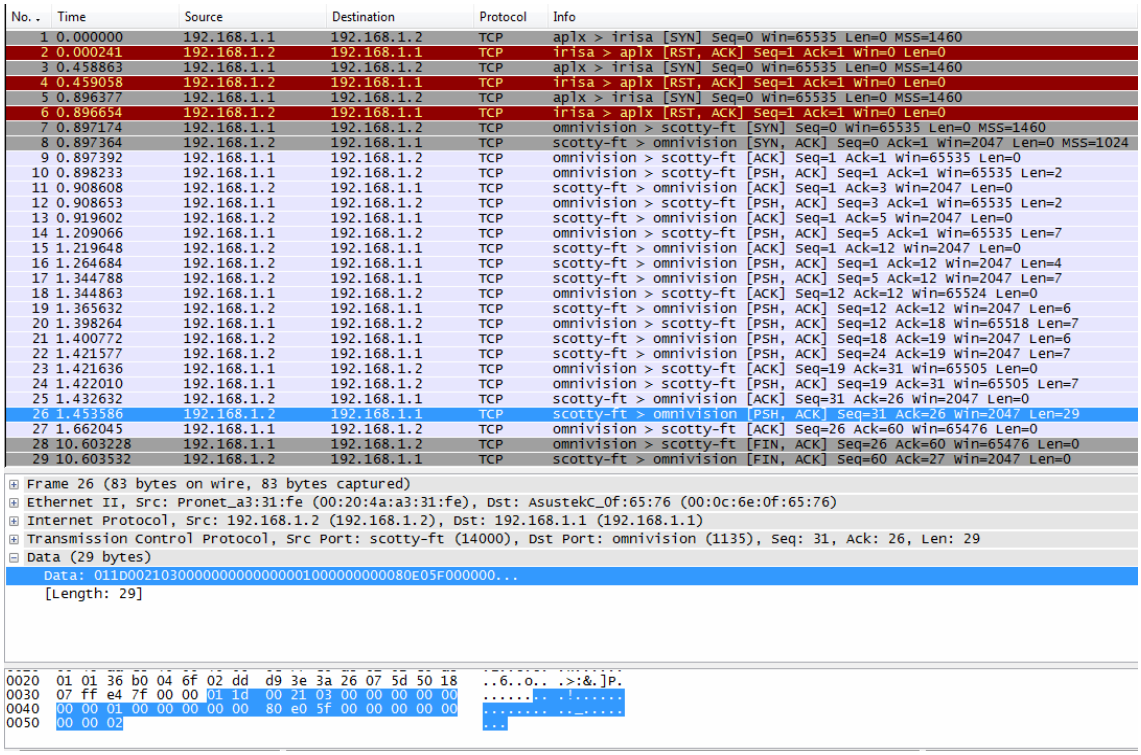
Data malých velikostí

Tyto data většinou slouží pro zjišťování a nastavování parametrů měřících přístrojů. Jedná se o data velikosti jednotek kilobajtů. V elektrické síti bude tento typ dat poměrně častý, protože komunikace s měřícími přístroji je nezbytná pro získávání a nastavování správných parametrů. V následující tabulce jsou uvedený příklady takových dat získaných při měření.

Tab. 4.1: Data malých velikostí

úkol	velikost dat v kB
informace o měřícím přístroji	2
test spojení	3
nastavení měření	4
nastavení parametrů	2
online měření	2

Na následujícím obrázku (Obr. 4.4) je vidět komunikace mezi měřícím přístrojem PQ monitor MEg 33 a síťovým rozhraním počítače. Na počátku komunikace proběhne sestavení spojení pomocí signálů RST, ACK a SYN, po úspěšném spojení dojde k samotnému přenosu naměřených dat a po skončení přenosu dojde k ukončení spojení signály FIN a ACK. Na obrázku je zvýrazněn (modrou barvou) přenášený rámec obsahující určitá naměřená data.



Obr. 4.4: Zachycený přenos při vyčtení informací o PQ monitoru

Data velkých velikostí

Tyto data slouží především k přenosu naměřených parametrů z měřičů kvality, elektroměrů apod. Data mohou mít různé velikosti podle četnosti měření, nastavení měřících intervalů atd. Jedná se o data o velikostech od desítek kB až po jednotky MB. V elektrické síti se tyto data mohou vyskytovat více i méně častěji podle toho, o jaký typ měřených údajů se jedná, jde-li o údaje z měřičů kvality nebo z elektroměrů a jiných zařízení. Při měření jednotlivých parametrů kvality se mohou data posílat velmi často, např. po několika sekundách či minutách nebo po delší době, jedná-li se o dlouhodobá měření. Při přenosu dat z elektroměrů je pravděpodobné, že se nebudou posílat data každých 10 minut, ale měření proběhne např. jednou za týden. V Tab. 4.2 jsou uvedeny příklady dat velkých velikostí.

Tab. 4.2: Data velkých velikostí

délka měření	velikost dat
krátkodobé	90 kB
dlouhodobé	6,9 MB
dlouhodobé	18,8 MB

Komunikace mezi měřícím přístrojem PQ monitor MEg 33 a síťovým rozhraním počítače probíhala stejně jako v případě přenosu dat malých velikostí.

Z analyzovaných dat bylo zjištěno, že v energetických sítích se vyskytují data ve velikostech od jednotek kilobajtů až po jednotky megabajtů. Data o velikostech

jednotek kilobajtů jsou data pro získání informací o měřícím přístroji, pro nastavení parametrů, nastavení měření, test spojení apod. Data o velikostech od desítek kilobajtů až po jednotky megabajtů obsahují již naměřené hodnoty kvality elektrické energie podle nastavení měřícího přístroje. Velikost naměřených dat je tedy závislá na délce měření, jedná-li se o krátkodobé nebo dlouhodobé měření, a také na nastavení měřícího intervalu.

Analyzovaná data lze tedy rozdělit na dva typy:

- data pro zjišťování a nastavování parametrů měřícího přístroje,
- data nesoucí již konkrétní naměřené hodnoty z měřícího přístroje.

