Univerzita Hradec Králové
Fakulta informatiky a managementu
Katedra informačních technologií

Monitoring průmyslových sítí v energetice

Bakalářská práce

Autor: Vojtěch Hájek
Studijní obor: Aplikovaná informatika

Vedoucí práce: Ing. Ondřej Hornig

Hradec Králové duben 2017

Prohlášení:

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

.....

V Hradci Králové dne 27.4.2017 Vojtěch Hájek

Poděkování:

Děkuji vedoucímu bakalářské práce Ing. Ondřeji Hornigovi, za metodické vedení práce a praktické poznámky a připomínky.

Anotace

Cílem práce je představit prostředí průmyslového Ethernetu, průmyslové protokoly a jejich využití v síti Ethernet, odůvodnění, proč je v průmyslových datových sítích nezbytná redundance v komunikaci. Jsou představeny protokoly k dosažení konvergence v síti. Důraz je kladen na také na synchronizaci zařízení v síti, jejich fyzickou odolnost vůči okolním podmínkám v souladu s normou IEC 61850. Nejsou opomenuty ani nástroje pro monitoring, jak obecné, využitelné také v běžném kancelářském prostředí, tak specializované do průmyslového prostředí normy IEC 61850. Praktické měření je zaměřeno na výběr nejlepšího protokolu k rychlé konvergenci v síti se zařízeními od různých výrobců tak, aby došlo k nejmenšímu výpadku v síti.

Annotation

Title: Network monitoring at energy industry

This work aquaints with a space of industrial Ethernet, an industrial procedure and a reason why to use them. It also contains an explanation of using reductance in communication. There are procedures of a convergence in network. Synchronization of a device in network is very important. It informs about a physical resistence to a vinicity in corresponcence with a norm IEC 61850. It includes implements for monitoring – common ones which could be used in an usual office and also the special ones for an industrial beckground of a norm IEC 61850. Select the best procedure from different producers for a fast convergence in network without drops out is the aim.

Obsah

1 Úvod ... 1
2 Cíl práce a metodika ... 2
3 Průmyslové datové sítě ... 3
3.1 Počítačová síť ... 3
3.2 Počátky průmyslového Ethernetu ... 4
3.3 Referenční model ISO/OSI ... 4
3.4 Ethernet ... 5
3.5 Zapouzdřování dat ... 6
3.6 Fyzická vrstva Ethernetu ... 6
3.6.1 Technické provedení průmyslového Ethernetu ... 7
3.6.2 Zařízení v síti ... 10
3.7 Linková vrstva ... 10
3.8 Síťová vrstva ... 11
3.8.1 IPv4 ... 12
3.8.2 IPv6 ... 14
3.8.3 ICMP ... 14
3.9 Transportní vrstva ... 15
3.10 Aplikační vrstva ... 16
4 Smart Grid ... 17
4.1 Topologie Smart Grid sítí ... 18
4.2 Bezpečnost energetických sítí ... 18
5 Protokoly průmyslového Ethernetu ... 20
5.1 Proč Ethernet do průmyslu? ... 20
5.2 Modbus ... 21
5.3 EtherNet/IP ... 21

5.3.1 Model producent-consumer 22
5.3.2 CIP 22
5.3.3 Bepečnost CIP 23
5.4 EtherCAT 23
5.5 Profinet 24
5.5.1 Práce v reálném čase 24
5.6 IEC 61850 25
5.6.1 Struktura IEC 61850 27
5.6.2 GOOSE 30
5.6.3 GSSE 31
5.6.4 MMS 31
5.7 IEC 60870-5-101 31
5.8 IEC 60870-5-104 32
5.9 DNP3 32
6 Nástroje monitoringu 33
6.1 SNMP 33
6.1.2 Typy SNMP objektů 35
6.1.3 MIB 36
6.1.4 Hodnoty v databázi 36
6.1.5 Problémy použití SNMP 37
6.2 Wireshark 37
6.3 Syslog 37
6.3.1 SIEM 39
6.4 Průmyslové controllery a testery 40
6.5 SCADA 41
7 Měření konvergence v heterogenních přepínaných sítích 42

7.1 Princip RSTP....42
7.1.1 BPDU....44
7.1.2 Proposal agreement systém v RSTP....45
7.2 Simulace IED....46
7.3 Měření....48
8 Shrnutí výsledků....52
9 Závěr....53
10 Seznam použité literatury....55

Seznam obrázků

Obrázek 1: Konceptuální model sítí Smart Grid, vlastní zpracování podle [18]. 18
Obrázek 2: Rozdíl mezi PDU a PDU Modbus, zdroj: [24]. 21
Obrázek 3: Možnosti označení portů u RSTP, zdroj: vlastní podle [61]. 44
Obrázek 4: Proposal/Agreement systém, zdroj: vlastní zpracování. 46
Obrázek 5: Testovaná topologie.....49

Seznam tabulek

Tabulka 1: Porovnání ISO/OSI a Ethernet model..... 6
Tabulka 2: Zprávy Syslog.....38
Tabulka 3: Výpadky GOOSE zpráv a ICMP. 50
Tabulka 4: Výpadky GOOSE a ICMP zpráv při použití RSTP. 51

Seznam zkratek

ADU..... Application Data Unit

ASCI ..... Abstract Communication Service Interface

ASIC ..... Application Specific Integrated Circuit

BPDU..... Bridge Protocol Data Unit

CIP..... Common Industrial Protocol

CLI..... Command Line Interface

CRC ..... Cyclic redundancy check

CSMA/CD..... Carrier Sense Multiple Access with Collision Detection

ČSN ..... Česká technická norma

ČEZ..... České energetické závody

DCE ..... data circuit-terminating equipment

DCS..... distributed control system

DNP3 ..... Distributed Network Protocol

DTE ..... Data terminal equipment

EN..... Evropská norma

Ethernet/IP ..... Ethernet/Industrial Protocol

FCS ..... frame check sequence

GNU..... GNU is Not UNIX

GOOSE..... Gerneric Object-Oriented Sbustation Event

GPL..... General Public License

GSSE ..... Generic Substation State Events

I/O..... Input/Output

ICMP..... Internet Control Message Protocol

ICS/SCADA..... Internet Caching Systém/Supervisory Control And Data Acquistion

IEC..... International Electrotechnical Commission

IEC/TS ..... International Electrotechnical Commission/Technical Specifications

IED ..... Intelligent electronic device

IEEE..... Institute of Electrical and Electronics Engineers

IoT..... Internet of Things

IP..... Internet Protocol

IPv4 ..... Internet Protocol version 4

IPv6 ..... Internet Protocol version 6

IPX..... Internetwork Packet Exchange

IRT ..... Isochronous Real Time

ISO/OSI ..... International Organization for Standardization/Open Systems Interconnection

L3..... Layer3

MAC ..... Media Access Control

MES..... Managed ethernet switch

MIB ..... Management Information Base

MMS..... Manufacturing Message Specification

MST..... Multiple Spanning Tree Protocol

MTU..... Maximum transmission unit

NAT..... Network Address Translation

NTP ..... Network Time Protocol

ODVA..... Open DeviceNet Vendor Association

OID..... Object Identifier

PDU..... Protocol Data Unit

PLC..... Programmable Logic Controller

PoE..... Power over Ethernet

PTP..... Precision Time Protocol

PVST ..... Per VLAN Spanning Tree

PVST+ ..... Per VLAN Spanning Tree Plus

RFC..... Request For Comments

RPVST+ ..... Rapid Per VLAN Spanning Tree Plus

RSTP..... Rapid Spanning Tree Protocol

R-T ..... Real-Time

RTT ..... Round Time trip

RTU..... Remote Teminal Unit

Rx..... Recieve

SCADA..... Supervisory Control And Data Acquistion

SCADA/HMI..... Supervisory Control And Data Acquistion/human machine interface

SCL..... Substion configuration language

SEM..... Security Event Management

SIEM..... Security Information and Event Management

SIM..... Security Information Management

SNMP..... Simple Network Management Protocol

SSH..... Secure Shell

SPAN..... Switched Port Analyzer

STP..... Spanning Tree Protocol

TCP/IP..... Transmission Control Protocol/Internet Protocol

TTL..... Time-to-Live

Tx..... Transmission

UDP..... User Datagram Protocol

VLAN..... Virtual Local Area Network

VPN..... Virtual Private Network

XML..... Extensible Markup Language

1 Úvod

V dnešní době je nejvíce rozšířená síťová komunikace. A to jak v domácnostech, tak firmách. Síťová komunikace se nevyužívá pouze v kancelářském prostředí, ale také v prostředí průmyslu, automatizace, energetiky a dalších odvětvích. Pro zajištění správného chodu sítě je nezbytný její monitoring pro předcházení a případně řešení problémů v síti, zpravidla výpadek linky nebo síťového prvku. Pokud k takovému defektu dojde a síť není správně nakonfigurována, dochází k rozpadu komunikace v síti a ke ztrátám. Jak časovým, tak finančním a v neposlední řadě také ke hmotným. Práce je rozdělena do čtyř částí, kde je řešena problematika v síťové komunikaci. První část představuje referenční model ISO/OSI a základní komunikaci v sítích. Je zde také řešena problematika zabezpečení průmyslových a resp. energetických sítí, historie průmyslového Ethernetu a rozdíly mezi prvky Ethernetu v kancelářském prostředí a průmyslovém prostředí. Stručně je zde vystižen pojem Smart Grid a možnosti využití.

Druhá část seznamuje s vybranými automatizačními protokoly a jejich napojení na Ethernet. V kapitole je řešen především na modely komunikace v automatizaci, bezpečnosti. Velmi důležitou část tvoří problematika synchronizace zařízení v síti a komunikace v reálném čase. V této kapitole je také představen komunikační standard IEC 61850, jeho struktura, důležitost a druhy zpráv, pomocí kterých jsou přenášeny informace o stavech zařízení.

Třetí část práce se zabývá problematikou monitoringu sítí. Jak obecně, za použití běžných nástrojů jako je logování, Syslog, použití protokolů SNMP a ICMP, tak za použití SCADA systémů a kontrolérů na protokolu IEC 61850 v energetickém průmyslu.

Ve čtvrté, praktické, části je řešena problematika konvergence v redundantních sítích v průmyslovém prostředí se zařízeními různých výrobců. Důraz je kladen na výběr nejideálnějšího protokolu s nejmenší ztrátou GOOSE zpráv. Součástí měření bylo také ověření dostupnosti zařízení při výpadku linky.

Na závěr jsou nastíněna řešení, která lze brát jako doporučení již při návrhu a realizace topologie v průmyslových, energetických sítí, vyplývající z testování.

2 Cíl práce a metodika

Cílem této bakalářské práce je seznámení s průmyslovými protokoly a jejich možnosti připojení do sítě Ethernet a představení problémů v případě vypadnutí linky. Problematika konvergence sítě je zaměřena do prostředí průmyslu, konkrétně energetiky a zařízení splňující standard IEC 61850. Cílem praktické části je analyzovat a optimalizovat síť v energetickém průmyslu pomocí protokolů zamezujících redundanci v síti s ohledem na nejrychlejší konvergenci.

3 Průmyslové datové sítě

Ethernetová síť je dnes hojně používána ke spojení nebo sdílení periferií (např. tiskárny, NAS) či počítačů. K jeho dalšímu šíření přispívá i jeho popularita, kdy je pozice Ethernetu stále více podporována v roli fyzického základu internetu jako nejvýznamnějšího informačního prostředku současnosti i blízké budoucnosti [1].

3.1 Počítačová síť

Počítačová síť vzniká tehdy, když jsou spojeny minimálně dva nebo více zařízení mezi sebou za účelem sdílení zdrojů. Dnešní nejrozšířenější síť je založena na technologii Ethernet, používající protokol TCP/IP [1].
V rámci počítačové sítě lze sdílet:

- Dokumenty
- Tiskárny
- Periferie (mechaniky, hardwarové zdroje)
- Modemy

Počítačovou síť lze zjednodušeně zobrazit pomocí stromové struktury. Ve skutečnosti je však síť složitější, neboť některé linky jsou zdvojené a propojené na více místech.
Podle rozlehlosti se sítě dělí na [2]:

- LAN – Local area network – zařízení jsou spojeny v rámci budovy, firmy; nejčastěji se používá přepínaný ethernet, v době IoT a smart zařízení Wifi, dle standardu 802.11. Jsou propojeny většinou metalickými kabely, páteřní sítě mohou být propojeny optickým vláknem.
- PAN – Personal area network – sítě s malou rozlehlostí – používají se pro propojení zařízení typu mobilní telefon, tablet nebo také v automobilovém průmyslu. Vyznačují se spíše odolností rušení a mají nízkou spotřebu energie. Jako nejznámější zástupce lze uvést Bluetooth, Infračervený port, NFC.
- WAN – Wide area network – spojuje sítě LAN do internetu.
- MAN – Metropolitan Area network – v dnešní době tyto sítě využívají poskytovatelé internetu ve městech, většinou bezdrátově.

Počítačová síť je heterogenní. Je využívána k propojování zařízení od různých zařízení. Každé zařízení je opatřeno jedinečnou adresou, jedná se o MAC ID. Ve standardu IPv4 jde o 48bitovou adresu, která se uvádí v hexadecimálním tvaru, kde první tři bajty definují výrobce síťového zařízení, další tři jsou unikátní číslo zařízení. Těchto adres využívá spojová vrstva, která zajišťuje přenos dat v jedné síti Ethernet.

3.2 Počátky průmyslového Ethernetu

V druhé polovině 80. let minulého století proběhly první pokusy využití Ethernetu za účelem komunikace v průmyslových řídicích systémech. Jako příklady lze uvést Sinec H1 uvedený v katalogu společnosti Siemens AG v roce 1985. Síť byla plně kompatibilní se standardem 802.3, měla však robustnější konektory a koaxiální kabel byl důkladně odstíněn. Počátkem 90. let byl na trh uveden model Sinec H1F0. Tento model používal, kromě koaxiálního kabelu, pro prostředí, kde je silné elektromagnetické rušení optické kabely. Optické kabely se dodnes využívají také pro překlenutí dlouhých vzdáleností.

Ethernet byl podobně využit v roli systémové sběrnice v některých distribuovaných řídicích systémech, např. PLS 80E firmy Eckard.

V následujících letech byly vynaloženy velké prostředky na vývoj průmyslových sítích a tak do roku 2002-2003 byly používány pro automatizaci průmyslové sběrnice (fieldbus) a nižší prostředky komunikace (Device Bus, Sensor/Actuator Bus). Byly používané, protože Ethernet nebyl původně konstruován pro práci v reálném čase [1].

3.3 Referenční model ISO/OSI

Referenční model ISO/OSI byl vypracovaný začátkem 80. let minulého století organizací ISO jako standard ISO 7498 pro propojování heterogenních počítačových systémů [3]. V modelu jsou stanoveny podmínky, za jakých mohou účastníci přenosu spolehlivě komunikovat mezi sebou. Komunikace probíhá po sériové sběrnici. Model je otevřený, není tedy závislý na žádném firemním řešení. Model tvoří sedm vrstev, přičemž každá má za úkol přesně definované funkce. Vlastní přenos je uskutečňován mezi dvěma účastníky přenosu prostřednictvím fyzického

spoje. Důležité je, že oba účastníci mezi sebou tvoří na každé vrstvě modelu virtuální spoje. K reálnému přenosu dochází pouze na fyzické vrstvě. Pod virtuálním spojem si lze představit komunikaci účastníků na sedmé vrstvy např. prostřednictvím instant messagingu aniž by měli ponětí o funkcích nižších vrstev.
Referenční model ISO/OSI má tyto vrstvy:

1. Fyzická
2. Linková
3. Síťová
4. Transportní
5. Relační
6. Prezentační
7. Aplikační

3.4 Ethernet

Vztah Ethernetu k modelu ISO/OSI představuje spojení první a druhé vrstvy. Tyto vrstvy byly standardizovány jako standard IEEE802.3 v 80. letech. Tato vrstva funkcí odpovídá fyzické a linkové vrstvě v modelu ISO/OSI. Avšak spolu s protokoly IP na třetí vrstvě a TCP na vrstvě čtvrté. Vynechává pátou a šestou vrstvu. S aplikačními protokoly je vyjádřena sedmá vrstva. Tvoří tak rozšířenou variantu modelu otevřené komunikace k ISO/OSI v místních sítích a jsou vázány také se sítí internet [3]. Je samozřejmé, že samotná data je potřeba před přenesením po Ethernetu upravit, zabezpečit, opatřit porty, adresami, zakódovat a modulovat. V místních ethernetových sítí se na tom podílí fyzická vrstva, datová linková a také protokoly IP a TCP. Tak se objevuje model Ethernet TCP/IP, výše uvedené protokoly se označují jako Ethernet Protocol Suite – soubor protokolů Ethernet[3].
Ethernetový model tedy vypadá takto:

1. Síťové rozhraní (přístupová)
2. Síťová vrstva
3. Transportní
4. Aplikační

Vrstva síťového rozhraní se někdy rozděluje na dvě části na fyzickou a datovou linkovou vrstvu. V tabulce [1] je porovnání modelů Ethernet a ISO/OSI, resp. jak jsou vrstvy zastoupeny v druhém modelu.

Tabulka 1: Porovnání ISO/OSI a Ethernet model

Ethernet	ISO/OSI
Aplikační	Aplikační
Prezentační	
Relační	
Transportní	Transportní
Síťová	Síťová
Linková	Vrstva síťového rozhraní
Fyzická	

Zdroj: vlastní tvorba podle [4].

3.5 Zapouzdřování dat

Při odesílání dat prochází data zapouzdřováním (encapsulací) od aplikační vrstvy dolů. Průběh je, že na aplikační vrstvě aplikace má data, které chce poslat na jiné zařízení a ty doplní o aplikační hlavičku. Takto upravená data potom pošle nižší vrstvě (transportní), kde dojde k segmentaci dat, opatří je aplikačními porty, a přidá TCP nebo UDP hlavičku. Takto upravená data se nazývají segment. Na síťové vrstvě se segmenty doplní o IP hlavičky a vznikne IP paket, lze se setkat i s označením IP datagram. V přístupové vrstvě se paket zaopatří ethernetovou hlavičkou a nakonec přidá trailer, který obsahuje kontrolní součet (FCS). Pro jeho výpočet se zpravidla používá CRC. Takto vzniknul ethernetový rámec, který je předán ne přenosové medium.

Při přijetí takového rámce na druhém zařízení probíhá deencapsulace od nejnižší vrstvy k aplikační. Díky tomu dostane cílová aplikace odesílaná data.

3.6 Fyzická vrstva Ethernetu

Ethernet je logická sběrnice, takže datové rámce jsou směrovány všem, avšak jednotlivě určeny jen těm, jejichž adresy jsou uvedeny v adresovém poli rámce[cit II]. Rámce jsou bit po bitu přenášeny médiem. Tok bitů je uveden startovací

posloupností používanou pro synchronizaci mezi stanicemi, od vysílající se všemi přijímacími. Po preambuli je prostor pro cílovou a zdrojovou MAC adresu, dále určení protokolu pro další vrstvu. Po typu následuje prostor pro data, celý rámec je zakončen kontrolním CRC součtem. Pole dat má stanovenou minimální délku 46B. Pokud se předává méně dat, než je minimální délka, doplní se datové na minimální délku. Příjemce vlastním výpočtem kontrolního součtu porovná součet v přijatém rámci, pokud je v pořádku, předá ho další vrstvě. Jestliže však kontrolní součet nesouhlasí, dojde k vyřazení rámce. Odesílatel nebude informován o nedoručení.
Protokoly na fyzické vrstvě specifikují [5]:

- Elektrické signály
- Tvary konektorů a jejich zapojení
- Typ média přenášejícího data
- Přenosové rychlosti
- Modulaci signálu
- Kódování
- Synchronizaci

V průmyslové automatizaci se používá měděná kroucená dvoulinka v odolných krytech z důvodu většího rozsahu teplot, než bývá v kancelářských sítích. Další nebezpečí pro kabely tvoří prostředí, např. kyseliny. Hrozí rozežrání opletu kabelu, případně jeho uhnití. Samozřejmostí jsou dnes optické kabely, z důvodů vyšších rychlostí a dostupnosti zařízení. Skleněné vlákno v multimódu má maximální dosah 3000m, v singlemódu až 120km. Záleží samozřejmě na připojených modulech k zařízení. Pokud je místo skleněného vlákna použito vlákno plastové tzv. Polymer Fiber, je dosah max. 50m, v případě Polymer Cladded Fiber max. 100m [6].
Bezdrátové sítě se v průmyslu využívají minimálně, protože průmyslové prostředí je zpravidla zarušené. Náklady na kvalitní bezdrátovou síť v průmyslu by byly vysoké a nerentabilní.

3.6.1 Technické provedení průmyslového Ethernetu

Fyzická topologie sítě Ethernet je velmi úzce spjata s plánováním a spuštěním počítačových sítí jako takových. Stejně jako počítačová síť, tak i průmyslová síť

prochází postupně přípravnou a vyhodnocovací etapou, realizační etapou a provozní [15].

3.6.1.1 Přípravná etapa

V přípravné etapě jde o vyhodnocení, která metoda a prostředky jsou vhodné pro daný účel. U Ethernetu je etapa zjednodušena, protože technika je velmi rozšířena jak v kancelářských sítích, tak i v průmyslových. Do průmyslových sítí však proniká Ethernet díky stále klesající ceně komponent a nahrazuje tak dominantní průmyslové sítě i v nižších úrovních sběru dat.

V síti Ethernet jsou k dispozici různé síťové prvky v různém provedení i ceně. Především se jedná o přepínače pro průmyslové ethernetové sítě, dostupné v krytí vyžadovaném v těžkých provozních podmínkách průmyslu [3]. Komponenty jsou rozdílné pro použití v průmyslu nebo v kanceláři. V průmyslu jsou komponenty napájeny 24V stejnosměrně, v kanceláři 230V střídavě. Protože koncová zařízení pracují v nepřetržitém provozu, musí se obejít bez ventilátorů. Zpravidla pracují ve vyšších teplotách než kancelářské stanice. Také musejí být uzpůsobeny k montáži na nosnou lištu. K dalším požadavkům patří například vykazování krátké přístupové doby a malá časová nejistota.

3.6.1.2 Topologie sítě

V dnešní době se sítě Ethernet vytváří pomocí topologií. Jsou to:

- Topologie Bus (liniová)
- Hvězda (star)
- Kruh (ring)

Liniová topologie se dnes jeví jako nepoužitelná, protože v případě výpadku jednoho zařízení dojde k odstavení celé sítě. Výpadkem systému může dojít k velkým ekonomickým ztrátám.

Ačkoliv výpadek centrálního prvku v topologii star rozdělí topologii a dojde k výpadku, používá se tato technologie častěji než liniová topologie. Navíc lze výpadku zamezit redundantním zařízením ve stejné úrovni jako je centrální prvek.

V topologii kruh jde o redundanci na úrovni spoje podle standardu IEEE 802.1D Spanning tree [3]. Nicméně po výpadku zařízení dojde k rekonfiguraci sítě

v průběhu 45-60s, což je pro průmyslové úlohy nepřijatelné. Řídicí systém se rozpadá, už když je výpadek delší než 5s. Alternativou je použití standardu Rapid Spanning Tree, který má povolenou dobu komunikace do 1s. Jedná se o standard IEEE 802.1.w, v roce 2004 byl zařazen do standardu IEEE 802.1.d. U tohoto protokolu mohou nastat tyto nestandardní situace:

- Zdvojení datových paketů,
- Může dojít ke změně pořadí paketů,
- Mohou vznikat smyčky,
- Je povoleno maximálně sedm přepínačů,
- Není definována doba přepnutí, a tak může v nepříznivých případech konvergence trvat 45-60s, jako při použití spanning tree.

V topologii zdvojený kruh je možný nejvyšší stupeň funkční pohotovosti. Nedochází zde k výpadku sítě ani při výpadku více zařízení najednou. Standard pro redundantní provedení komunikace v síti pro průmyslové účely zatím neexistuje, a tak si někteří výrobci vyvinuli vlastní řešení. Mezi ně se řadí např. Hiper-Ring vyvinutý firmou Hirschmann (dnes již součástí společnosti ABB), který je přední výrobce komponent průmyslového Ethernetu. Standard Hiper-Ring zaručuje zotavení sítě do 500ms i při velkých vzdálenostech mezi až 50 přepínači [15].
Lze se také setkat s proprietárním protokolem společnosti Moxa Turbo Ring. Stejně jako STP a RSTP využívá k ověření dostupnosti spojů BPDU zprávy. Dokáže reagovat a změnit síťové cesty do 20ms [16]. Dalším protokolem je protokol MST standardizovaný jako IEEE 802.1s, protokol vychází z RSTP, jeho výhodou je mapování více VLAN do jedné STP instance. Dochází tak k tomu, že všechny VLAN sítě v instanci mají stejnou cestu v síti, může se tedy ušetřit počet STP pro velký počet VLAN.
Nelze také opomenout protokoly společnosti Cisco: PVST, PVST+ a RPVST+. Použitím těchto protokolů lze docílit toho, aby každá VLAN síť nebo skupina VLAN sítí měla vlastní cestu v síti [17].

3.6.2 Zařízení v síti

V síti lze nalézt buď na koncová zařízení, nebo na prvky, přes které prochází rámce v síti. Jedná se buď o prvky aktivní, kam lze zařadit hub, switch, router nebo pasivní, kde je to optická kabeláž, zatím se používá především na dlouhé a páteřní spoje, a metalická kabeláž.

Zařízení pro energetický průmysl mají oproti běžným, kancelářským zařízením další doplňky. Např. router Cisco 829 je vybaven 3G/LTE modemem, sériovými linkami, gigabitové ethernetové porty se sdíleným, 30 W PoE (dle standardu IEEE 803.3at), portem pro optické vlákno, wifi radiem na frekvencích 2.4GHz dle standardu IEEE 802.11n i 5GHz, teplotním rozsahem od -40°C do 60°C. Napájen je v rozsahu 6-30 V stejnosměrných [13].

V podmínkách, v jakých se vyskytují, je nutné, aby měly odolnost podle norem IEC 529 a IEC 61850-3[23]. Zařízení Cisco 829 má stupeň krytí 54. Zařízení je tedy částečně odolné proti prachu a proti stříkající vodě ze všech úhlů. Zařízení jsou také vybavena podporou více protokolů, tedy nejen protokolu Ethernet, ale také datových protokolů a protokolů např. pro automatizaci nebo energetiku.

Zařízení Cisco Nexus 5000 Series jsou vybaveny PTP protokolem pro přesnější distribuci času v síti než v případě protokolu NTP. Jedná se o distribuovaný protokol, který vzájemně v reálném čase synchronizuje zařízení v PTP systému. PTP systém je hierarchicky uspořádán v síti na principu master-slave. Nejvýše položený master v hierarchii (grandmaster), řídí celý PTP systém. Jeho čas se zasílá a distribuuje napříč sítí. Synchronizace probíhá výměnou PTP zpráv se členy za použití časových informací a časování, dochází k nastavení času od grandmastera. PTP systém lze kombinovat mezi zařízeními, které nepodporují PTP zařízení [14].

3.7 Linková vrstva

Úlohou linkové vrstvy je zajištění dat mezi zařízeními v síti. Datové bloky, které se na linkové vrstvě přenáší, nazýváme linkový rámec. Rámec obsahuje hlavičku, samotná data a často i zápatí., ve kterém je obvykle kontrolní součet z dat, která jsou přenášena. Pomocí tohoto mechanismu zajišťujeme, zda při přenosu data nedošlo k jejich porušení [5].

Druhá vrstva má funkci zabezpečení přenosu a definování přístupové metody. U Ethernetu se jedná o metodu, která je založená na principu CSMA/CD. Tato metoda zajišťuje právo použití média, pokud na něm v nevysílá jiný účastník. Pro ověření, jestli nastala kolize, musí být maximální doba od odesílatele k nejvzdálenějšímu zařízení v doméně kratší než doba, která je potřebná k vyslání rámce s nejmenší povolenou délkou. Pro ověření obousměrného zpoždění (RTT) lze použít nástroj ping.

U Ethernetu při přenosové rychlosti 10 Mb/s je minimální délka rámce 64 bajtů. Musí být zajištěno, aby maximální doba signálu od odesílatele nepřekročila polovinu doby potřebné k přenesení 64 bajtů. Při dané rychlosti je to 100ns, takže RTT musí být kratší než 51,2 mikrosekund. Aby zdrojová stanice mohla rozpoznat případnou kolizi, musí první bit dosáhnout konce fyzického segmentu sítě nejpozději za 25,6 mikrosekund. Zdrojová stanice po odeslání rámce čeká minimálně 51,2 mikrosekund, a za předpokladu, že nedostane informaci o kolizi, považuje rámec za přijatý.

Pokrok v mikroelektronice způsobuje růst rychlosti v Ethernetové síti. Významnou roli mezi nimi má požadavek na přenos ve full-duplexním režimu[3]. Full-duplexní režim přišel do ethernetové sítě s kroucenou dvoulinkou. Tím došlo ke změně topologie na strom a hvězdu, a použitím nejdříve hubů, později switchů. K full-duplexnímu režimu dochází, protože se využívají dva páry kroucené dvoulinky, jeden pro příjem zpráv (Rx) a druhý pár pro odesílání (Tx). Použitím switchů se výrazně zmenšila pravděpodobnost kolize, a zvýšila se efektivita přenosu.

Průmyslový Ethernet je navržen tak, aby metodu CSMA/CD využíval pouze pro časově nekritické zprávy. Pro přenosy v reálném čase jsou použity jiné metody [3].

3.8 Síťová vrstva

Hlavním úkolem síťové vrstvy je směrování (routing), tj. zajištění komunikace mezi jednotlivými sítěmi, subnety. Zařízení určené pro routing byl původně určen router, v dnešní době lze také využít L3 switche, firewally, servery nebo počítač. Úkol takového zařízení je přeposílání komunikace z jedné sítě do jiné [7].

Na síťové vrstvě dojde k přidání IP hlavičky. Její tvar záleží na použitém protokolu. Stěžejním protokolem na síťové vrstvě je IP protokol. Používáme dva protokoly IP:

- IPv4
- IPv6

IP protokol je odpovědný za přijmutí segmentů od TCP, zapouzdřit je do paketů a přiřadit jim příslušné adresy a najít nejlepší cestu, přes kterou doručí paket k cílovému hostiteli [8].
IPv4 má adresní prostor 32bitů. Dochází k nedostatku veřejných IP adres, a tak dochází k přechodu na IPv6, které má adresní prostor 128bitů. Data se opatří zdrojovou a cílovou IP adresou, zdrojovým a cílovým portem a protokolem transportní vrstvy.
Mimo protokoly IP na síťové vrstvě pracují i další protokoly, např. ICMP – používá se pro zjišťování stavů sítě.
Mezi další protokoly patří proprietární protokoly IPX (Novell Internetwork Packet Exchange), AppleTalk, Connectionless Network Service (CLNS/DECNet).