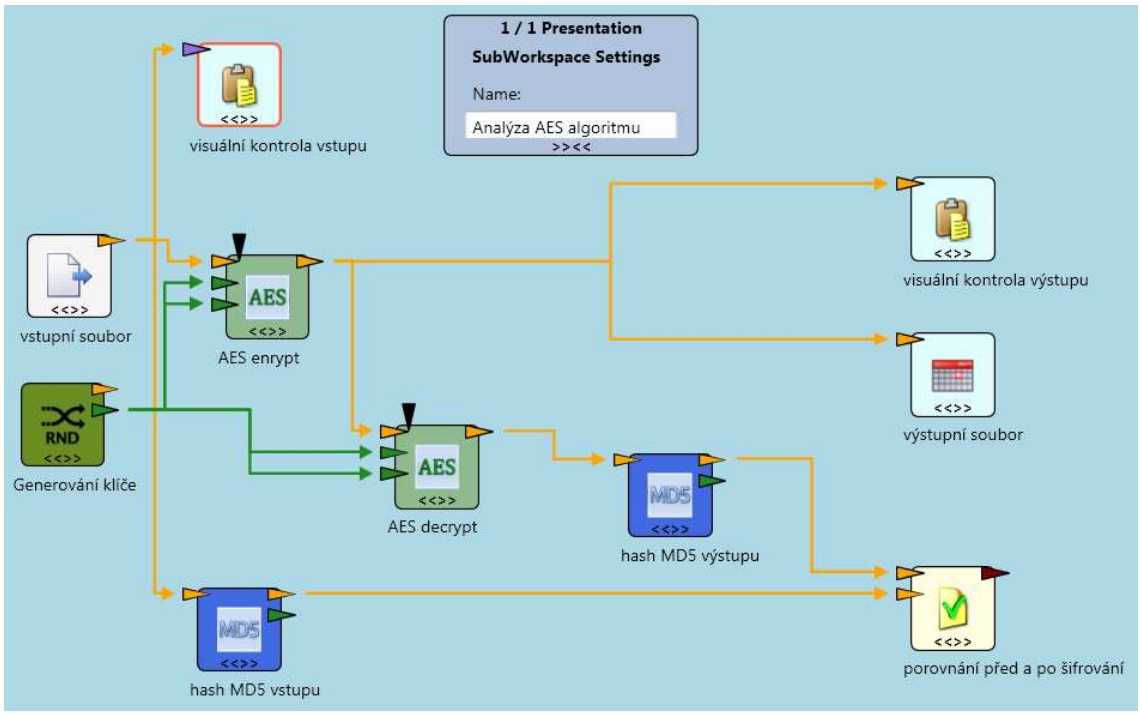
4.2 Vyhodnocení metod zabezpečení pro jednotlivé typy dat

Ke srovnání a vyhodnocení nejvhodnějších šifrovacích metod pro zabezpečení přenášených dat z měřičů kvality elektrické energie byl použit software CrypTool 2. Jedná se o software pro aplikaci a analýzu kryptografických metod. S jeho pomocí lze vytvářet nové dokumenty, otevírat existující a také je modifikovat. Dokumenty lze šifrovat a dešifrovat pomocí různých šifrovacích metod – klasických a moderních (např. RSA, DES, AES, metody eliptické křivky…).

CrypTool navíc dokáže vypočítat hash hodnoty dokumentu. Automatické analyzátory pro klasická šifrovací schémata jsou stanoveny tak, že umožňují určit klíč, který má být použit pro šifrování dokumentu (v některých případech jsou nutné některé další informace).

Při testování jednotlivých šifrovacích algoritmů byla použita analyzovaná data, která byla naměřena pomocí PQ monitoru MEg 33 (viz. kapitola 4.1). Prvním testovaným souborem byl malý soubor o velikosti 3 kB, který slouží k testu spojení mezi měřícím přístrojem a PC. Dalším testovaným souborem byl soubor se záznamem kvality elektrické energie získaný při krátkodobém měření, který má velikost 90 kB. Pokud šifrování tohoto souboru proběhlo bez problémů, byl dále testován velký soubor o velikosti 6,9 MB se záznamem kvality elektrické energie získaný při dlouhodobém měření s nastaveným měřícím intervalem 2 s.

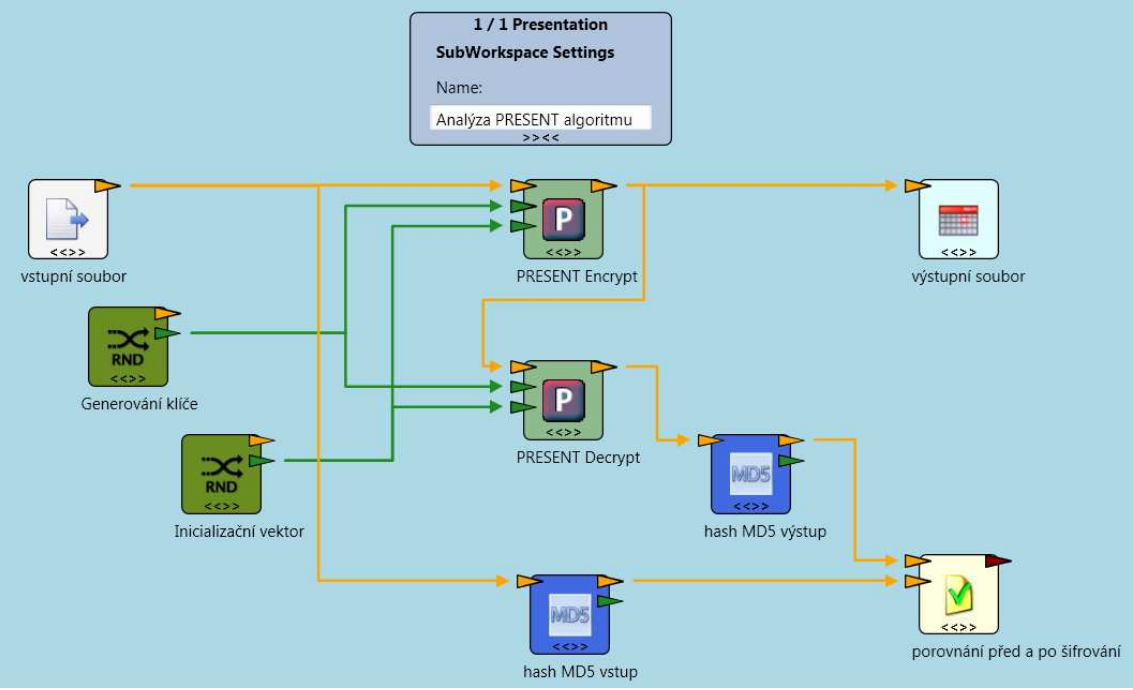
Šifrovací algoritmus AES



Obr. 4.5: Schéma šifrování pomocí algoritmu AES

Při testování šifrovacího algoritmu AES byly postupně šifrovány všechny druhy analyzovaných dat. Po porovnání dat před a po šifrování bylo zjištěno, že se šifrovaná data shodují, což znamená, že nedošlo k žádné změně šifrovaných dat. Tento výsledek je dán vlastnostmi algoritmu AES, který data šifruje do dostatečně velkých bloků o velikosti 128 bitů, čímž lze bezpečně šifrovat i větší objemy dat a má i dostatečnou velikost šifrovacího klíče, který zajistí bezpečnost dat při přenosu. Další výhodou je vysoká rychlost šifrování.