3.8.1 IPv4

IPv4 se používá od roku 1983, kdy byla nasazena na síť Advanced research Projects Agency Network (ARPANET), kterou lze chápat jako předchůdce dnešního internetu. IPv4 paket má 2 části:

- IP hlavička – obsahuje vlastnosti paketu
- Data – obsahuje segment čtvrté vrstvy a aktuální data

IPv4 hlavička obsahuje pole z důležitými informacemi o paketu. Tyto pole obsahují binárně zapsané informace, které jsou zkoumány při deencapsulaci na síťové vrstvě. IPv4 hlavička obsahuje [8]:

- Verze IP protokolu – čtyřbitová, která idetifikuje verzi IP paketu.
- Internet header length (IHL) – čtyřbitová hodnota; délka internetové hlavičky v 32-bitovém slově, minimální hodnota pro správnou hlavičku je pět.
- Differentiated services (DS) – osmibitové pole, dříve nazývané Type of Service, slouží k určení priority paketu. Prvních 6 bitů idetifikuje Differentiated services code point (DSCP) hodnotu, která je použita

mechanismem quality of service. Poslední dva bity idnetifikují explicitní přetížení (ECN), které mohou být použité k zabránění zamítnutých paketů během přetížení sítě.

- Total length – dva bajty, délka datagramu.
- Identifikace – dva bajty, identifikační hodnota odesílatele, která umožňuje lepší skládání fragmentů datagramu. Pokud byl datagram fragmentován, mají všechny fragmenty datagramu stejnou identifikaci.
- Flags (příznaky) – tři bity, kontrolní příznaky: nultý bit je rezervovaný, musí být nula, první bit řeší fragmentaci datagramu (DF), druhý bit je pro další fragmenty.
- Fragment Offset – třináctibitové pole, identifikuje pořadí fragmentu v datagramu. První fragment má offset nula.
- Time to live – osmibitová hodnota, která se používá k omezení životnosti paketu. Je uvedeno v sekundách, běžně je však označováno jako počet skoků. Odesílatel paketu nastaví počáteční hodnotu a pokaždé, když je datagram zpracován směrovačem se hodnota time-to-live sníží o jednotku. Pokud klesne hodnota TTL na nulu, směrovač paket zahodí a pošle zprávu pomocí protokolu ICMP Time Exceeded na zdrojovou IP adresu. K identifikaci směrovačů používaných mezi zdrojovou a cílovou stanicí se používá příkaz traceroute.
- Protocol – určení, který protokol další vrstvy bude s paketem pracovat, protokoly jsou definovány v RFC 760, např. protokol ICMP je „1“
- Header Checksum – kontrolní součet pouze IP hlavičky
- Zdrojová adresa – 32-bitová IP adresa odesílatele
- Cílová adresa – 32-bitová IP adresa příjemce paketu

Nejčastěji odkazovaná pole jsou zdrojová a cílová adresa. Tyto pole identifikují, odkud a kam paket cestuje.

IP adresa je logická adresa zařízení v síti [10]. Velikost adresy v IPv4 je 32bitů, rozdělených do čtyř oktetů po osmi bitech. Její zápis je pomocí čtyř dekadických hodnot, které jsou odděleny tečkou. Vše je však zpracováváno v zařízeních, které používají binární soustavu.

3.8.2 IPv6

Již v roce 1990 byla společnost Internet Engineering Task Force znepokojována problémy protokolu IPv4 a začala hledat náhradu. Aktivita společnosti vedla k vývoji protokolu IPv6, který překonává omezení a vylepšuje protokol IPv4.
Vylepšení poskytované protokolem IPv6 [9]:

- Zvýšení adresního prostoru – adresy protokolu IPv6 jsou tvořeny ne 32bity jako u IPv4 ale 128 bity. Díky tomu se rapidně zvyšuje počet dostupných IP adres.
- Vylepšení ovládání paketu – došlo ke zjednodušení IPv6 hlavičky. Tímto se zlepšuje ovládání paketů prostřednictvím mezilehlých routerů a poskytnutí podpory pro rozšíření a možnost zvýšení škálovatelnosti a dlouhověkosti paketu.
- Integrované zabezpečení – Protokol IPv6 podporuje autentizaci a ochranu soukromí. Do IPv4 je nutné tyto funkce implementovat.
- Eliminování překládání adres – s velkým počtem veřejných IPv6 adres není potřeba používat NAT. Ať velké podniky nebo domácnosti, tak mohou všichni dostat veřejnou adresu IPv6. Tímto lze předejít některým problémům s NATem. Některé aplikace vyžadují end-to-end konektivitu

V průmyslu se však zatím s IPv6 nesetkáme, z protože je ještě stále čerstvý a nelze spoléhat na neověřené nebo neotestované protokoly. IPv6 protokol je ideální pro IoT, k zapojení nespočetného množství zařízení (senzory, čidla, apod.).
Protokol IPv6 také stále přináší hrozby. Pokud je firewall určený pro protokol IPv4, je majitel zařízení proti IPv6 naprosto nechráněný. Při zapojení prvků na protokolu IPv6 napříč internetem bez NATu, může dojít k nechtěnému sdílení dat. Zařízení, počítače apod., mají defaultně protokol IPv6 povolen. Pokud protokol společnost nechce využívat, musí správce sítě na každém zařízení deaktivovat protokol IPv6.

3.8.3 ICMP

Servisní protokol ICMP je vyžadovanou součástí protokolu IP, je definován v RFC 792. Protokol ICMP vy Musí být podporován každým zařízením v síti. Základním

úkolem ICMP je informovat zdrojové zařízení a chybách při přenosu datagramů. Zprávy mohou být nejen chybové, ale i informativní a diagnostické. Chyby mohou vznikat např. [11]:

- Je zjištěna chybná syntaxe IP hlavičky,
- Router neví, kam má poslat paket, nemá záznam v routovací tabulce,
- Došlo k zahození paketu překročením TTL

ICMP zprávy lze generovat pouze na jedno protější zařízení. Adresa datagramu nesmí být typu broadcast nebo multicast. Zpráva ICMP je v datagramu uložena hned za IP záhlavím. Pole protokol v IPv4 hlavičce je nastaveno na „1“. ICMP zpráva se skládá ze záhlaví a datové části. Hlavička se skládá z [12]:

- Typu zprávy – objasňuje, o jaký typ zprávy se jedná
- Kódu – speciální kódy pro daný typ zprávy
- Proměnné části
- Kontrolního součtu

3.9 Transportní vrstva

Transportní vrstva realizuje spojení pro počítačové programy. Programů může být i několik a tak mezi dvěma zařízeními může být současně navázáno několik různých spojení. Mezi stěžejní protokoly na transportní vrstvě patří spolehlivý a spojovaný protokol TCP. Protokol je sestaven tak, aby mohl zajišťovat zabezpečený přenos dat větších objemů. Příjem dat je kontrolovaný cílovou stanicí, a odesílá se potvrzení zdrojové stanici. Pokud nepřijde potvrzení do časového limitu, posílá se daný paket znovu. Chybu tak lze detekovat i odstranit. Pomocí tohoto algoritmu, který je označován jako Nagelův, lze měnit MTU, čili kolik bajtů lze přenést v daný okamžik. Standardní MTU délka je 1500 bajtů. Navazování spojení je rovněž řízeno protokolem TCP. Dokud je funkční spoj mezi dvěma zařízeními, je vytvořený full-duplexní okruh.
Pokud dojde k přerušení komunikace, uvědomí vrstva TCP příslušnou vyšší vrstvu komunikačního modelu.

Čísla portů mají funkci rozhraní k aplikačním úlohám. Některé úlohy mají rezervované určité porty, jedná se o tzv. well-known ports (např. 443 je pro HTTPS). Jestliže port není rezervován, při navazování spojení se rezervuje.

Zkombinování IP adresy a čísla portu se nazývá socket. Zapisuje se ve tvaru IP adresa: číslo portu (např. 10.1.1.10:8080). Díky tomuto dochází k jednoznačnému vytvoření koncového bodu pro komunikaci.

Kromě spolehlivé a spojované komunikace protokolem TCP, může funkci transportní vrstvy realizovat protokol nespolehlivý UDP. Na rozdíl od TCP je protokol UDP pouze jednosměrný, zdrojová stanice tak nedostává informaci, zda byl paket v pořádku přijat. Přenos dat protokolem UDP je rychlejší, avšak za cenu, že nevíme, jestli daný paket přišel. Chyba musí být řešena až v aplikační vrstvě, adresování probíhá stejně jako u TCP protokolu pomocí portů. UDP je tedy vhodný protokol pro cyklické a rychlé přenášení dat. Používá se tedy tam, kde potřebujeme získat data v reálném čase.

3.10 Aplikační vrstva

Aplikační vrstva má za úkol poskytnou aplikačním procesům přístup ke komunikačnímu systému a umožnit tak komunikaci. Úkolem protokolů na aplikační vrstvě je porozumění si mezi zařízeními. Pro každou službu (např. pošta, přenos dat, web, automatické přidělování IP adres) je přidělený protokol (SMTP, POP3…). Přitom protokoly stále vznikají, buď zcela nové, nebo jako náhrada původních.

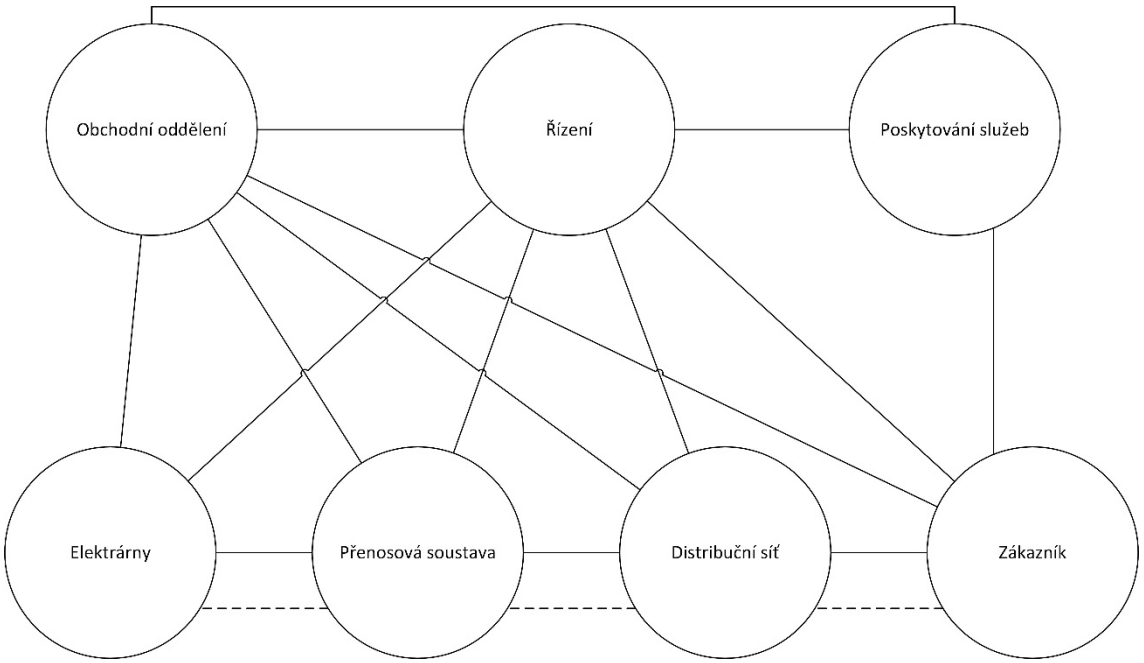
Protokoly pro účely IT lze bez problému používat v sítích typu internet i dalších sítích LAN. Nicméně aplikační protokoly pro automatizaci se systémem Ethernet TCP/IP jsou vzájemně nekompatibilní. Například Organizace ODVA zavedla pro komunikaci po Ethernetu aplikační protokol Ethernet/IP, organizace IDA Group používá modifikaci aplikačního protokolu Modbus pod názvem Modbus/TCP, organizace uživatelů sítě Profibus využívá protokoly skuipny Profinet apod. [3].

4 Smart Grid

Pojem Smart Grid, česky *„inteligentní síť“*, označuje energetické komunikační sítě, které v reálném čase regulují výrobu a spotřebu elektrické energie. Oproti standardním rozvodným elektrickým sítím přináší [19]:

- Integrovanou obousměrnou komunikaci,
- Pokročilé komponenty a metody řízení,
- Plná automatizace (senzorické a měřící technologie) - díky automatizaci dokážeme v reálném čase zjistit informace o provozu sítě, kvalitě dodávky, přerušení dodávky,
- Vylepšenou rozhodovací podporu.

Sítě Smart Grid přináší také integraci zákazníků. Zákazník je vybaven čidly s obousměrným tokem dat, což podle aktuální situace v síti umožňuje tvorbu cenových tarifů. Takové zařízení je zpravidla smart elektroměr (tzv. Smart metr), který umožňuje dálkový odečet energie. Při plné integraci může zákazník efektivně řídit energetickou spotřebu v domácnosti [20].
Smart Grid dává příležitost také decentralizovaným výrobním technologiím (např. solární a větrné elektrárny, vodní elektrárny atd.). To dává příležitost vyrobenou energii zákazníkům prodávat do elektrické sítě.
Pro zásady komunikace je vytvořen konceptuální model. Konceptuální model je tvořen sedmi doménami, mezi kterými existuje spojení buď komunikační, nebo elektrické. Model nereprezentuje finální architekturu Smart Grid sítí. V podstatě se jedná o nástroj pro popis, diskuzi a rozvoj architektury. Konceptuální model poskytuje kontext pro analýzu interoperability a standardů a další vývoj architektury Smart Grid.
Na obr. [1] je jeho znázornění, plná čára znázorňuje komunikaci procesů, přerušovaná tok elektrického proudu mezi doménami (kruhy).



Obrázek 1: Konceptuální model sítí Smart Grid, vlastní zpracování podle [18].

V České republice byl testován v letech 2010-2015 projekt Smart Grid společností ČEZ Distribuce a. s. v mikroregionu Vrchlabí. Koncepty sítí Smart Grid lze však najít i v jiných lokacích v ČR, např. v Litoměřicích byla představena chytrá lavička, která pomocí solárních panelů umožňuje chodcům nabíjet telefon, buď pomocí kabelu, nebo bezdrátového nabíjení. Lavička má také integrovaný LTE modem pro lepší připojení do internetu a senzor Capasitty pro měření kvality ovzduší [21].

4.1 Topologie Smart Grid sítí

Topologie se děli podle rozlehlosti na sítě [19]:

- HAN – Home area network, jednotlivé zařízení v rámci jednoho domu,
- NAN – Neighbourhood area network, sdružují HAN sítě v blízkém okolí,
- WAN – Wide area network – podobně jako u běžných datových sítí, zajišťuje propojení vzájemných HAN sítí.

4.2 Bezpečnost energetických sítí

Součástí bezpečnosti energetických sítí je kromě monitoringu, firewallu, šifrování apod. také fyzická ostraha objektu. Další součástí jsou interní bezpečnostní politiky daných energetických společností.

Z důvodu maximální bezpečnosti je důležitá fyzická ostraha objektu. Ochrana je standardizována podle kategorizace objektů – mechanické zabezpečení, elektronické zabezpečení, fyzická ostraha a kombinace těchto způsobů zabezpečení. Dále provoz kamerového systému se záznamem, oprávněný přístup do serveroven pouze povolaným zaměstnancům.

5 Protokoly průmyslového Ethernetu

V této kapitole jsou popsané protokoly využívané v průmyslové automatizaci. Důraz je kladen především na práci v reálném čase, synchronizaci a model komunikace. Jsou zde také vysvětleny pojmy, synchronizace a způsoby zasílání zpráv na standardizovaných protokolech, které jsou používány v energetice.

5.1 Proč Ethernet do průmyslu?

Protokol Ethernet nabízí oproti průmyslovým sběrnicím další výhody, díky kterým lze výrazně zjednodušit. Dnešní uživatelé mají zájem o [22]:

- Integraci s kancelářským prostředím,
- Integraci existujících průmyslových sběrnic,
- Větší šířku pásma, rozsáhlejší soubory pro komunikaci s více a inteligentnějšími automatizačními přístroji,
- Komunikaci v reálném čase se synchronizací pro splnění požadavků aplikací v oblasti řízení pohonů,
- Možnost připojení a adresování většího počtu zařízení ve větších oblastech
- Homogenní sítě většinou na bázi Ethernetu,
- Nové funkce typu MES, možnost přímé (on-line) aktualizace firmwaru, dálkové konfigurace, a ošetření chyb,
- Integraci existujících průmyslových sběrnic.

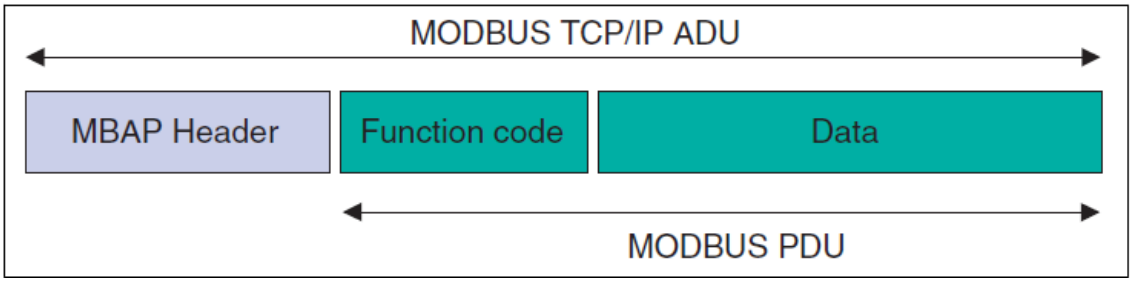
Vývoj k průmyslovému Ethernetu přešel z důvodu nedostatečného splňování podmínek systémů automatického řízení. Jedná se o R-T (real-time) vlastnosti, spolehlivost), bezpečnost a robustnost. V průmyslu patří mezi stěžejní parametry rychlost odezvy. V Ethernetu s protokolem TCP/IP je komunikace nedeterministická. Často je reakce větší než 100ms, přičemž vzdálené jednotky vyžadují reakční dobu od 5 do 1 ms. Řízení pohonů má ještě vyšší nároky a vyžaduje reakční dobu v μs. Ke snížení reakční doby lze dopomoci několika způsoby:

- Rozdělení sítě do segmentů s několika zařízeními klesá hodnota k 20ms,
- Pokud použijeme UDP místo TCP, může být reakce 10ms i méně,
- Adresací pomocí MAC v segmentu dokáže snížit dobu až k 1ms.

5.2 Modbus

Modbus je otevřený protokol na úrovni aplikační vrstvy ISO/OSI pro komunikaci různých zařízení architekturou klient-server. Umožňuje vzájemnou komunikaci různých zařízení a přenášení dat různými sběrnicemi (RS-232, RS-422-RS485, optické a rádiové sítě, Ethernet s protokolem TCP/IP [24,25].

Struktura protokolu je definována na úrovni protokolu nezávisle na typu komunikační zprávy. Podle typu sítě je PDU rozšířené o další části, aby splňovalo požadavky daného protokolu, vzniká tzv. ADU.



Obrázek 2: Rozdíl mezi PDU a PDU Modbus, zdroj: [24].

Architektura klient-server pracuje na základě žádosti od klienta. PDU přenáší kód funkce, a data. Pokud nenastane v průběhu komunikace problém, provede server akci a vyšle klientovi zprávu s původním kódem a výsledkem akce.

V případě, že při výkonu operace dojde k chybě, je obsahuje PDU pro vyřízení zprávy v kódu funkce kód zvýšený o nastavený nejvyšší bit indikující neúspěch a v datové části chybový kód.

Na straně klienta je nezbytné nastavit časový limit pro přijetí zprávy, aby v případě ztráty PDU klient nečekal na zprávu, která nemusí přijít [25].

Časová synchronizace protokolu Modbus přes Ethernet řešena pomocí NTP protokolu.

5.3 EtherNet/IP

Protokol EtherNet/IP je jeden z široce používaných standardů průmyslového Ethernetu vyvinutý pro průmyslovou automatizaci. Hlavní výhodu přináší plná kompatibilita s Ethernetem TCP/IP. Hlavní výhodou je možnost použít standardní technické a programové prostředky Ethernetu ke konfiguraci a ovládání automatizačních prostředků. Standard EtherNet/IP byl představen v roce 2001

konsorciem výrobců a organizací sdružených v asociacích ODVA a ControlNet International v čele s firmou Rockwell Automation [26]. Byl standardizován jako IEC 62413 v roce2005. Je také součástí normy IEC 61158.

V rámci sítě EtherNet/IP jsou jednotlivým ethernetovým uzlům přiřazeny předem definované typy zařízení, které mají specifické vlastnosti a funkce. Funkce zařízení a aplikační vrstva je tvořena protokolem CIP, který se používá i v dalších typech průmyslových sítí DeviceNet a ContoNet. Protokol CIP využívá objektový model a komunikaci typu producent-consumer. Použitím protokolu CIP lze dosáhnout spolupráce systémů, které protokol CIP podporují. Hlavními přednostmi protokolu EtherNet/IP jsou:

- Přenos dat systémem producent-konzument,
- Průběh s dalšími úlohami v síti Ethernet,
- Využití standardního Ethernetu a běžných síťových komponent.

Síť Ethernet/IP je plně kompatibilní se sítí Ethernet. Předností této sítě je nejen koexistence s ostatními aplikačními programy Ethernetu, ale i kompatibilita s prvky a infrastrukturou včetně dalšího vývoje Ethernetu a jeho protokolů.

5.3.1 Model producent-consumer

Jedná se o vysílání zpráv multicastem. CIP používá tento model namísto běžnému adresnímu schématu. V běžné hlavičce je zdrojová adresa a cílová adresa. V modelu producent-consumer je pouze jeden multicastový identifikátor.

5.3.2 CIP

Objektově orientovaný protokol CIP pracuje na aplikační vrstvě. Podle protokolu je každé zařízení reprezentováno skupinou objektů, přičemž každý objekt má atributy, operace a reakce na události. V protokolu CIP je definováno, jaká data musí každý objekt obsahovat. Existují tři skupiny objektů – povinné, aplikační a objekty definované výrobcem [26,27].

Mezi povinné objekty patří objekt identifikující zařízení, objekt pro správu spojení, objekt specifikující, jak se zprávy předávají a alespoň jeden objekt s parametry konfigurace komunikační sítě.

Protokol CIP lze využít na EtherNetu/IP, zde jako identifikátor používá IP adresu, DevicNet, ControlNet, CompoNet. Na těchto protokolech je hlavním identifikátorem MAC ID.

5.3.3 Bepečnost CIP

Aplikace bezpečnosti zahrnutá do protokolu CIP poskytuje možnost míchat bezpečnostní a standardní zařízení ve stejné síti pro hladkou integraci a zvýšení flexibility. CIP Safety zabezpečuje komunikaci mezi uzly, jako jsou I/O bezpečnostní spínače, PLC v zabezpečovacích zařízeních až do SIL 3 podle normy IEC 61508 [27].

5.4 EtherCAT

Tento standard byl vyvinut s důrazem na rychlý přenos dat v krátkém komunikačním cyklu. O vývoj a propagaci se starají dodavatelé EtherCAT Technology Group. Standard EtheCAT zcela nahrazuje přístupovou vrstvu standardního Ethernetu. Je to proto, aby se dosáhlo vysokého výkonu. V roce 2005 byl protokol EtherCAT publikován jako IEC 62407 (průmyslové komunikační sběrnice) a IEC 61784-2 (komunikační profily) [26].

Oproti standardu EtherNet/IP nahrazuje protokol EtherCAT standardní ethernetové protokoly a využívá Ethernet jako prostředek k realizaci velmi výkonné sběrnice pro práci v reálném čase.

Využívá komunikace **master-slave**. EtherCAT master vysílá do sítě zprávu. Každé EtherCAT slave zařízení po přečtení zprávy určené pro jeho zařízení vloží data do rámce procházejícího sítí. Zpoždění rámce je způsobené pouze hardwarovou propagaci. Poslední zařízení v segmentu detekuje otevřený port a pomocí ethernetového full-duplexního okruhu pošle zprávu masterovi. EtherCAT master je jediné zařízení v síti, které umožňuje posílat EtherCAT rámce. Všechny ostatní zařízení rámce předávají dál po datovém proudu. Tento koncept zabraňuje nepředvídatelným zpožděním a zaručuje komunikaci v reálném čase[26].

EtherCAT podporuje všechny druhy topologií. EtherCAT je ryzí sběrnicová nebo liniová topologie se stovkami zařízení schopná bez jakýchkoliv omezení, které vznikají. V případě topologie strom nebo hvězda je nutné, aby zařízení mělo více než dva ethernetové porty, aby mohl rámec rychle procházet zařízením. Všechny

topologie tvoří logický kruh. Fyzický kruh je možné vytvořit také uzavřením smyčky mezi posledním zařízením a dalším portem řídícího zařízení. Při zapojování systému je prospěšné kombinovat linky s pobočkami (větvemi) nebo s nastavitelnou hranicí. Porty, které jsou nezbytné k vytvoření větve, jsou přímo integrovány do I/O modulů. Díky tomu nepotřebujeme další přepínače nebo aktivní prvky infrastruktury.
Pokud dojde k připojení nebo odpojení zařízení za běhu, zajistí funkce Hot Connect rychlou konvergenci mezi ostatními zařízeními. Pokud je odstraněna sousední hranice, dojde automaticky k uzavření portu. Zbytek sítě může dále pokračovat. Hladký průchod zajistí velmi krátká doba detekce, která bývá menší než 15 mikrosekund.

5.5 Profinet

Profinet je standard pro průmyslové sítě v automatizaci. Propojuje zařízení systémy usnadňující rychlejší bezpečnější, levnější a vyšší kvalitu vyráběných produktů. Lze integrovat do existujících systémů sítě Ethernet. Profinet je nejrozšířenější řešení průmyslového Ethernetu, propojuje výrobní zařízení a vybavení jako PLC, DCS a podnikové sítě. Je plně kompatibilní s kancelářskou sítí Ethernet. Jsou zde rozdíly, především kancelářský Ethernet není schopen komunikace v reálném čase podávat takový výkon, jako požaduje průmyslová automatizace. Kancelářský Ethernet je také méně odolný vůči prostředí průmyslové výroby [30].
Je založen na zkušenostech s real-time sběrnicí PROFIBUS, která je jedním z nejoblíbenějších automatizačních řešení.
Toto řešení je schopné pracovat v náročných podmínkách průmyslu. Je pracovat rychle a přesně podle požadavků výrobních závodů. Poskytuje také další funkce, např. bezpečnost, Energy Manegment a integraci IT. Tyto funkce mohou být použity v kombinaci s kontrolními monitorovacími funkcemi [2].

5.5.1 Práce v reálném čase

Profinet zvládá různorodé požadavky IT a automatizační poažadavky ve výrobních provozech pomocí tří služeb [29]:

- Standardní TCP/IP: používá se pro nedeterministické funkce jako je parametrizace, video/audio přenos a přenos dat vyšším vrstvám,

- Real Time (Profinet RT): Dochází k vynechání vrstev TCP/IP z důvodu poskytnutí deterministického výkonu pro automatizační aplikace v rozsahu 1-10ms. Toto zajišťuje softwarové řešení typicky na bázi I/O aplikací, včetně řízení pohybu a požadavků na energetickou náročnost,
- Izochronní Real Time (Profinet IRT): Priorita signálu a plánované přepínání poskytuje vysokou přesnost synchronizace pro aplikace jako je řízení pohybu. Tempo cyklu odchylky se pohybuje v rozmezí milisekund, se odchylkou v rozsahu mikrosekund. Tato služba vyžaduje hardwarovou podporu v podobě ASIC čipů.

Všechny tři služby mohou být použity současně. Sdílená šíře pásma zajišťuje, aby alespoň 50% z každého I/O cyklu bylo dostupné pro TCP/IP komunikaci, bez ohledu na podporu ostatních funkcí. V kombinaci s odolnou kabeláží, konektory a Ethernetovými switchi má Profinet vše, co potřebuje pro požadavky automatizace [30].

5.6 IEC 61850

Norma IEC 61850, případně český ekvivalent ČSN EN 61850, který je přesný, je soubor norem pro komunikaci v energetice. Norma definuje pravidla pro komunikaci mezi zařízeními, které jsou v rozvodnách. Zároveň také stanovuje požadavky na rozvodny z hlediska komunikace. Obsahuje také standardy pro řídicí funkce a inženýring rozvoden a nebytné definice komunikačních protokolů. Norma říká jak propojit zařízení a nástroje od různých výrobců, aby mohli spolupracovat dohromady (=interoperabilita) [31].

Soubor norem IEC 61850 představuje jednotnou, standardizovanou metodu pro tvorbu komunikační sítě, která je nezávislá na výrobci zařízení, a integraci jednotlivých zařízení do rozvodny. Cílem při tvorbě souboru bylo umožnit vytváření systémů, kde budou komunikovat zařízení různých výrobců. Tato zařízení jsou označována zkratkou IED a zajišťují ochranu rozvodny, dohled nad jejím provozem a automatizaci, regulování a měření v rozvodně. Standardizuje rozhraní, protokoly a datové modely a zajišťuje tak spolupráci zařízení a systémů v rozvodnách a síti a snižuje tím náklady na integrování zařízení rozvoden. Soubor norem IEC 61850

definuje protokoly nejen pro komunikaci mezi zařízeními v rozvodně, ale také mezi rozvodnami a dalšími uzly sítě. Může to být např. elektrárna, dispečink. Přenáší informace mezi rozvodnami, i při výpadku elektrizační sítě. Vytváří ze zařízení a podsystémů v elektrizační síti jednotný a úplný komunikační systém, čím zefektivňuje technické a ekonomické řízení procesů v energetických a rozvodných společnostech.

Pro komunikaci s ostatními zařízení používá TCP/IP a Ethernet. Díky tomu lze využít širokou škálu vlastností, které jsou běžné v komunikaci, vysoký výkon a otevřenost novým komunikačním konceptům [32]. IEC 61850 přináší objektově orientovaný přístup do systémové automatizace. Podporuje standardizované modely zařízení s použitím jména namísto registračních čísel a indexů. Norma podporuje komplexní sadu funkcí rozvodny. Umožňuje snadný návrh, specifikaci, konfiguraci, nastavení a údržbu. High-level služby umožňují samo popisování přístrojů a automatické zjišťování objektů v síti, konfigurační soubory vylučují závislosti zařízení a mapování tagů a umožňuje výměnu konfigurací zařízení. Protokol IEC 61850 se také stále rozšiřuje podle potřeb a vývoje systému [33].

Rozvodné stanice jsou nezbytnou součástí při přepravě elektřiny z elektráren do domácností, podniků a továren. Rozvodná síť je složena ze stovek rozvodných stanic, které je nutné sledovat a ovládat. Díky vývoji výpočetní a komunikační techniky lze využívat a spoléhat se na inteligentní samoobslužné sledování a řízení. Klíčovým faktorem pro vytvoření funkčního automatizačního systému jsou rychlá a spolehlivá síťová řešení.

Automatizační systémy pro řízení rozvodné stanice se skládají ze tří fyzických vrstev [32]:

- Přístrojová vrstva – bývá založena na sběrnici RS485, skládá se z jednotek ochran a řídících jednotek,
- Komunikační vrstva – jádro monitorovaného systému. Shromažďuje data z jednotek ochran a zasílá je do nadřazeného řídicího centra. Také komunikuje pomocí povelů z řídícího centra řídícím jednotkám,
- Vrstva rozvoden – zajišťuje ethernetové připojení k serverům a zabezpečuje pracovní stanice před vlivy nesprávně navržené elektrické izolace a jističů.