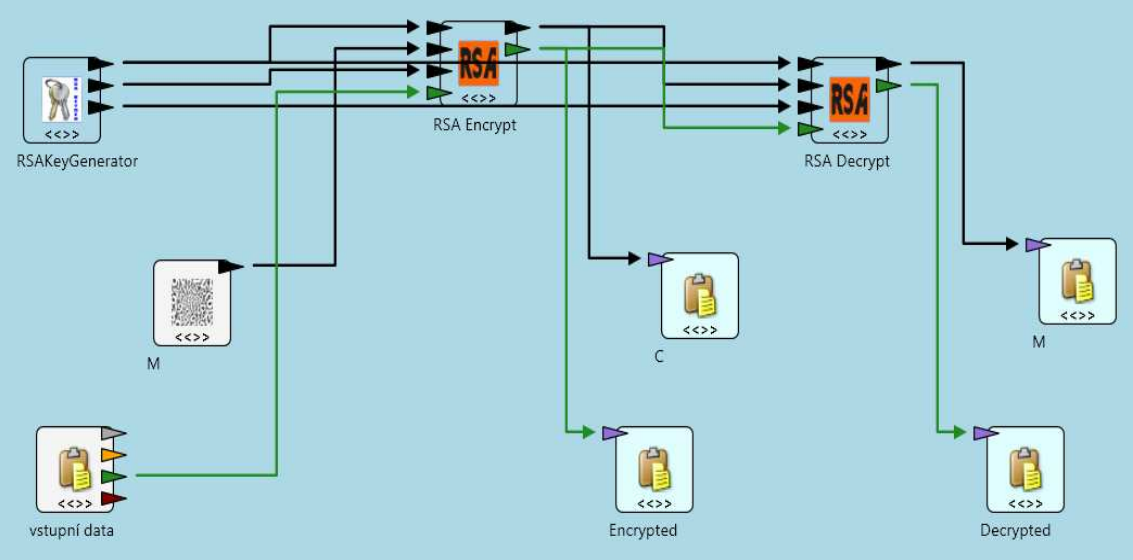
Šifrovací algoritmus PRESENT



Obr. 4.6: Schéma šifrování pomocí algoritmu PRESENT

Při šifrování analyzovaných dat algoritmem PRESENT došlo ke shodě vstupních a výstupních dat, což znamená, že v analyzovaných datech nedošlo k žádné změně. Ke změně přenášených zašifrovaných dat by mohlo dojít např. při zásahu do přenosu a pokusu změnit přenášená data apod. Shodnost dat je dána vlastnostmi tohoto algoritmu, který data šifruje do bloků o velikosti 64 bitů a pro zabezpečení využívá klíče délky 80 nebo 128 bitů. Ovšem šifrovací algoritmus PRESENT byl vyvinut spíše jako šifra pro streamové aplikace. Algoritmus PRESENT je tedy spíše nevhodný k šifrování přenášených dat z měřičů kvality elektrické energie, z důvodu menší velikosti bloku pro data a délky zabezpečovacího klíče.

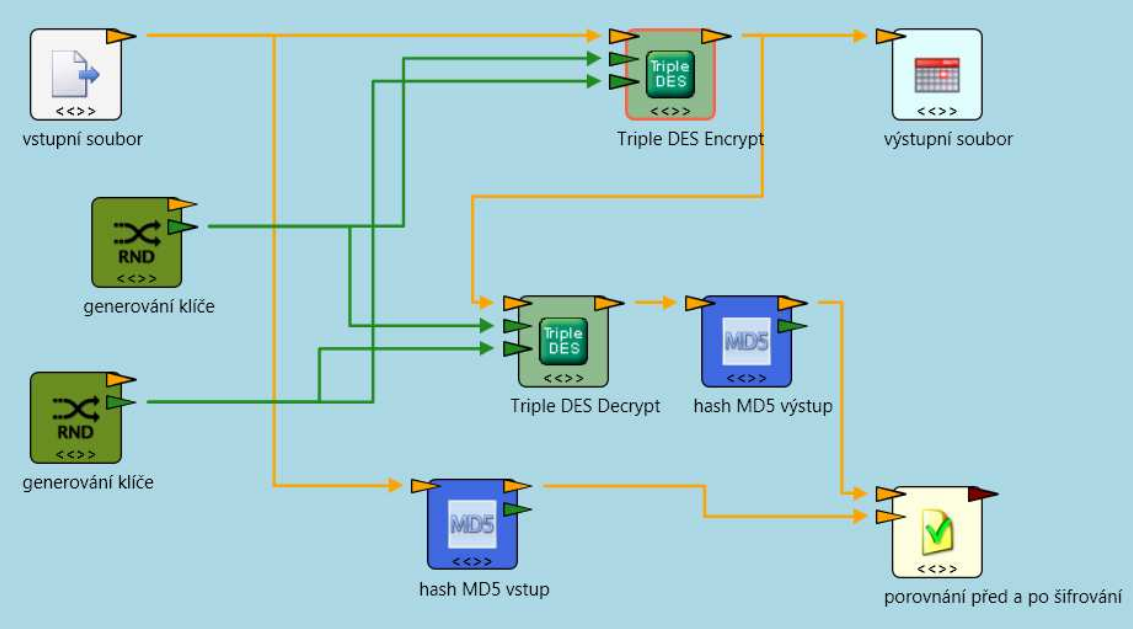
Šifrovací algoritmus RSA



Obr. 4.7: Schéma šifrování pomocí algoritmu RSA

Při šifrování všech typů analyzovaných dat byla data před i po šifrování shodná, což znamená, že nedošlo k žádné změně dat při šifrování. To je dáno odolností vůči kryptoanalýze tohoto algoritmu spočívající na obtížnosti problému faktorizace. Velkou nevýhodou šifrovacího algoritmu RSA je, že při šifrování větších souborů (stovky kB a větší) je doba šifrování a dešifrování poměrně dlouhá, proto se dá použít pouze pro šifrování malých souborů. Tuto nízkou provozní rychlost způsobuje nutnost operací s velmi velkými čísly, aby byla zaručena dostatečná bezpečnost algoritmu.

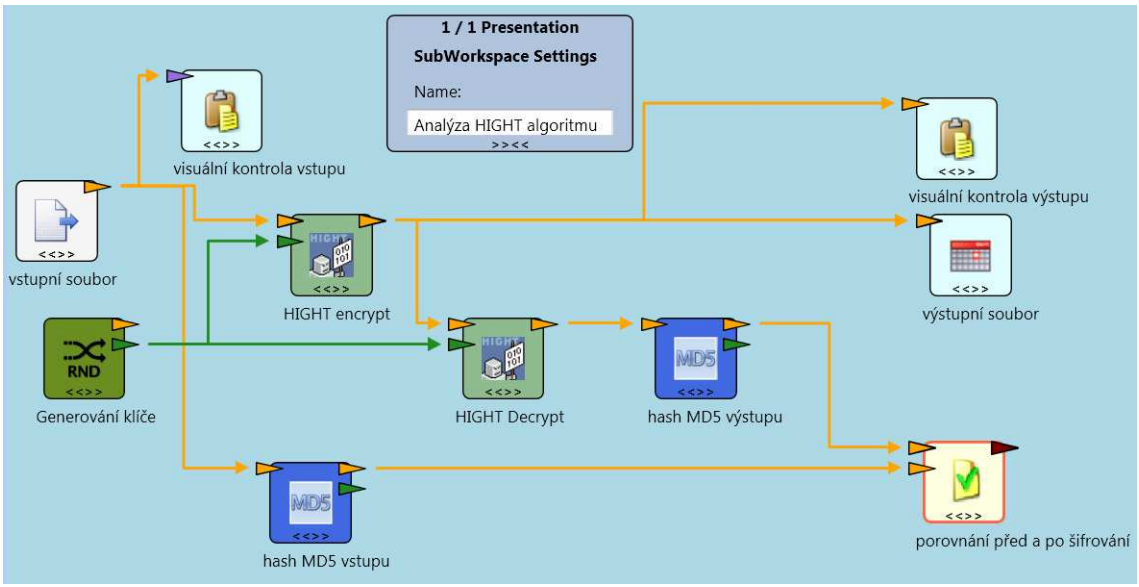
Šifrovací algoritmus 3DES (TripleDES)



Obr. 4.8: Schéma šifrování pomocí algoritmu 3DES

Při testování šifrovacího algoritmu 3DES byly postupně šifrovány všechny druhy analyzovaných dat. Po porovnání dat před a po šifrování bylo zjištěno, že se šifrovaná data shodují, což znamená, že nedošlo k žádné změně šifrovaných dat. Tento výsledek je dán vlastnostmi algoritmu 3DES, který šifruje data pomocí 168 bitů dlouhého šifrovacího klíče, který zajistí dostatečnou bezpečnost dat při přenosu. Oproti algoritmu AES je 3DES daleko pomalejší, což je dáno tím, že AES je novějším typem šifrovacího algoritmu.

Šifrovací algoritmus HIGHT



Obr. 4.9: Schéma šifrování pomocí algoritmu HIGHT

Při šifrování analyzovaných dat algoritmem HIGHT došlo ke shodě vstupních a výstupních dat, což znamená, že v analyzovaných datech nedošlo k žádné změně. To je dáno vlastnostmi tohoto algoritmu, který data šifruje do bloků o velikosti 64 bitů a pro zabezpečení využívá klíče délky 128 bitů. Ke změně přenášených zašifrovaných dat by mohlo dojít např. při zásahu do přenosu a pokusu změnit přenášená data apod. Šifrovací algoritmus HIGHT byl vyvinut spíše jako šifra pro aplikace s nízkými nároky. Algoritmus HIGHT je tedy spíše nevhodný k šifrování přenášených dat z měřičů kvality elektrické energie, z důvodu menší velikosti bloku pro data a délky zabezpečovacího klíče.

4.3 Výsledná šifrovací metoda

Tab. 4.3: Vyhodnocení použitelnosti šifrovacích algoritmů

algoritmus	**přenášený soubor**	
	malý (jednotky kB)	**velký (desítky až jednotky MB)**
AES	vhodný	vhodný
PRESENT	použitelný	použitelný
RSA	vhodný	nevhodný
3DES	vhodný	vhodný
HIGHT	použitelný	použitelný

Z uvedené tabulky je patrné, že pro zabezpečení přenášených dat z měřičů kvality elektrické energie by bylo možné použít téměř všechny testované šifrovací algoritmy. Po vyhodnocení je nejméně vhodný šifrovací algoritmus RSA, který není vhodný pro přenos větších souborů z důvodu pomalého šifrování takových souborů, čímž by

nebyl zaručen rychlý a bezpečný přenos naměřených údajů. Šifrovací algoritmus PRESENT byl vyvinut spíše pro streamové aplikace a ani jeho vlastnosti nejsou pro rychlý přenos a zabezpečení přenášených dat z měřičů kvality elektrické energie příliš dostačující. Podobné parametry nabízí šifrovací algoritmus HIGHT, tudíž ani tento algoritmus není příliš vhodný pro zabezpečení přenášených dat. Dalšími testovanými šifrovacími algoritmy byly algoritmus AES a 3DES. Tyto dva algoritmy mají velmi podobné vlastnosti, které by byly schopny zaručit bezpečný a rychlý přenos pro naměřená data. Výhodou šifrovacího algoritmu AES proti algoritmu 3DES je mnohem větší rychlost šifrování dat. Z těchto poznatků je zřejmé, že nejvhodnějším šifrovacím algoritmem pro data vyskytující se v energetické síti je šifrovací algoritmus AES. Jedná se o velmi rozšířený a bezpečný algoritmus, který šifruje data do bloků o velikosti 128 bitů a délka šifrovacího klíče může být 128, 192 nebo až 256 bitů. Navíc se šifra vyznačuje vysokou rychlostí šifrování.

5 MĚŘENÍ KVALITY ELEKTRICKÉ ENERGIE

Metody měření výše uvedených charakteristik napětí (viz str. 12) jsou popsány v souhrnné normě [7]. Dále existují další standardy [4], [5], [6] a [8], které nejen popisují jednotlivé charakteristiky napětí, ale také jejich měřící metody. Je samozřejmé, že k prokazování charakteristik kvality napětí je na trhu k dispozici řada měřících přístrojů. K vyhodnocení a správné interpretaci jimi naměřených výsledků je však nutná znalost nejen jejich obsluhy, ale především znalost problematiky příslušné charakteristiky kvality napětí.

5.1 Popis měření základních charakteristik napětí

Mezi základní charakteristiky napětí patří kmitočet, velikost a odchylka napájecího napětí.

Kmitočet napětí

Podle normy ČSN EN 50160 se měří kmitočet napájecího napětí v intervalu 10 s. Protože za interval 10 s nemusí být počet cyklů celé číslo, měří se při přesném měření kmitočtu počet a doba trvání všech ukončených cyklů a z těchto dvou hodnot je vypočten kmitočet pro daný interval 10 s. Ne více než 0,5% intervalů 10 s za 1 rok, to je 15778, smí mít u systémů se synchronním připojením kmitočet mimo rozmezí 49,50 Hz až 50,50 Hz a žádná hodnota kmitočtu nesmí překročit meze 47,00 Hz a 52,00 Hz. Dovolená nejistota měření frekvence je 10 mHz. U systémů bez synchronního připojení je pro 95% intervalů za 1 týden dovoleno kmitočtové rozmezí 49 Hz až 51 Hz a žádná hodnota kmitočtu nesmí překročit hranice 42,5 Hz a 57,5 Hz. Měření kmitočtu se děje na tzv. referenčním kanále, obvykle napětí U_1.