K normě IEC 61850 mají blízko také další normy. Norma IEC 62271-3: Vysokonapěťová spínací a řídicí zařízení – část 3: Digitální rozhraní podle IEC 61850, definuje specifikaci zařízení pro digitální komunikaci se zařízeními v rozvodně. K této normě existuje český ekvivalent ČSN EN 62271-3.
Norma IEC/TS 62351-6 definuje zabezpečení protokolu IEC 61850 nebo norem odvozených. Definuje zprávy, procedury a bezpečnostní algoritmy.
Norma IEC/TS 62351-1 se zabývá zabezpečením a komunikace dat v energetických sítí a systémech, které souvisejí s distribucí elektrické energie. Využívá k tomu dalších norem, které pracují jako rozhraní pro systémy řízení výroby a distribuce elektrické energie. Konkrétně jsou to protokoly IEC 60870-5, IEC 60870-6, IEC 61850, IEC 61970 a IEC 61968 [31].

5.6.1 Struktura IEC 61850

Standard IEC 61850 je rozdělen do deseti částí, z nichž některé mají několik dílů. Normy byly publikovány pod názvy Komunikační sítě a systémy v podřízených stanicích a Komunikační sítě a systémy pro automatizaci v energetických společnostech. První čtyři části (IEC 61850-1 až IEC 61850-4) popisují prostředí, specifikaci terminologii, požadavky na zařízení.
Např. norma IEC 61850-3 definuje mechanickou a klimatickou odolnost síťových prvků, které se používají v rozvodných stanicích. Tato norma specifikuje požadavky na hardwarovou konstrukci zařízení, které se používají v elektrických rozvodných stanicích. Aby byla zařízení certifikována, musí splňovat tři hlavní požadavky [23]:

- Odolnost proti elektromagnetické indukci – zařízení, která jsou špatně chráněná, mohou být působením elektromagnetické indukce poškozena nebo zničena. Je nutné použít hardwarové komponenty, které jsou odolné proti elektromagnetické indukci a musí být dostatečně testovány,
- Široký rozsah provozních teplot – široký teplotní rozsah (-40°C až 75°C) je důležitým faktorem, protože v prostředí, kde jsou rozvodny umístěné, může být vysoká teplota až 75°C, ale i nízká (až -40°C). Ke splnění požadavků lze dojít buď efektivním rozptylem tepla při extrémně vysokých teplotách, nebo za použití systému pro vlastní vyhřívání při nízkých teplotách,

- Odolnost vůči nárazům a vibracím – zařízení musí splňovat limity odolnosti, proti vibracím a nárazům k zajištění trvalého provozu a to i pokud dojde k mechanickému problému (vypadnutí z úchytů v rozvodné skříni). Tyto požadavky lze splnit pomocí ochranných prvků tlumících náraz při pádu zařízení.

Norma IEC 61850-5 z roku 2013: Požadavky na komunikaci pro funkce a modely zařízení. Standardizuje komunikaci mezi IED zařízeními [39]. Šestá část řeší komunikační jazyk v elektrických stanicích, které se týkají komunikace mezi IED. Jedná se o tzv. Substation configuration language. Jazyk specifikuje formáty souborů pro popis konfigurace mezi jednotlivými IED zařízeními. Společně s částmi 5 a 7 zajišťuje kompatibilitu zařízení různých výrobců [40].

Sedmá část standardu IEC 61850 popisuje komunikační strukturu systémů rozvoden a napájecích zařízení. Je rozdělena do několika částí: první část IEC 61850-7-1: Základní struktura komunikační struktura pro podřízené stanice a napájecí zařízení – Zásady a modely; část poskytuje přehled o architektuře interakcích mezi zařízeními v rozvodnách, například zařízeními ochran, jističi, transformátory, základními systémy v rozvodně apod. Druhá část normy IEC 61850-7-2 řeší základní komunikační strukturu pro podřízené stanice a napájecí zařízení – Abstraktní rozhraní pro komunikační služby (ASCI). ASCI lze použít pro oblast aplikací společnosti vyžadující spolupráci IED v reálném čase. Definice ACSI byla vytvořena tak, aby na vlastních komunikačních systémech bylo nezávislé. Mapování specifických komunikačních služeb definuje IEC 61850-8-x a IEC 61850-9-x.

Norma IEC 61850-7-3: Obecné třídy dat; V této části jsou specifikace třídy dat pro informace o stavech zařízení, vzorkovaných veličinách, informace spojené s řízením stavu zařízení, o analogových veličinách žádaných v regulačních smyčkách a o konfiguraci zařízení. Tento díl normy definuje obecné typy atributů vázaných na použití v rozvodnách pro obecné třídy. Normu lze použít pro popis modelů zařízení a pro popsání funkcí, které zajišťují výměnu dat mezi rozvodnami a napájecími zařízeními [37].

Čtvrtý díl sedmé části, Třídy kompatibilních logických uzlů a třídy dat, definuje kompatibilní názvy logických uzlů a dat mezi programovatelnými zařízeními a vztahy mezi logickými uzly a daty.

Navíc má sedmá část ještě dvě pod části, část IEC 61850-7-410 se zabývá vodními elektrárnami, kde definuje komunikaci pro sledování a řízení, speciálně pro vodní elektrárny. V části IEC 61850-7-420 [43]: Logické uzly pro decentralizované zdroje elektrické energie, definuje informační modely pro výměnu informací v sítích, které mají decentralizované zdroje elektrické energie a akumulační stanice (např. fotovoltaické elektrárny, mikroturbíny, kombinovaná výroba tepla a elektrické energie, zařízení pro akumulaci el. Energie). Pokud je to možné, využívá logické uzly definované v IEC 61850-7-4 a jestliže je to nutné, vytváří nové logické uzly [41].

Osmá část normy, IEC 61850-8, má pouze jednu část. Norma IEC 61850-8-1: Mapování specifických komunikačních služeb (Specific Communication Service Maping), mapování na MMS (ISO 9506-1 a ISO 9506-2) a na ISO/IEC 8802-3 (IEEE 802.3). V tomto díle jsou specifikovány metody pro výměnu časově kritických i nekritických zpráv v lokální síti pomocí mapování na MMS a na etheretové rámce. Časově kritické zprávy jsou zasílány pomocí tzv. Gerneric Object-Oriented Sbustation Event (GOOSE) zprávy, které jsou specifikovány v normě IEC 61850-8-1 [39].

Devátá část normy má dvě části: IEC 61850-9-1: Mapování specifických komunikačních služeb – přenos vzorkovaných hodnot po sériovém jednosměrném (neorientovaném) vícebodovém spoji bod-bod podle normy IEC 60044-8 (Přístrojové transformátory – elektronické transformátory proudu). Norma platí pro komunikaci slučovacích jednotek elektrických transformátorů a zařízením pole rozvodny.

Část IEC 61850-9-2: Mapování specifických komunikačních služeb – Vzorkované hodnoty z ISO/IEC 8802-3, se používá v případě potřeby použití rychlejší připojení, než je specifikováno v normě IEC 61850-9-1, mapování je podle IEC 61850-8-1.

V třetí části normy IEC 61850-9-3: Mapování specifických komunikačních služeb – Precision time protocol for power utilty automation. Norma zatím nemá český překlad, byla vytvořena v roce 2016, specifikuje PTP a jeho použití v energetickém

průmyslu dle normy IEC 61588 s důrazem na synchronizaci definovanou v IEC 61850-5 a IEC 61869-9 [37].

V desáté části normy, IEC 61850-10: Zkoušky shody, jsou definovány metody, pro zkoušení shody zařízení, které se používají v automatizovaných systémech v rozvodnách a abstraktní situace zkoušek [38].

5.6.2 GOOSE

Jak vyplývá z názvu, jedná se o generickou objektově orientovanou událost rozvodny. Do jednoho objektu jsou zde seskupeny stavová data a hodnoty proměnných. Tento objekt je potom přenášen v časovém intervalu. GOOSE zpráva přenáší data mezi rozvodnami po spolehlivé, ethernetové technologii. Datový soubor je vysílán multicastem. Musí být přenášen cyklicky v určitém časovém intervalu, který se nazývá T_0 nebo T_{max}. Časový interval je 5-100ms. Pokud dojde v rozvodně k události, vytvoří se nové GOOSE zpráva. Tento režim se nazývá T_1 nebo T_{min}, má rozpětí od 0,5 do 5ms. Po přijetí této zprávy se postupný čas hlášení zdvojnásobí, až dosáhne T_0 [39].

5.6.2.1 Priorizace GOOSE

Norma IEC 61850 umožňuje stanovit priority GOOSE zpráv přes Ethernet tak, aby se vyhnula vyrovnávací paměti Ethernetu, je však důležité, aby switch tuto funkci podporoval. GOOSE zpráva je uložena v rámci druhé vrstvy, dle definice IEEE 802.1Q. Tímto je norma IEC 61850 a GOOSE odlišná od protokolů, které nepoužívají Ethernet. Rámec obsahuje další parametr, který definuje priority pro switche. Podle priority obchází vyrovnávací paměť a upřednostňuje GOOSE zprávy [39]. Parametr, který definuje prioritu, se nazývá 802.1p. Jedná se o čtyřbitové číslo. Vzhledem k tomu, že zpráva existuje ve druhé vrstvě modelu ISO/OSI, může switch posílat zprávy pomocí broadcastu nebo multicastu na všechny porty bez zpoždění. Tímto dochází k rychlejšímu přenosu GOOSE zpráv v síti a snižuje pravděpodobnost, že se při rekonfiguraci ztratí. Lze také možnosti mít pro GOOSE zprávy vlastní VLAN síť.

5.6.3 GSSE

Generic Substation State Events, neboli generická stavová událost ústředny. Tato zpráva přenáší pouze stavová data. Na rozdíl od GOOSE se nejedná o datový objekt, ale pouze stavový seznam. Zprávy jsou přenášeny prostřednictvím mechanismu MMS. Oproti GOOSE trvá jejich zpracování a přenos déle [43].

5.6.4 MMS

MMS je mezinárodně standardizovaný IEC 9506 [42] systém pro přenos zpráv v reálném čase. Objektové modely a služby přenosu jsou obecně vhodné pro širokou škálu zařízení v průmyslovém prostředí. Objektové modely, služby a zprávy MMS jsou totožné, ať se jedná o PLC systém nebo robota.

Rozdíl v doručování mezi GOOSE a MMS zprávami je především v adresování. MMS využívá k adresování IP adresy a pro doručení zprávy MAC tabulky v přepínačích tak, aby došlo pouze k přímému zajištění cesty. GOOSE zprávy nelze směrovat, protože používá adresy na druhé vrstvě. Pouze MAC adresy, nepoužívá tedy MAC tabulky switchů pro nalezení nejlepší přístupové cesty jako MMS zprávy [42].

5.7 IEC 60870-5-101

Norma IEC 60870-5-101 (IEC 101) je mezinárodní standard pro sledování energetického systému, jeho kontrolu a komunikaci. Standard je kompatibilní se standardy IEC 60870-5-1 až IEC 60870-5-5. Používá standardní asynchronní sériové vzdálené komunikace na rozhraní mezi DTE a DCE. Standard je vhodný pro různé topologie, např. point-to-point, hvězda.

Protokol IEC 101 má následující vlastnosti [45]:

- Podporuje nesymetrický (komunikaci zahájil master) i symetrický (komunikace je zahájil buď master nebo slave) způsob přenosu dat,
- Adresa linky a ASDU adresy jsou stejné pro koncové stanice,
- Data jsou přenášené jako informační objekty se specifickou adresou,
- Při přenášení zpráv vysoké priority a nízké priority a přenosu dochází k odlišným mechanismům přenosu,

- Možnost dělit data do různých skupin a získávání dat dotázáním se na konkrétní skupinu nebo vydáním příkazu k získání dat ze všech skupin,
- Provádí cyklické a spontánní aktualizace dat programů,
- Zařízení pro synchronizaci času,
- Systémy pro přenos dat.

5.8 IEC 60870-5-104

Norma IEC 60870-5-104 (IEC 104) umožňuje komunikovat mezi kontrolní stanicí a rozvodnou pomocí TCP/IP sítě. Protokol je částí normy IEC 60870-5 – komunikační profily pro zasílání zpráv mezi dvěma systémy, který je založen na stále zapojených datových okruzích. Protokol TCP je použitý pro bezpečný, spojově orientovaný přenos dat. Norma je omezena typem informací a konfiguračních parametrů definovaných v IEC 60870-5-101. Ne všechny funkce definované v IEC 60870-5-101 jsou v IEC 60870-5-104 dostupné. Výrobci zařízení však velmi často kombinují aplikační vrstvu IEC101 s dopravním profilem IEC104aniž by kladli těmto omezením pozornost. Pokud zařízení striktně dodržuje standard, může nedodržení vést k problémům.

Protokol IEC 104 je běžně používán v ICS/SCADA prostředích. Různé ICS/SCADA zařízení používají IEC 104 ke komunikace s dalšími ICS zařízeními [46].

5.9 DNP3

DNP3 je sada komunikačních protokolů používaných mezi komponentami v automatizačních systémech. Jeho přední využití je v energetických a vodních společnostech. Ač je technicky možné využití i v jiných průmyslových odvětvích, tak to není běžné. Protokol byl vyvinutý s cílem zjednodušení komunikace různých typů získávání dat a regulační techniky. Což hraje klíčovou roli ve SCADA systémech, kde jsou použity SCADA master stanicemi (řídicí centra), RTU a IED zařízeními. Je to nástupce protokolu Modbus. Je sice spolehlivý, bohužel neposkytuje dobré zabezpečení [47, 48].

6 Nástroje monitoringu

Pokud chceme zvládat správu sítě, je monitoring síťových prvků, serverů a dalších zařízení v síti nutný. Pro monitoring lze využít řadu technologií a protokolů. Monitoring sítě lze rozdělit na dva pohledy:

- Zjištění informací, zda došlo k problému (překročení limitu apod.).
- Zjištění informací o stavu systému – informace aktuální i historické; krátkodobý výpadek v síti může znamenat ztrátu, ať časovou nebo finanční. V průmyslu může dojít i k poškození zařízení ovládaných pomocí sítě.

Základními principy monitoringu jsou zachytávání paketů v síti a testování dostupnosti. Zachytávat (tzv. sniffování) komunikaci v síti lze pomocí speciálního hardware (v případě zachytávání GOOSE zpráv např. GOOSER pro zachytávání GOOSE zpráv) nebo software (Wireshark apod.). Pakety jsou zachycovány, když protékají sítí. Pokud je to nezbytné, dojde k dekódování na surová data, které zobrazí hodnoty různých polí paketu. Zachytávat tok paketů lze buď v rámci celé sítě, segmentu sítě nebo pouze jediného zdroje v síti.
Rozlišujeme dva způsoby monitoringu [49]:

- Monitoring s agentem – na server nainstalovaný monitorovací agent klienta. Většinou se k němu lze připojit pomocí vzdálené zprávy, např. SSH nebo Telnet. V průmyslu nemusí být agent nainstalovaný na server, ale využít controller, který sbírá data na síti a počítač se připojuje k němu, nebo pracuje autonomně (GOOSER, gooseAir apod.),
- Monitoring bez agenta – probíhá testování služeb pomocí standardních protokolů (SNMP, ICMP).

6.1 SNMP

Simple Network Management Protocol je jednoduchý protokol pro správu sítě. Využívá architektury klient-server. Naslouchá na protokolu UDP, portu 161. Manažer zasílá požadavky agentovi na portu 161. Na straně serveru se používá port 162. SNMP podporuje velké množství zařízení. Hodnoty lze získávat pravidelným dotazováním. Lze je ukládat do databáze a vykreslit je do grafu [51].