Velikost napájecího napětí

Hodnota napětí se měří v časovém intervalu 10 cyklů pro síť s kmitočtem 50 Hz. Měří se pravá efektivní hodnota - TrueRMS, přičemž pro přístroje třídy A se požaduje v měřícím rozsahu 0 až 2 x U_{jm} nejistota měření 0,1% U_{jm}. Přístroje třídy B musí měřit napětí s nejistotou lepší než 0,5% U_{jm}.

Odchylky napájecího napětí

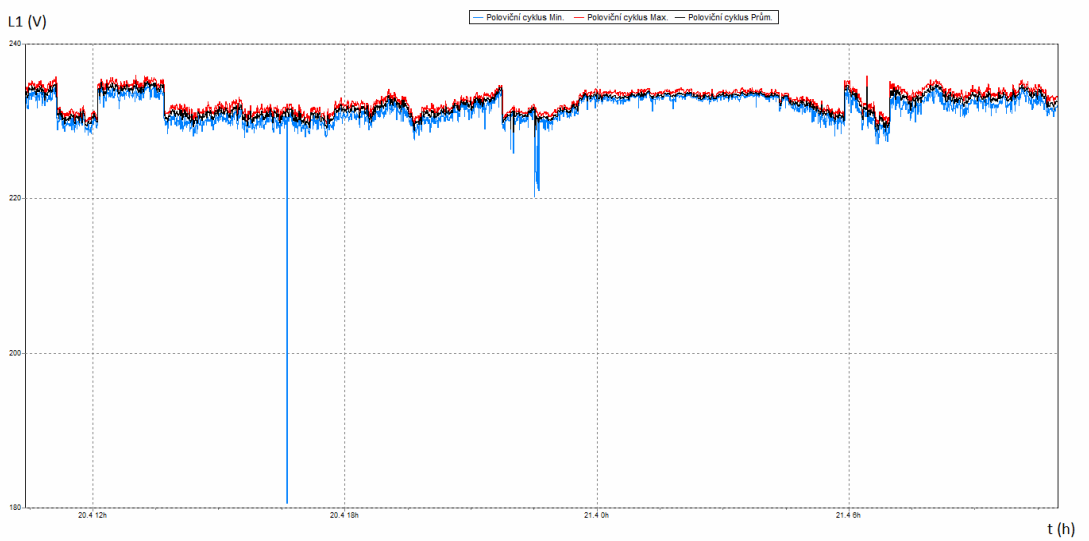
Za normálních provozních podmínek musí být více než 95% průměrných efektivních hodnot napětí změřených v deseti minutových intervalech jednoho týdne v rozsahu U_{jm}+6%,−10%. Deseti minutová průměrná hodnota se vypočte ze 3000 hodnot napětí změřených za 10 period (0,2 s). 95 procentní kriterium znamená, že 95% tj. 958 desetiminutových intervalů týdne, kterých je celkem 1 008, musí mít průměrná napětí v toleranci 207,0 V až 243,8 V. Žádná 10 minutová hodnota napětí nesmí na nn vedeních normální délky překročit 230 V + 10%, -15% tj. 195,5 V až 253 V.

5.2 Měření kvality napětí přístrojem FLUKE VR1710

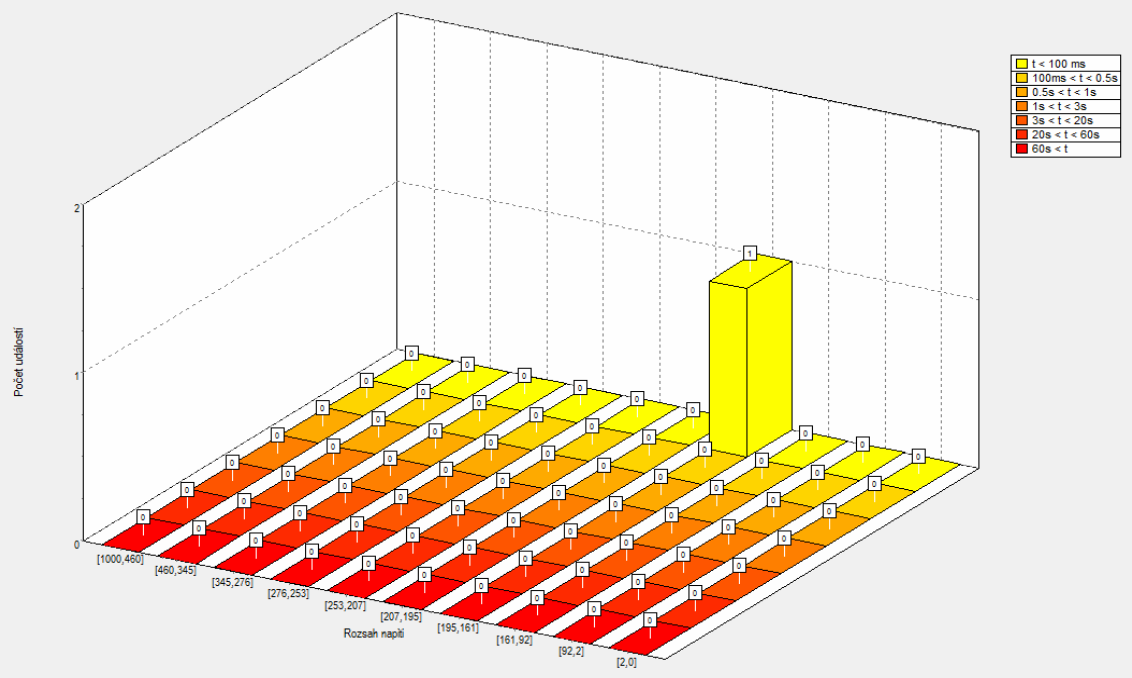
Fluke VR1710 je jednofázový záznamník kvality energie, který poskytuje rychlý a jednoduchý záznam průběhu napětí, výpadků, harmonických kmitů a obecně kvality elektrické energie včetně poklesů a přepětí. Sleduje a zaznamenává síťové napětí, měří průměr RMS, min. a max. hodnoty a kontroluje, zda je ze zásuvky dodáváno napětí v toleranci. Měří frekvenci a harmonické kmity a kontroluje, zda zkreslená zátěž (systémy UPS, pohony, atd.) ovlivňují jiná zařízení. Umožňuje měření flickeru (mihotání světel), čili stanovuje působení spínacích zařízení na systémy osvětlení. Zaznamenává napěťové přechodové jevy – zachycuje ty jevy, které se vyskytují občas, přechodné jevy, které mohou mít vliv na zařízení (je zachycena celá křivka s datem, údajem o čase a době trvání). Dále zaznamenává harmonické kmity až do 32. harmonické. Lze nastavit průměrnou zaznamenávací dobu v rozmezí od 1 sekundy do 20 minut podle typu měření (krátkodobá nebo dlouhodobá) a celkový čas záznamu může být až 339 dnů.