Protokol SNMP se vyvíjel ve třech verzích: první verze zajišťuje funkčnost SNMP, do druhé byla v implementována autentizace a do verze SNMPv3 bylo přidáno šifrování.

SNMP je především využíván na počítačích, které mají za úkol sleddování nebo řízení skupiny počítačů či jiných zařízení v síti. Na straně sledovaných zařízení je spuštěn agent, který následně poskytuje pomocí SNMP informace manažerovi.

Protokol vyžaduje dvě strany pro komunikaci. Na jedné straně je manager, proti agent. Existují dvě možnosti, jak pracuje SNMP [51]:

- Manažer se dotazuje agenta a přijímá odpovědi, hodnoty tak může sbírat více managerů,
- Zprávy jsou zasílány agentem manažerovi.

6.1.1.1 Trap

SNMP umožňuje agentovi oznámit významné události prostřednictvím nevyžádané SNMP zprávy. Jedná se o příkaz, který je vysílán od agenta k manažerovi. Obsahuje aktuální hodnotu sysUpTime, OID identifikaci problému a nepovinné vazby proměnných. U verze SNMPv2 k přejmenování PDU na SNMPv2-Trap a úpravy formátu zprávy. Zpráva může být vyslána i bez vyžádání, v případě, že agent detekuje hrozbu [65].

6.1.1.2 Response

Vrací vazby proměnných a potvrzení od agenta manažerovi. Pokud je neúspěšné zpracována žádost, SNMP agent zastaví zpracování a zaznamená identifikátor instance error-indexu. Do pole error-status také zaznamená chybový kód [63].

6.1.1.3 Request

Rozlišuje se na [52]:

- SetRequest – požadavek od manažera k agentovi na změnu hodnoty proměnné nebo pro změnu více hodnot v MIB databázi. Není však podporován všemi výrobci zařízení, poté už nelze provádět správu zařízení, ale pouze ho monitorovat [65],

- GetRequest – Požadavek od manažera k agentovi pro zjištění dostupných proměnných a jejich hodnot. Vrací odpověď s hodnotou proměnné lexikograficky navazující na předchozí proměnnou v MIB. Celá MIB tabulka může být přečtena iterativní aplikací pomocí GetNextRequest od OID na pozici 0. Řádky tabulky lze číst zadáním OID sloupců ve vazbách proměnných na základě vytvořené žádosti zpráva je vytvořena na základě informací, které požaduje uživatel nebo aplikace [66],
- GetBulkRequest – Byl představený v SNMPv2. Požadavek je posílán od manažera agentovi pro více iterací GetNextRequest. Poskytuje metodu pro snadné získání dat na jeden požadavek od SNMP. Ve verzi SNMPv3 poskytuje vylepšené zabezpečení a ochranu soukromí [67]. Odpověď od agenta jsou proměnné s více vazbami. PDU specifikuje velikost a opakování pole, sloužící k ovládání chování odezvy.

6.1.2 Typy SNMP objektů

SNMP objekty existují dvou typů – skalární hodnoty a tabulky. Skalární objetky mohou nabývat pouze jednoduché nestrukturované hodnoty. Jsou to zejména tyto hodnoty [50]:

- Integer – jednoduché celé číslo. Limit není definován, je však implementacemi omezeno na 32 bitů,
- Counter – nezáporný integer, plynule zvyšuje svoji hodnotu, při dosažení max. hodnoty (2^{32} - 1) začíná znovu od nuly. Používá se pro počítání zajímavých událostí v systému. Absolutní hodnota je méně důležitá než rozdíl (delta) od posledního vzorku, ze kterého lze usuzovat na rychlost změn,
- Gauge – nezáporný integer, jehož hodnota může vzrůstat i klesat, nikdy ale nemůže překročit max. hodnotu (2^{32} – 1). Hodnota Gauge je maximální, kdykoliv modelovaná informace je větší nebo stejná než toto maximum. Pokud dojde k poklesu, sníží se i hodnota Gauge,
- TimeTicks – nezáporný integer, který reprezentuje v setinách sekundy čas od jisté doby modulo (2^{32} - 1). Lze ho použít k vyjádření doby chodu nějakého zařízení od jeho zapnutí,
- IpAddress - 32 bitová IP adresa,

- OCTET STRING – sekvence octetů (bajtů). Je používán k vyjádření buď řetězce znaků, např. jméno systému, nebo libovolných binárních dat, např. MAC adresy zařízení,
- OBJECT IDENTIFIER – reprezentuje název uzlu. SNMP umožňuje ještě tři jiné typy skalárních hodnot (NULL, Opaque a Network Address), ty se však nepoužívají.

Jako rozšíření těchto nestrukturovaných jednoduchých objektů, lze strukturovat data do tabulek. Tabulky jsou uspořádány do řádků a sloupců. Jednotlivé položky takovéto tabulky jsou pak libovolné skalární hodnoty, uvedené výše. Tabulky nelze do sebe vnořovat.

SNMP operace nad tabulkami však nelze provádět jako nad celkem, pouze jen nad jednotlivými skalárními objekty. Jako příklad lze použít např. směrovací tabulky routerů – tcpConnTable – object identifier je 1.3.6.1.2.1.6.13, sloupce jsou reprezentovány hodnotami tcpConnState, tcpConnLocalAddress, tcpConnLocalPort, tcpConnRemAddress a tcpConnRemPort.

Identifikace jednotlivých polí v SNMP tabulkách je prováděna indexací. Indexy jsou buď jednoduché hodnoty, nebo sady hodnot, tvořené hodnotami polí uvnitř tabulky. K polím pak lze přistupovat náhodně, tedy příkazem Get a specifikací pozice nebo sekvenčně, tedy příkazem GetNext postupně procházíme celou tabulku [51].

6.1.3 MIB

Management Information Base popisuje sadu objektů, jež jsou předmětem zprávy. Zařízení, které spravujeme, může implementovat jednu nebo i více MIB, závisí na jeho funkci. MIB databáze jsou podobné standardním databázím – popisují jak strukturu, tak formát.

6.1.4 Hodnoty v databázi

Každá hodnota v databázi je definována jednoznačným identifikátorem OID. Je to posloupnost čísel oddělených tečkou. Hodnota vzniká tak, že vezmeme OID nadřazeného objektu, přidáme tečku a doplníme aktuální číslo. Celá tato struktura je uložena v databázi

6.1.5 Problémy použití SNMP

Některé omezení protokolu mají kořeny přímo v jeho architektuře, která používá pasivní agenty. Ti jsou definováni pouze SNMP dotazy. Za největší nedostatek je ale někdy považované slabé zabezpečení protokolu.

6.2 Wireshark

Wireshark patří mezi nejlepší snifferovací nástroje. Je vyvíjen jako bezplatný, pod licencí GNU GPL, avšak dosahuje kvality komerčních produktů. Umí dekódovat přes 400 protokolů a je stále aktivně vyvíjen a aktualizován. Je běžně používaný i v produkčním prostředí [49].

Díky využívání knihovny libpcap (Promiscous Caputre Library) je schopen spolupracovat s dalším aplikacemi používající s daty knihovny libpcap. Wireshark dokáže číst data i jiných formátů. Automaticky dokáže rozeznat typ souboru, který čte a dokáže komprimovaná data rozbalit.

Mezi velké benefity Wiresharku patří velké množství protokolů, které dokáže dekódovat. Dekodéry protokolů jsou buď přidány přímo do aplikace, nebo je lze přidat pomocí plug-in modulů. Obsahuje jak servisní protokoly, aplikační protokoly a protokoly transportní vrstvy. Také obsahuje protokoly využívané i v průmyslu např. protokol MMS, GOOSE, Modbus/TCP, a mnoho dalších.

6.3 Syslog

Nejběžnější způsob, jak přistupovat k systémovým zprávám je pomocí protokolu Syslog. Syslog byl vyvinutý pro UNIXové systémy v roce 1980. Prvně byl standardizován v RFC 3164 v roce 2001, revidován je v RFC 5424. Syslog pro posílání zpráv, které upozorňují na události v IP sítích. Naslouchá na UDP portu 514. Syslog je podporován většinou síťových zařízení (musí být puštěn). Protokol umožňuje zařízením v síti zasílat systémové zprávy na syslog server.

Syslog poskytuje tři základní funkce [53]:

- Shromažďovat informace logů pro monitoring a řešení problémů
- Zvolit typ zpráv, které budou sledovány
- Určit místo doručení zprávy syslogu

Výstup zpráv získávaných od síťových zařízení závisí na nastavení daného zařízení. Nemusíme získávat všechny události, ale např. jen události týkající se routování apod. Zprávy jsou odesílány na syslog server. Zprávy a výstupy uložené na syslog serveru mohou být zabaleny do zpráv pro jednodušší další zpracování.

Syslog zprávy mohou být vypsány také pouze do vyrovnávací paměti zařízení (RAM zařízení). Takové zprávy lze zobrazit pouze v CLI zařízení. K vyrovnávací paměti zařízení se lze připojit i vzdáleně pomocí terminálu, konzole, syslog serveru, přímo na zařízení, Telnet nebo SSH.

Zařízení vytváří syslog zprávy při nějaké události v síti. Každá syslog zpráva obsahuje úroveň závažnosti. Důležitost zpráv je značena číslovkou. Menší hodnoty jsou kritičtější alarmy syslogu. Na monitorovacím zařízení lze nastavit úroveň zpráv, od které se budou zprávy řešit. Seznam úrovní je uveden v tabulce [2].

Tabulka 2: Zprávy Syslog

Název zprávy	**Úroveň zprávy**	**Popis**
Mimořádná událost	Level 0	Systém nelze použít
Upozornění	Level 1	Nutná okamžitá opatření
Kritický stav	Level 2	Kritický stav
Chyba	Level 3	Chybový stav
Varování	Level 4	Výstražný stav
Notifikace	Level 5	Normální, ale významná podmínka
Informační	Level 6	Informační zpráva
Debuggování	Level 7	Debuggovací zpráva

Zdroj: vlastní zpracování, podle [53].

Každá úroveň má svůj vlastní význam:

- Kritické a mimořádné zprávy informují o selhání systému. Buď softwarové, nebo hardwarové části. Tyto zprávy na nefunkčnost části sítě. Závažnost určuje skutečná úroveň zprávy syslogu,
- Ladicí úroveň (Tuning level) má za úkol generovat výstupní sestavy a vysílat příkazy ladění,
- Notifikační úroveň oznamuje pouze informace, nedochází k funkčnosti zařízení.

Kromě závažnosti zprávy obsahují syslog zprávy informace o objektu. Používá identifikátory, které identifikují a kategorizují stav systému při chybovém hlášení a hlášení událostí. Možnosti logování jsou specifické podle možností zařízení.
Syslog serverový agent je k dispozici nejen pro Unixové systémy, ale i pro systémy platformy Windows. K dispozici je jak v komerčních řešeních, tak ve freeware licencích.

6.3.1 SIEM

SIEM technologie provádí analýzy bezpečnosti v reálném čase. Sbírá data generována síťovými zařízeními a aplikacemi. SIEM řešení je kombinací bezpečnostního informačního managementu (SIM) a událostního bezpečnostního managementu (SEM). SIEM nástroje zajišťují monitoring a jsou schopny vyložit bezpečnostní hrozby a informovat administrátory. Použití SIEM systému přináší síťovému administrátorovi přínosy [56]:

- Snížení rizikovosti aplikací,
- Přehled provozu nad aplikacemi,
- Získávání informací z různých zařízení a aplikací v reálném čase.

Data lze získat pomocí několika způsobů, např. [56]:

- Syslog,
- Databázové konektory,
- SNMP,

- Prosté soubory,
- Síťové svazky.

6.4 Průmyslové controllery a testery

Jedná se o zařízení, které jsou vybaveny speciálními konektory pro připojení různých zařízení tak, aby dokázaly sledovat tok v síti. Zařízení splňují normu IEC 61850.

Např. Zařízení GOOSER, od výrobce PROGRAMMA-MEGGER, je vybaven dvěma galvanicky oddělenými Ethernetovými porty, k maximální ochraně vnitřní smyčky. Jeden port je k připojení k PC, na kterém je nainstalovaný PC-GOOSER software. Druhý port je pro připojení k zařízením do energetické sběrnice. Přístroj je dále vybaven deseti binárními vstupy a výstupy. Umožňuje integrací SCL souboru a rozkládáním GOOSE zpráv dojde k převodu na binární signalizaci. Konfigurační soubory jdou nahrát také pomocí flash paměti přes USB rozhraní. GOOSER splňuje požadavky normy IEC 61850-8-1 na testování vybavení. Navíc má pro rychlou úpravu konfigurace a čtení dat 6,4“ dotykový displej. Typická doba konverze je okolo 0,6ms [52].

Oproti GOOSERu gooseAir PC představuje počítač postavený na linuxové distribuci Gentoo s předpřipravenými síťovými službami splňující požadavky IEC 61850. Je konfigurovatelný pomocí webového rozhraní, které běží na gooseAir PC. GooseAir PC být využit nejen jako server, ke kterému se lze připojit pomocí programu na PC, ale i jako klientská stanice, či server/klient pro MMS zprávy. Základní verze gooseAir PC je k dostání ve třech provedeních. Liší se od sebe procesorem, vstupními porty (COM, VGA, USB, SFP, Ethernet) i rozměry. Od malých zařízení určené k montáži na nosnou lištu, až k PC určeného k zabudování do racku [55].

Další možností pro sledování síťového provozu je malý ruční analyzér GOOSE Meter ONE. Snadno rozpozná aktivní, nedávné a zastaralé zprávy. Dokáže je označit, kategorizovat a filtrovat podle potřeb uživatele pro rychlé vyhodnocení diagnostiky. Je to pouze nástroj k získávání dat, zařízení tedy nemůže ohrozit síťový provoz [58].

6.5 SCADA

Systémy pro dispečerské řízení a sběru dat (Supervisory Control And Data Acquistion) hrají významnou úlohu pro sledování, analyzování stavu a ovládání rozvodných sítí a ostatních energetických systémů. V reálném čase zpracovává data z čidel v provozu a posílá je na centrální počítač, který je dále zpracovává. SCADA systémy jsou používány od 60. let 20. století ve většině rozsáhlých průmyslových procesech, kde je počet vstupů/výstupů v řádu tisíců. SCADA je tedy využívána jako dispečerské zařízení v [57]:

- Výrobě a rozvodu elektřiny,
- Chemickém průmyslu,
- Hutnictví,
- Potravinářství, farmaceutickém průmyslu.

Mezi komponenty systému SCADA patří:

- Central SCADA master systém,
- Komunikační síť,
- Terminálové jednotky (RTU) kombinované s PLC zařízeními, dnes již dochází ke splývání terminálových jednotek a PLC. Terminálové jednotky podporovaly komunikaci, ale nebyly plně programovatelné nebo složitě. Dnes již jsou programovatelné plně.
- Čidla a aktuátory.

Nedílnou součástí SCADA systému jsou regulátory, databáze, sítě, HMI, komunikace, databáze a software. Nesmí chybět také vstupně výstupní software.
SCADA/HMI je systém s rozhraním pro uživatele (operátora), kde zobrazuje informace o procesech a umožňuje zadávat operátorovi příkazy. Obvykle se zde zobrazují i grafické vizualizace. Obnovovací frekvence stavu systému je od dvou do deseti sekund. SCADA systémy využívají protokoly Modbus, v dnešní době nahrazován DNP3, a komunikačními protokoly IEC 60870-5-101 a IEC 60870-5-104.

7 Měření konvergence v heterogenních přepínaných sítích

V práci byly zmíněny protokoly pro zamezení redundance v sítích: STP, RSTP, MST a proprietární protokoly od ABB, Hiper-Ring a společnosti Moxa, Turbo Ring. Vzhledem k různým okolním vlivům a zájmům, může dojít ve společnostech k výměně distributora, který dodává síťové prvky. Je nutné zařízení od různých společností zapojit do jedné sítě a vytvořit funkční topologii. Nezbytností v energetickém průmyslu je nízká doba konvergence. V případě výpadku velkého množství stavových GOOSE zpráv může dojít k problémům.