Praktické měření bylo provedeno dlouhodobě od 20.4.2010 10:24:51 hod. do 21.4.2010 10:57:35 hod., fáze byla během dne zatížena spotřebiči jako počítač, notebook, stolní lampička, tiskárna) a v noci byla fáze téměř bez zatížení.

Na Obr. 5.1 je zobrazen průběh napětí v závislosti na čase. Z grafu je patrné, že po většinu měření se hodnota napětí pohybovala na hodnotě 230 V. V určitých okamžicích došlo k mírnému snížení nebo zvýšení hodnoty napětí od hodnoty 230 V. Průměrná hodnota napětí byla naměřena 232,249 V, minimální hodnota napětí 180,63 V a maximální hodnota napětí 236 V. Průměrná i maximální hodnota napětí je v toleranci podle normy [3]. V grafu je také patrné, že 20.4.2010 v čase 16:36:59 hod. došlo ke značnému poklesu minimální hodnoty napětí na hodnotu 180,625 V. Minimální hodnota napětí dokonce překročila maximální povolenou odchylku napájecího napětí definovanou normou [3], která je 207 V. Pokles trval méně než 100 ms, jak ukazuje Obr. 5.2. Takový pokles mohl být způsoben velkým zvětšením odběru elektrické energie v daný časový okamžik.

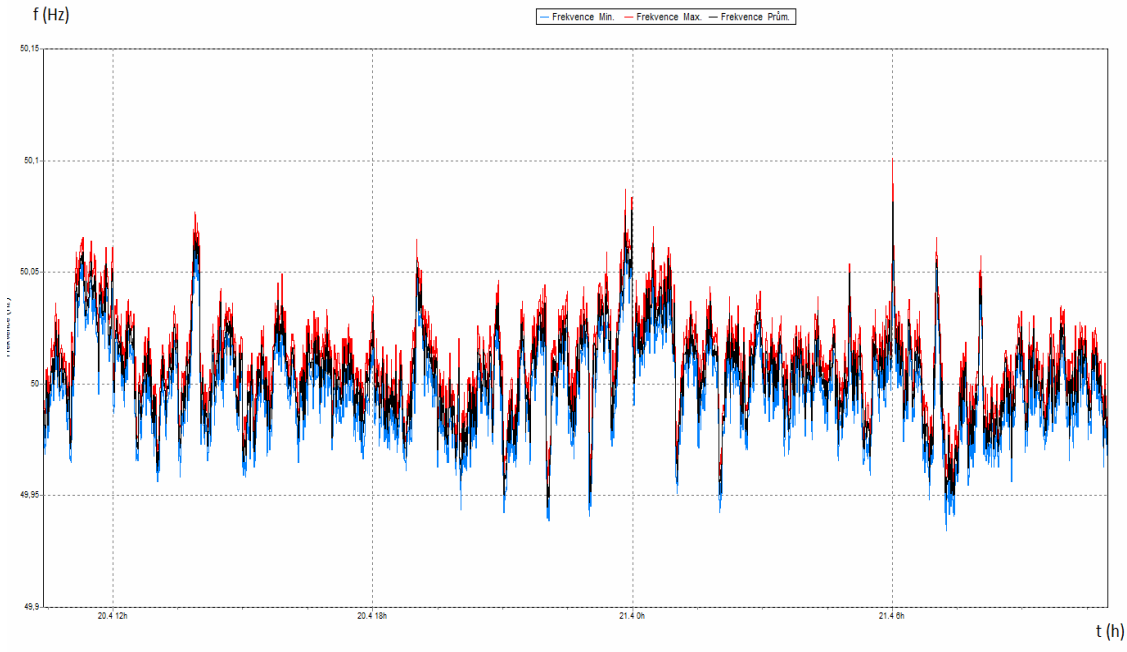


Obr. 5.1: Průběh napětí v závislosti na čase



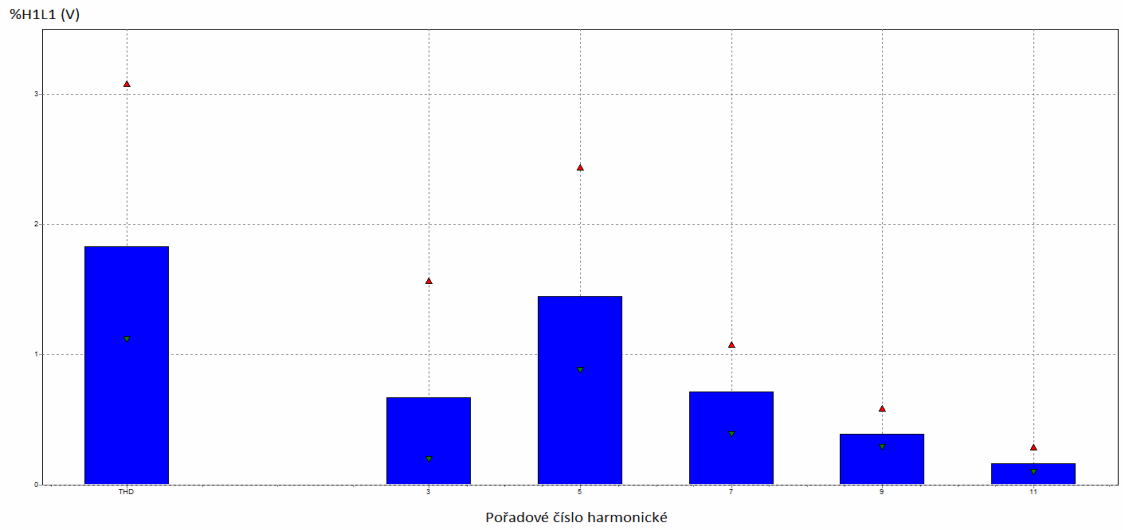
Obr. 5.2: Poklesy a nadměrná napětí

Na Obr. 5.3 je zobrazen průběh kmitočtu v závislosti na čase. Z průběhu je vidět, že se kmitočet po většinu měření pohyboval těsně kolem 50 Hz. Minimální kmitočet byl naměřen 49,934 Hz a maximální kmitočet 50,101 Hz. Všechny naměřené hodnoty byly v toleranci s normou [3], což odpovídá požadovaným předpokladům. Z tohoto grafu vyplývá, že kmitočet se během měření nijak výrazně neměnil.