Nyní se tedy v dané společnosti, která se zabývá dodávkou elektrické energie ve východních Čechách, lze setkat se zařízeními firmy Cisco, RuggedCom od společnosti Siemens a zařízení firmy ABB. Nastává tedy problém ve vzájemné komunikaci zařízení mezi sebou. Je nutné zvolit nejlepší možné řešení pro redundanci sítě. Standardní doba konvergence STP protokolu, 50s, je nevyhovující, k redundanci musí dojít v řádu milisekund. Samozřejmostí je certifikace zařízení dle normy IEC 61850-3, specifikující hardwarovou odolnost vůči okolnímu prostředí.

Při měření byly použité dva Cisco switche 2520 a dva switche RuggedCom RSG2100. Zařízení od společnosti Hirschmann (ABB) byl switch Hirschmann RSP525.

Předmětem měření bylo zjišťování výpadku GOOSE zpráv při výpadku linky nebo výpadku root bridge. Součástí měření bylo i testování dostupnosti zařízení pomocí ICMP.

7.1 Princip RSTP

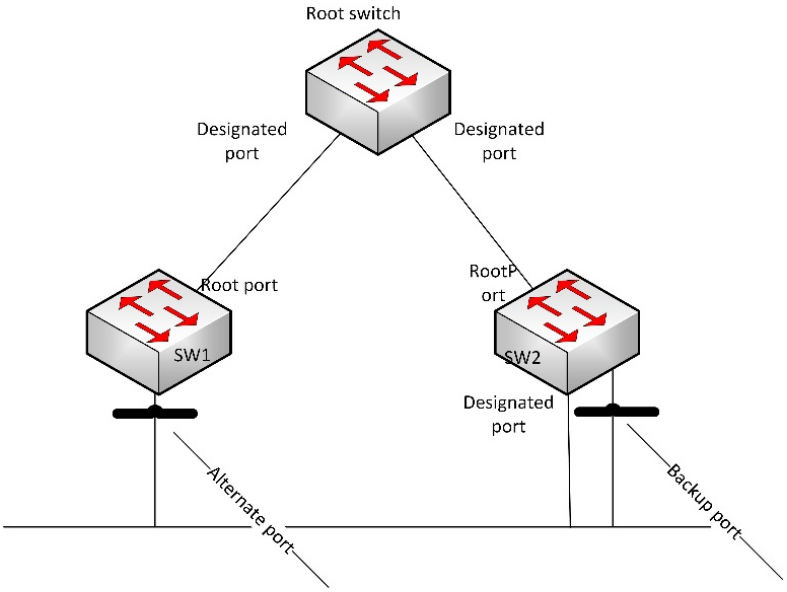
Protokol RSTP vznikl ve chvíli, kdy konvergence STP přestala být dostačující. K tomu došlá nástupem L3 switchů. Dochází k tomu, že routování, konkrétně protokoly OSPF a EIGRP, nachází cestu při výpadku rychleji než při přepínání. Z protokolu RSTP vychází a jeho strukturu využívá protokol MST.

Oproti STP přidal protokol RSTP nové stavy portů a role portů. RSTP je zpětně kompatibilní se Spanning tree protokolem, když na switch přijde BPDU zpráva STP, přepne se switch do klasického STP protokolu. Pro chod RSTP v síti je tedy nutné vyvolat konvergenční mechanismus [61].

V RSTP jsou tři stavy portů:

- Dicarding – port není aktivní v topologii, ani se neučí MAC adresy,
- Learning – port je aktivní v topologii a učí se MAC adresy, pouze přijímá BPDU zprávy a upravuje si MAC tabulku,
- Forwarding – port je aktivní v topologii a učí se MAC adresy, předává dále BPDU zprávy síťovým segmentem jako v STP.

Role portů jsou určeny hodnotou, která je danému portu přiřazena. K rolím root a designated jsou navíc přidány backup a alternate. Každá role plní svoji úlohu.
Root port dostává BPDU, která má nejvyšší váhu. Takový port je nejblíže k root switchi. Výpočetní Spanning tree algoritmus vybere jeden přepínač v síti, který je pro celou síť root switch. V případě použití Cisco proprietárních protokolů může být pouze pro VLAN. Takto označený root switch rozesílá BPDU zprávy s nejvyšší váhou. Všechny porty root switche jsou ve stavu forwarding.
Designated port je proti root portu, jedná se o port, který vysílá BPDU zprávu, která má v segmentu největší váhu.
Alternate port je definován jako port, který není ani root, ani designated. Dostává BPDU zprávy s větší váhou BPDU od ji switche, který je ve stejném segmentu sítě. Je to port, který umožňuje alternativní cestu k root switchi. Tento alternate port může nahradit, v případě vypadnutí, root port.
Backup port má podobnou úlohu jako alternate. BPDU zprávy však dostává od portu stejného přepínače. Backup port nezaručuje cestu k root switchi, ale redundantní spojení do stejného segmentu sítě. Jako edge porty jsou označovány ty, které vedu ke koncovým stanicím. Jsou ve stavu forwarding, na obyčejný port se přepínají ve chvíli, kdy na ně přijde BPDU zpráva.



Obrázek 3: Možnosti označení portů u RSTP, zdroj: vlastní podle [61].

7.1.1 BPDU

Oproti STP používá RSTP všech osm flag bitů BPDU. V případě RSTP se používá tzv. BPDU type 2. Zařízení, které nerozpozná tuto BPDU zprávu, ji zahodí. Bity jsou využívání pro zašifrování stavu a role portu. BPDU nejsou zasílány jen root switchem, je tedy nutné rozlišit je podle směrodatnosti. Podle parametrů rozlišujeme důležitost zprávy. Jedná se o:

- ID root switche,
- Cost k root switchi,
- ID switche, za kterého byla zpráva odeslána.

Váha BPDU zprávy se liší podle parametrů, větší váhu získává pokud:

- BPDU obsahuje lepší root switch ID, čím nižší lepší,
- V případě stejného root switch ID rozhoduje cost k root switchi, čím nižší lepší,
- Pokud je obojí stejné, rozhoduje se podle switch ID, od kterého odchází zpráva, čím nižší lepší.

Zprávy jsou zasílány v intervalu hello-time a přenáší aktuální informace o stavu v síti. Jestliže nepřijde třikrát po sobě BPDU zpráva, je linka považována za

odpojenou. Pokud se tak stane na root portu, začne se switch chovat jako root switch a na své ostatní porty pošle BPDU s informací, že je root. Když jiný switch zachytí jinou vyslanou zprávu na svém portu, vyšle na svůj root port dotaz, zda je root switch dostupný. V případě, že je přes něj dostupný root switch, zašle na port, od kterého převzal BPDU zprávu o nedostupnosti root switche, zprávu, že je root switch dostupný přes něj. Původní switch zprávu akceptuje a již dále nebude vysílat informační BPDU zprávy [61].

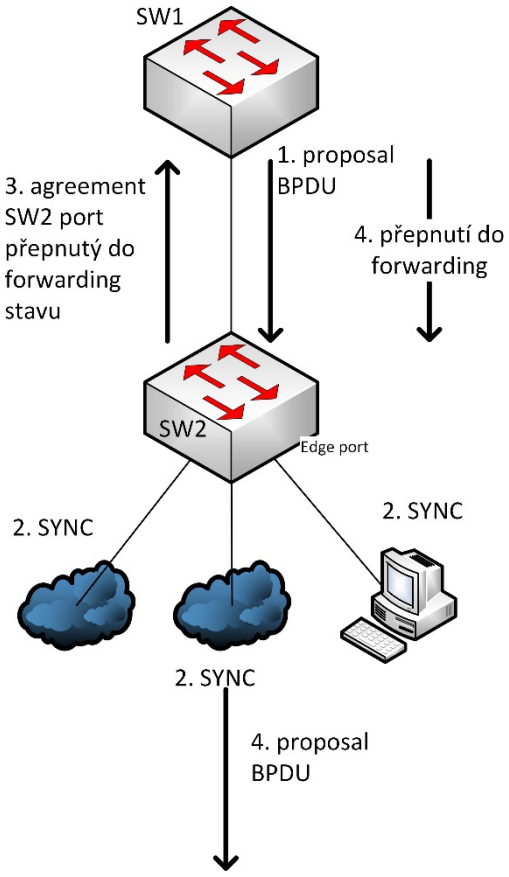
7.1.2 Proposal agreement systém v RSTP

K událostem v topologii může dojít, když je do stávající struktury připojen nový přepínač. RSTP využívá systém Proposal/Agreement ve spojeních typu point-to-point. Cílem je přepnutí portu do stavu forwarding bez vytvoření smyčky nebo narušení služeb.

Při přidání nové point-to-point linky mezi dva switche se oba porty, jsou oba ve výchozím stavu designated discarding. Porty ve stavu discarding nebo Learning rozesílají BPDU zprávy, kde mají nastavený proposal bit. Oba switche to udělají v případě, že mají oba porty nastavené ve stavu designated.

Pokud je BPDU přijato na designated discarding portu, je určeno jako nadřazeno. Jeho role se změní z designated na root discarding. V tomto procesu dojte také k aktualizaci rolí portů. Pokud switch příjme BPDU s proposal bitem na root portu, přepne všechny non-edge porty do stavu discarding. Tento mechanismus je nazýván jako synchronizace. Switch, který je v synchronizačním stavu, je izolován od sítě, díky tomu je zabráněno smyčkám.

Jakmile dojde k synchronizaci, switch přepne vybraný port do root stavu, forwarding stav informuje protější switch, že je na něj možné přesunout port do stavu learning nebo forwarding. To provádí switch, který odesílá BPDU s agreement bitem, je to root port po provedení synchronizace.



Obrázek 4: Proposal/Agreement systém, zdroj: vlastní zpracování.

7.2 Simulace IED

K měření bylo potřeba kromě průmyslových switchů zařízení, které bude generovat GOOSE zprávy. Ideálně ve velkém množství. Bohužel IED zařízení se nepodařilo sehnat, ale pomocí IED Builder od společnosti Gridsoftware, bylo nasimulováno jednoduché IED zařízení a vyexportováno do *.scl souboru. IED zařízení v takové podobě je xml dokument, který lze upravovat např. v poznámkovém bloku. V IED zařízení je nezbytné nastavit:

- VLAN ID – číslo VLAN, přes kterou bude GOOSE zpráva vysílána,
- MAC adresa protější stanice pro úspěšné doručení zprávy,
- DataSet – stavové informace, které jsou přenášené v GOOSE zprávě,
- Interval odesílání zpráv – časová hranice, která říká, v jakém rozmezí budou GOOSE zprávy odesílány.

Po vytvoření IED, je nutné použít další software, který umožní spustit simulaci a na druhém zařízení, v našem případě PC, software, který bude schopen zprávy přijímat. Takové podmínky splňuje program IEDScout od společnosti Omicron. Je poskytován v trial verzi na 30 dní. IEDScout umožňuje simulované IED také částečně upravovat (měnit DataSet, VLAN ID). Má také monitorovací systém, kde je zobrazena komunikace mezi IED a IEDScout přes navázání komunikace k zobrazení GOOSE toku zpráv apod.

Nejprve tedy došlo k otevření SCL souboru do IEDScout. Následně, na druhém zařízení v síti, bylo třeba zařízení objevit (Discover IED). Zařízení je objevitelné na IP adrese protějšího zařízení a portu, na kterém je spuštěna simulace. V případě používání firewallu nebo antiviru je nutné povolit komunikaci na daném portu nebo ochranu vypnout.

Na IED zařízení nutné spustit simulaci GOOSE zpráv. Při spuštění simulace lze vybrat druh zprávy a port, na kterém bude vysíláno. Pro sledování komunikace je vhodné mít zapnutý monitoring. Nejen na simulačních stanicích, ale i na dalších zařízeních v síti. Při měření byl na dvou stanicích u různých switchů spuštěn Wireshark. Sniffování probíhalo na sdružených portech ve SPANu, po kterých procházel síťový datový tok. Jednak, aby byl vidět tok GOOSE zpráv, druhý důvod byl zjišťování zpráv protokolu ohledně redundance sítě.

```
<GSE ldInst="LD0" cbName="GooseCB1">
          <Text source="txt">val1
val2</Text>
          <Address>
            <P type="VLAN-ID" xsi:type="tP_VLAN-ID">002</P>
            <P type="VLAN-PRIORITY" xsi:type="tP_VLAN-PRIORITY">1</P>
            <P type="MAC-Address" xsi:type="tP_MAC-Address">01-0C-CD-01-00-00</P>
            <P type="APPID" xsi:type="tP_APPID">0000</P>
          </Address>
          <MinTime unit="s" multiplier="m">2</MinTime>
          <MaxTime unit="s" multiplier="m">4</MaxTime>
        </GSE>
<PhysConn type="Connection" desc="phycsonn1">
          <P type="Cable">nn</P>
          <P type="Port">1</P>
          <P type="Type">1000BaseT</P>
          <P type="Plug">RJ45</P>
        </PhysConn>
```

Výše je zobrazena část zachycující nastavení IED zařízení, kde jsou specifikovány informace o VLAN, zdrojové MAC adrese, po jakém fyzickém médiu je připojené do sítě pro instanci nazvanou GooseCB1. Z ukázky je patrné, že zařízení bude pracovat ve VLAN 2, jakou má zdrojovou MAC adresu, a že GOOSE zprávy budou vysílány v intervalu od 2 do 4 milisekund. Zařízení je připojené metalickým kabelem skrze RJ45 rozhraní v rychlosti gigabitového Ethernetu.