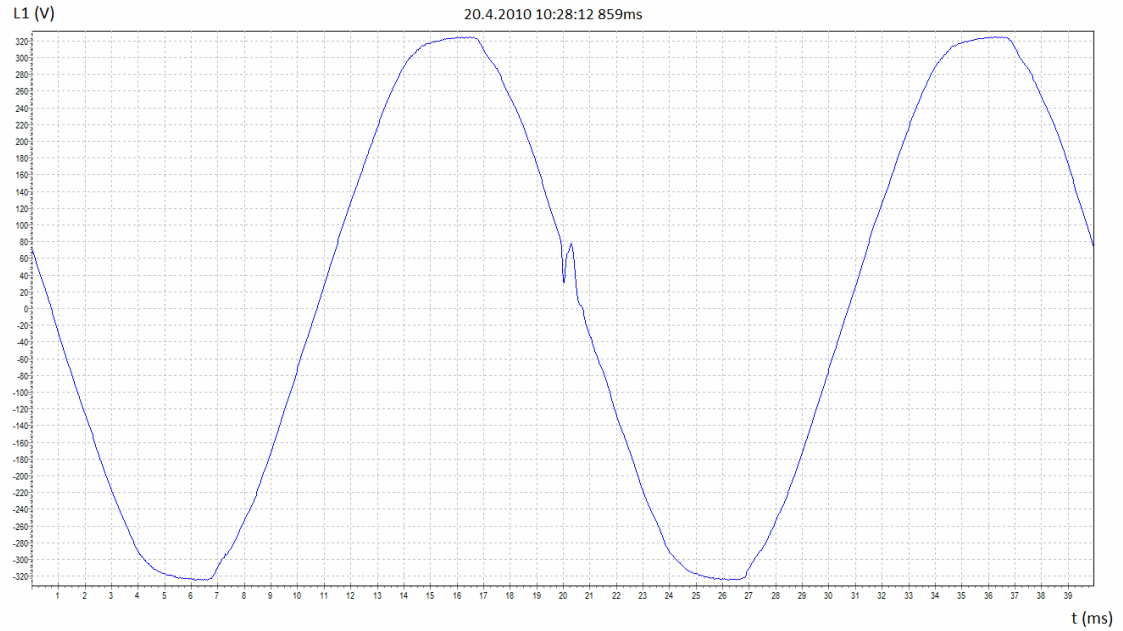
Obr. 5.3: Průběh kmitočtu v závislosti na čase

Na následujícím obrázku je vidět vzniklé vyšší harmonické kmity, které jsou generovány zpět do energetické sítě. V průběhu měření došlo ke vzniku až 25. harmonické. Velikost vzniklých harmonických je v toleranci s normou [3], která uvádí, že maximální povolená hodnota THD musí být v nn sítích menší nebo roven 8,0% U_{jm}.



Obr. 5.4: Harmonické kmity

Na posledním obrázku je zobrazen vzniklý napěťový přechodný jev, který nastal 20.4.2010 10:28:12. Při tomto napěťovém přechodném jevu se amplituda napětí zvýšila přibližně na hodnotu 323 V a jev trval 859 ms. Tyto hodnoty jsou v toleranci s normou [3].



Obr. 5.5: Průběh vzniklého přechodného jevu

ZÁVĚR

Pro měření kvality elektrické energie je nutné znát, jaké parametry se dají měřit. Jako výchozí hodnoty pro porovnání získaných výsledků měření slouží normy. Český normalizační institut popisuje, jaké veličiny lze vyhodnocovat a v jakých mezích se dané veličiny mají pohybovat. Norma [3] definuje základní charakteristiky napětí elektrické energie, které jsou popsány v první kapitole.

V druhé a třetí kapitole je zmíněno několik způsobů přenosu naměřených dat a metody zabezpečení přenášených dat. Prvním ze způsobů přenosu dat je využití Internetu nebo Ethernetu. Odečtená data jsou odeslána z měřícího zařízení pomocí sběrnice RS232 do komunikační jednotky, která je poté odešle pomocí protokolu TCP/IP do sběrové centrály. Pro zabezpečení přenášených dat po Internetu nebo Ethernetu je nejvhodnější použít symetrické blokové šifry AES. Výhodou této šifry je vysoká rychlost šifrování a dobrá odolnost proti neoprávněným přístupům k datům. V dnešní době by tento způsob přenosu dat neměl být problém, protože Internet je dostupný téměř kdekoli. Problémem by mohly být útoky ze strany hackerů a tím znehodnocování naměřených údajů. Další technologií použitelnou pro přenos dat z měřičů kvality elektrické energie je GSM resp. datové služby GPRS dostupné v GSM. GPRS v kombinaci s kódovým schématem CS-1 nabízí dobré zabezpečení pro přenášená data a dostačující přenosové rychlosti vzhledem k přenášeným objemům dat z měřičů kvality el. energie. Částečnou nevýhodou GPRS může být dostupnost signálu v určitých oblastech, i když v dnešní době je pokrytí signálem velmi dobré. Poslední rozebranou technologií pro přenos dat je přenos dat pomocí silnoproudých sítí technologií PLC. Pro přenos dat z měřičů kvality el. energie je používán úzkopásmový PLC systém využívající úzkopásmové modulace. Tyto systémy mají nízkou úroveň rušení, ale pomalejší rychlosti přenosu, ovšem vzhledem k přenášeným objemům dat z měřičů kvality el. energie jsou tyto rychlosti dostačující. Velkou výhodou u PLC je využití energetických rozvodů el. energie jako přenosového média, které patří celosvětově mezi nejrozšířenější síť. Nevýhodou při praktické realizaci je odlišnost silových rozvodů v různých zemích a vznik různých dějů (např. rušení) v napájecí síti. Pro zabezpečení přenášených dat v silnoproudých sítích je nejvhodnější použít symetrické blokové šifry AES, která má vysokou rychlost šifrování a dobrou odolnost proti neoprávněným přístupům.

Ve čtvrté kapitole je provedena analýza dat z měřičů kvality elektrické energie a následně vyhodnoceno zabezpečení pro jednotlivé typy dat. Analýza dat byla provedena pomocí programu Wireshark. Analyzovaná data byla získána měřením na měřícím přístroji PQ monitor MEg 33. Měření bylo provedeno dlouhodobě na fázi, na kterou jsou napojeny zásuvky v bytě panelového domu. Naměřené hodnoty napětí, kmitočtu, flickeru a vzniklých harmonických kmitů byly v toleranci s normou [3]. Při měření také došlo ke dvěma přerušením napětí. Obě přerušení trvala dohromady 15 sekund. Následně je provedena analýza naměřených dat. Výsledky analýza jsou takové, že analyzovaná data lze rozdělit na dva typy - data pro zjišťování a nastavování parametrů měřícího přístroje a data nesoucí již naměřené konkrétní hodnoty z měřícího přístroje. K vyhodnocení nejvhodnějších šifrovacích metod pro zabezpečení přenášených dat z měřičů kvality elektrické energie byl použit software CrypTool 2. Testování bylo provedeno na pěti různých šifrovacích algoritmech - AES, PRESENT, RSA, 3DES a HIGHT. Ze získaných výsledků je patrné, že nejvhodnějším šifrovacím algoritmem je

algoritmus AES, který je spolehlivý při šifrování malých i velkých souborů. Vyznačuje se vysokou rychlostí šifrování, spolehlivostí a výborným zabezpečením přenášených dat. Naopak nejméně vyhovujícím algoritmem z uvedených je algoritmus RSA, který by bylo možné použít pouze pro zabezpečení malých souborů, protože při šifrování velkých souborů je pomalý.

V poslední kapitole je popsáno měření kvality elektrické energie a zpracováno praktické měření kvality elektrické energie pomocí záznamníku kvality Fluke VR1710. Měření bylo provedeno dlouhodobě na fázi el. vedení, která byla zatížena během dne počítačem, notebookem, stolní lampičkou a tiskárnou. Průměrná hodnota napětí se pohybovala kolem 233 V. V určitém časovém okamžiku došlo k výraznému poklesu minimální hodnoty napětí na hodnotu 180,625 V. Tato hodnota překročila maximální povolenou odchylku napětí definovanou normou [3]. Maximální hodnota napětí byla naměřena 236 V, což je v toleranci podle normy. Závislost kmitočtu na čase ukazuje, že kmitočet se v průběhu měření nijak výrazně neměnil a jeho průměrná hodnota se pohybovala těsně kolem 50 Hz, což je v toleranci s normou [3]. Dalším naměřeným parametrem jsou harmonické kmity (vyšší harmonické), které jsou generovány zpět do energetické sítě. V průběhu měření došlo ke vzniku až 25. harmonické. Posledním naměřeným parametrem byl napěťový přechodný jev, který nastal 20.4.2010 10:28:12. Při tomto napěťovém přechodném jevu se amplituda napětí zvýšila přibližně na hodnotu 323 V a jev trval 859 ms. Hodnoty tohoto napěťového přechodného jevu jsou v toleranci s normou.

Při srovnání většiny naměřených charakteristik napětí s hodnotami a tolerancemi uvedenými v normě [3] je patrné, že naměřené charakteristiky napětí jsou v daných tolerancích uvedených v normě [3]. Jedinou výjimkou je minimální hodnota napětí, jejíž hodnota přesáhla normou povolenou maximální odchylku napájecího napětí. Tato nepovolená odchylka napětí v elektrické síti by mohl být způsobena velkým zvětšením odběru elektrické energie v daný časový okamžik nebo např. sepnutím velmi výkonného spotřebiče v daný časový okamžik.

LITERATURA

[1] BIGELOW, Stephen J. Mistrovství v počítačových sítích : Správa, konfigurace, diagnostika a řešení problémů. 1.vyd. Brno : Computer Press, 2004. 990 s. ISBN 80-251-0178-9.

[2] BURDA, Karel. Bezpečnost informačních systémů : skripta. Brno : FEKT VUT v Brně, 2005. 104 s.

[3] ČSN EN 50160 : Charakteristiky napětí elektrické energie dodávané z veřejné distribuční sítě. červen 2000.

[4] ČSN EN 61000-4-11 : Krátkodobé poklesy napětí, krátká přerušení a pomalé změny napětí. březen 2005.

[5] ČSN EN 61000-4-15 : Měřič blikání – specifikace funkce a dimenzování. červenec 1999.

[6] ČSN EN 61000-4-27 : Nesymetrie – zkouška odolnosti. září 2001.

[7] ČSN EN 61000-4-30 : Metody měření kvality energie. leden 2004.

[8] ČSN EN 61000-4-7 : Všeobecná směrnice o měření a měřících přístrojích harmonických a meziharmonických pro rozvodné sítě a zařízení připojovaná do nich. červenec 2003.

[9] E.ON (Parametry elektřiny – vlastnosti výrobku) [online]. 2009 [citováno 2009-12-09]. Dostupné z WWW: < http://www.eon.cz/cs/info/parameters.shtml >

[10] Energetický regulační úřad, Pravidla provozování distribučních soustav. listopad 2005.

[11] MEgA Měřící Energetické aparáty: PQ monitor: MEg30, MEg31, MEg32 a MEg33. 2006. Online: <http://e-mega.cz/doc/pqmonitor_mail.pdf>

[12] NĚMEC, Karel. Datová komunikace : skripta. Brno : FEKT VUT v Brně, 2007. 172 s.

[13] NĚMEC, Marek. Síť skrze zásuvku [online]. 10/2003 [citováno 2009-12-09]. Dostupné z WWW: < http://www.zive.cz/clanky/sit-skrze-zasuvku/sc-3-a-114358/default.aspx >

[14] NOVOTNÝ, Vít. Architektura sítí : skripta. Brno : FEKT VUT v Brně, 2002. 136 s.

[15] RICHTR, Tomáš. Technologie pro mobilní komunikace [online]. 1/2002 [citováno 2009-12-09]. Dostupné z WWW: < http://tomas.richtr.cz/mobil/gsm-hs.htm >

SEZNAM ZKRATEK, VELIČIN A SYMBOLŮ

AES	Advanced Encryption Standard
AMM	Automated Meter Management
AMR	Automated Meter Reading
ATM	Asynchronous Transfer Mode
CDMA	Code Division Multiple Access
CENELEC	Evropský výbor pro elektrotechnickou standardizaci
CS	Code Scheme
CSD	Circuit Switched Data
DES	Data Encryption Standard
ECSD	Enhanced CSD
EDGE	Enhanced Data rates for Global Evolution
EGPRS	Enhanced GPRS
FDM	Frequency Division Multiplexing
FSK	Frequency Shift Keying
GMSK	Gaussian Minimum Shift Keying
GPRS	General Packet Radio Service
GSM	Globální Systém pro Mobilní komunikaci
HDO	hromadné dálkové ovládání
HLR	Home Location Register
HSCSD	High Speed Circuit Switched Data
IEEE	Institute of Electrical and Electronics Engineers
IP	Internet Protocol
LAN	Local Area Network
MAC	Media Access Control
MAN	Metropolitan Area Network
MCS	Modulation and Code Scheme
NMT	Nordic Mobile Telephone
nn	nízké napětí
NRZI	Non Return to Zero
OFDM	Orthogonal Frequency-Division Multiplexing
PLC	Power Line Communication

P_{lt}	dlouhodobý flikr
PQ monitor	Power Quality monitor
PSK	Phase Shift Keying
P_{st}	krátkodobý flikr
QoS	Quality of Service
RC	Rivest Cipher
RMS	Root Mean Square
SGNS	Serving GPRS Support Node
TCP	Transmission Control Protocol
TDM	Time Division Multiplex
TDMA	Time Division Multiple Access
THD	Total Harmonic Distortion
U_{jm}	jmenovité napětí
UMTS	Universal Mobile Telecommunication System
UPS	Uninterruptible Power Supply
USB	Universal Seriál Bus
UTP	Unshielded Twisted Pair
U_Z	nesymetrie napětí
vn	vysoké napětí
vvn	velmi vysoké napětí
WAN	Wide Area Network