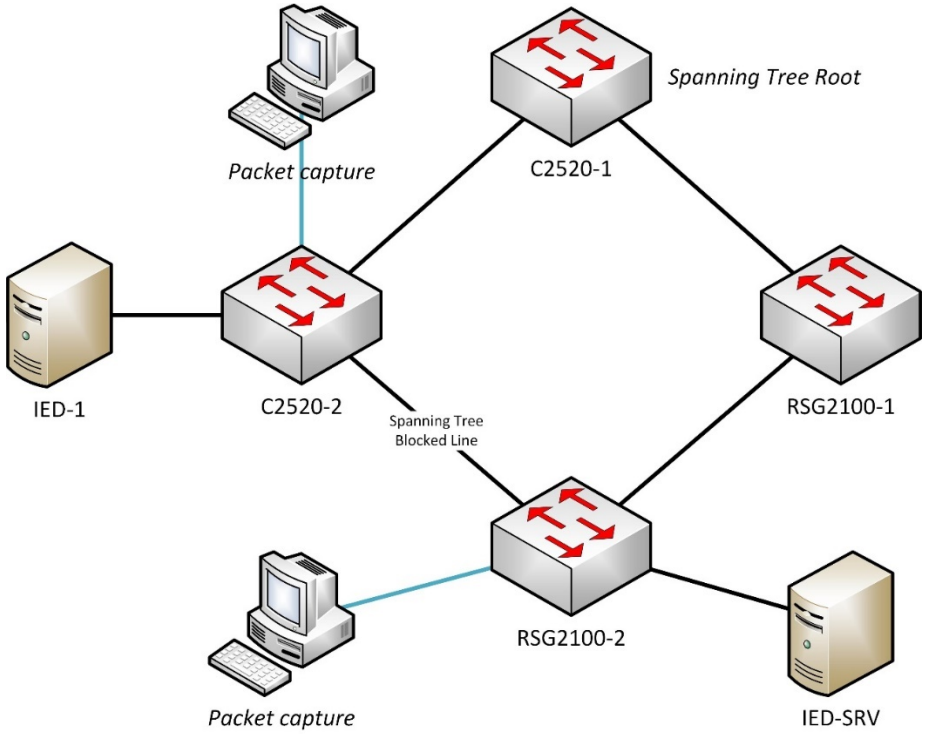
V následující ukázce je zobrazen DataSet a v něm uspořádání logických uzlů a logických zařízení, výrobce zařízení datum vytvoření apod.:

```
<IED name="TEMPLATE" manufacturer="Grid Software" originalSclVersion="2007"
originalSclRevision="B">
    <AccessPoint name="AP1">
      <Server timeout="30">
        <Authentication />
        <LDevice inst="LD0">
          <LN0 lnClass="LLN0" inst="" lnType="LLN0_f2c22b17-147e-46ae-9763-
9d2d64eaffd3">
            <DataSet desc="(created on Wednesday, April 05, 2017 3:35:52 PM)"
name="DataSet1">
              <FCDA ldInst="LD0" lnClass="LLN0" doName="Beh" daName="stVal" fc="ST" />
              <FCDA ldInst="LD0" lnClass="LLN0" doName="Beh" daName="t" fc="ST" />
              <FCDA ldInst="LD0" lnClass="LLN0" doName="Beh" daName="q" fc="ST" />
            </DataSet>
            <DOI name="Beh">
              <DAI name="q" sAddr="shAdd" valImport="false" valKind="Conf" />
            </DOI>
            <GSEControl desc="(created on Wednesday, 05 April 2017 14:46:54)"
name="GooseCB1" type="GOOSE" fixedOffs="false" confRev="1"
securityEnable="SignatureAndEncryption" appID="NULL" datSet="DataSet1" />
            <Protocol mustUnderstand="true">R-GOOSE</Protocol>
            </GSEControl>
          </LN0>
        </LDevice>
      </Server>
    </AccessPoint>
    <AccessPoint name="AP2" />
  </IED>
```

7.3 Měření

Při měření byla použita topologie zobrazena na obr. [5]. Switche byly propojeny optickými kabely, koncové zařízení metalicky. Měření probíhalo na protokolech MST a RSTP při výpadku linky mezi switchi na obrázku [5] označeny jako C2520-2 a RSG2100-2. Protože Cisco zařízení pracují na svých proprietární protokolech

PVST(+) nebo RPVST(+), čili řeší spanning tree pro každou VLAN síť, je nemožné ho v takové topologii použít. Byly tedy použity standardizované běžné protokoly.



Obrázek 5: Testovaná topologie

Další měření bylo provedeno při výpadku root switche a obnovení. U protokolu MST bylo provedeno celkem dvacetkrát. Každá GOOSE zpráva má také identifikátor, díky kterému lze zjistit, která zpráva nedorazila. Z tabulky [3], kde je uveden počet vypadlých zpráv je vidět, že největší ztráta zpráv je při výpadku root switche, kde je průměrná ztráta zpráv 21,667, se směrodatnou odchylkou 4,77. Naopak nejnižší výpadky byly zaznamenány při obnově linky mezi switchi.

Tabulka 3: Výpadky GOOSE zpráv a ICMP při použití MST.

ODPOJENÍ	ICMP VÝPADEK	PŘIPOJENÍ	ODPOJENÍ ROOTA	ICMP VÝPADEK	PŘIPOJENÍ ROOTA
15	**0**	**7**	**16**	**1**	**12**
16	1	6	20	1	5
16	**1**	**6**	**34**	**2**	**11**
16	1	6	25	2	12
16	**1**	**9**	**20**	**1**	**10**
17	1	6	18	1	6
14	**0**	**10**	**18**	**1**	**9**
20	1	6	22	1	11
13	**0**	**8**	**21**	**1**	**10**
18	1	3	23	1	11
17	**1**	**7**	**24**	**1**	**13**
18	1	8	25	2	11
19	**1**	**7**	**15**	**1**	**8**
16	1	8	27	2	10
15	**1**	**8**	**17**	**1**	**11**

Zdroj: vlastní zpracování.

U použití protokolu RSTP při výpadku byly nejhorší výsledky zaznamenány při obnovení root switche. Ač při výpadku root switche i linky docházelo k podobným výpadkům jako při použití MST, tak při zpětném procesu konvergence při zapojení docházelo k rapidním výpadkům jak ICMP paketů vysílaných v intervalu 50ms, tak k výpadkům GOOSE zpráv. Doba konvergence přesahovala 30s. V tabulce [4] jsou uvedeny výsledky testování RSTP protokolu.

Tabulka 4: Výpadky GOOSE a ICMP zpráv při použití RSTP.

PŘIPOJENÍ ROOTA	ICMP VÝPADEK
9163	**208**
9008	205
8713	**202**
9066	204
9262	**208**
8917	203
9290	**208**
9144	205
9004	**204**
8953	203
9601	**201**
8703	202
9007	**204**
9162	208
9027	**205**

Zdroj: vlastní zpracování

Ještě před konfigurací Cisco switchů, protože došlo k nesprávnému připojení zdrojového kabelu, došlo k výpisu chybových hlášek do konzole, dokonce nefungovaly ani již nakonfigurované porty. Po připojení zemnícího vodiče již bylo vše v pořádku. Je nutné podotknout, že zásah do elektrického rozvodu může provést pouze kvalifikovaný elektrikář, který má elektrikářské zkoušky, konkrétně vyhlášku č. 50/1978 o odborné způsobilosti v energetice.

8 Shrnutí výsledků

Z testování a měření vcelku jasně vyplývá, že pro vyžadovaný chod sítě se zařízeními od různých výrobců, je nezbytné použití protokolu MST. Další možností zapojení sítě je, pokud to lze a je dostatek zařízení, zokruhovat v rámci rozvodny pouze zařízení stejného výrobce, kde za použití proprietárního protokolu nebo RSTP bude docházek ke konvergenci v předpokládané době. Nicméně to stále neřeší konvergenci sítě v celém sektoru při výpadku centrálního prvku.

Protokol MST je použit také proto, že zařízení Cisco mají svůj spanning tree protokol proprietární. Protokoly PVST, PVST+ a RPVST+ používají spanning tree instanci pro každou VLAN síť zvlášť. Kdežto ostatní zařízení používají při jakékoliv verzi STP jednu instanci pro všechny VLAN sítě. Oba způsoby mají své výhody i nevýhody. Použití Cisco protokolů umožňuje mít pro různé VLAN sítě různé přístupové cesty, síť se však bude zaplavovat BPDU zprávami. Při použití neproprietárního STP protokolu bude BPDU zpráv chodit méně, nicméně při výpadku linky dojde k přerušení datového toku u všech VLAN sítí najednou. MST protokol využívá pro rychlou konvergenci, stejně jako RSTP, princip Proposal/Agreement. Díky tomuto principu je MST, jak ukázalo měření, pro průmyslové sítě nepostradatelný.

Simulované zprávy GOOSE přenášené při testování byly vysílány ve stejném nebo velmi podobném intervalu jako při reálné komunikaci. V reálné komunikaci je nesmí být očekávaná doba mezi GOOSE zprávami delší než 4ms.

Zařízení Hirschmann se nepodařilo s ostatními zařízeními zkonvergovat v rozumné době, neboť nepodporuje standardizovaný protokol MST. Bohužel nepřesvědčilo ani v možnostech konfigurace, konkrétně webové rozhraní napsané v Javě. V dnešní době je již přeci jenom tyto webové technologie přežité. Za povšimnutí stojí, že v dnešní době nemá společnost Hirschmann ve svých zařízeních implementovaný standardizovaný protokol.

9 Závěr

V práci byly představeny rozdíly v použití Ethernetu v prostředí kancelářském a průmyslovém. Byl představen a vysvětlen pojem Smart Grid, včetně praktických příkladů použití. Je velmi pravděpodobné, že se tento koncept bude nadále rozvíjet. Pokud však bude Smart Grid síť používána na veřejné síti, mohou existovat hrozby v podobě útoků hackerů. Může tak docházet např. ke krádeži informací z elektroměrů a následným úpravám hodnot nebo vydírání zákazníka. Pořizovací náklady také nejsou nízké.

U průmyslových protokolů byly popsány jejich modely komunikace se zařízeními a principy synchronizace. Díky Ethernetu v průmyslovém prostředí lze optimalizovat produktivitu. Přináší také výhody kancelářského Ethernetu (spolehlivost, jednoduchá rozšiřitelnost). Stále se vyvíjející standard IEC 61850, který definuje standardy pro komunikaci, má v energetickém prostředí velmi podstatnou roli. Vývoj dokazuje standard IEC 61850-9-3 z roku 2016, který přináší lepší distribuci času v rozvodnách pomocí protokolu PTP.

V rámci protokolů byly vysvětleny principy komunikace a získávání informací pomocí SCADA systémů. SCADA systému jsou a budou v průmyslovém monitoringu nezbytnou součástí pro kvalitní správu sítě a řešení případných problémů.

Pro praktické měření by bylo vhodné, kdyby místo simulování IED bylo použité opravdové zařízení a sledovat provoz použitím SCADA/HMI systému. Z výsledků vyplývá, že vždy k nějakému výpadku dojde, při použití protokolu MST však bude výpadek minimální. Bylo prakticky ověřeno, že pokud zařízení různých výrobců nepodporuje standardizované protokoly, stává se v daném okamžiku nepoužitelným.

Nedílnou součástí energetické sítě je její bezpečnost, především fyzická ostraha. Do rozvodny smí mít přístup pouze oprávnění lidé (správci), zaměstnanci dané společnosti nesmí manipulovat se zařízeními ani používat flash paměti, či jiné zařízení, na kterých lze přenášet data. K zabezpečení patří samozřejmě nejen fyzické ale i firewally, šifrování komunikace, používání VPN a další funkce zabezpečení (bezpečnostní politiky spolčenosti apod.). Pokud dojde k infiltraci sítě a případné rekonfiguraci může nastat výpadek sítě nebo další, mnohdy horší hrozby

(kybernetický útok, zavirování apod.) a zcela jistě dojde i k finančním ztrátám. Nicméně v energetickém průmyslu jsou možná horší než finanční ztráty výpadky energetické sítě nebo úplné zamezení dodávek elektrické dodávky.

10 Seznam použité literatury

[1] ZEZULKA, František a Ondřej HYNČICA. Průmyslový Ethernet I: Historický úvod. *Automa*. 2007, (1), 3. Dostupné také z: http://automa.cz/cz/casopis-clanky/prumyslovy-ethernet-i-historicky-uvod-2007_01_34298_2430/.

[2] BOUŠKA, Petr. Počítačové sítě a jejich typy. Samuraj [online]. 2007 [cit. 2016-08-29]. Dostupné z: http://www.samuraj-cz.com/clanek/pocitacove-site-a-jejich-typy/.

[3] ZEZULKA, František a Ondřej HYNČICA. Průmyslový Ethernet II: Referenční model ISO/OSI. Automa. 2007, 2007(3), 5. Dostupné také z: http://automa.cz/cz/casopis-clanky/prumyslovy-ethernet-ii-referencni-model-iso/osi-2007_03_34209_3890/

[4] BOUŠKA, Petr. Počítačové sítě a jejich typy. Samuraj [online]. 2007 [cit. 2016-08-30]. Dostupné z: http://www.samuraj-cz.com/clanek/osi-model/

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

[6] Sítě průmyslového Ethernetu: Profinet - 1.TIA. Siemens [online]. c2001 [cit. 2017-02-20]. Dostupné z: https://w5.siemens.com/web/cz/cz/corporate/portal/home/produkty_a_sluzby/IADT/tia_na_dosah/Documents/1.%20TIA_Site_prumysloveho_Ethernetu.pdf

[7] BOUŠKA, Petr. TCP/IP - routing - směrování. Samuraj [online]. 2007 [cit. 2017-02-24]. Dostupné z: http://www.samuraj-cz.com/clanek/tcpip-routing-smerovani/

[8] Cisco networking Academy: CCNA 1: 6.1.3 IPv4 Packet [online]. San Jose, USA: Cisco Systems, c2015 [cit. 2017-03-27]. Dostupné z: www.netacad.com

[9] Cisco networking Academy: CCNA 1: 6.1.4 IPv6 Packet [online]. San Jose, USA: Cisco Systems, c2015 [cit. 2017-03-27]. Dostupné z: www.netacad.com

[10] BOUŠKA, Petr. Adresování v IP sítích. Samuraj [online]. 2007 [cit. 2017-03-3]. Dostupné z: http://www.samuraj-cz.com/clanek/adresovani-v-ip-sitich/

[11] ODVÁRKA, Petr. ICMP - Internet Control Message Protocol. Svět sítí [online]. 2001 [cit. 2017-03-04]. Dostupné z: http://www.svetsiti.cz/clanek.asp?cid=ICMP-Internet-Control-Message-Protocol-1012001

[12] ICMP. Mendelova univerzita v Brně [online]. [cit. 2017-03-05]. Dostupné z: https://is.mendelu.cz/eknihovna/opory/zobraz_cast.pl?cast=597

[13] Cisco 829 Industrial Integrated Services Routers. Cisco [online]. [cit. 2017-03-05]. Dostupné z: http://www.cisco.com/c/en/us/products/routers/829-industrial-router/index.html

[14] Cisco Nexus 5000 Series NX-OS System Management Configuration Guide, Release 5.2(1)N1(1). Cisco [online]. 2014 [cit. 2017-03-05]. Dostupné z: http://www.cisco.com/c/en/us/td/docs/switches/datacenter/nexus5000/sw/system_management/521_n1_1/b_5k_System_Mgmt_Config_521N11/b_5k_System_Mgmt_Config_521N11_chapter_0110.html#concept_2AFC73E113214F55B2147E0F3CB3DAAF

[15] ZEZULKA, František a Ondřej HYNČICA. Průmyslový Ethernet III: Fyzické provedení sítě Ethernet. Automa. 2007, (6), 5. Dostupné také z: http://automa.cz/cz/casopis-clanky/prumyslovy-ethernet-iii-fyzicke-provedeni-site-ethernet-2007_06_34395_2402/

[16] Použití optických mediakonvertorů v síti Ethernet: Co vám přinese redundance. Moxa [online]. 2009 [cit. 2017-03-07]. Dostupné z: http://www.moxa.cz/zpravodaj/2009/08/Pouziti-optickych-mediakonvertoru-v-siti-Ethernet.htm

[17] BOUŠKA, Petr. Cisco IOS 10 - Rapid Spanning Tree Protocol. Samuraj [online]. 2007 [cit. 2017-03-07]. Dostupné z: http://www.samuraj-cz.com/clanek/cisco-ios-10-rapid-spanning-tree-protocol/

[18] HOSSAIN, Ekram, Zhu HAN a H. POOR. Smart Grid communications and networking. NewYork: Cambridge University Press, 2012, xxviii, 481 p. ISBN 978-110-7014-138

[19] DIVIŠ, Roman. Principy bezpečností Smart Grid sítí [online]. Pardubice, 2013 [cit. 2017-03-10]. Dostupné z: http://dspace.upce.cz/bitstream/handle/10195/52349/DivisR_PrincipyBezpecnosti_JH_2013.pdf?sequence=3

[20] Grid Modernization and the Smart Grid. Energy.gov [online]. 2007 [cit. 2017-03-10]. Dostupné z: http://energy.gov/oe/technology-development/smart-grid

[21] Smart lavička je český vynález. Startitup [online]. 2016 [cit. 2017-03-10]. Dostupné z: https://www.startitup.cz/smart-lavicka-je-cesky-vynalez/

[22] Průmyslový Ethernet versus Ethernet [online prezentace]. In: GROSMAN, Josef. [cit. 2017-03-15]. Dostupné z: www.fm.tul.cz/esf0247/index.php?download=880

[23] Certifikace podle IEC 61850-3 je důležitým faktorem při výběru zařízení pro automatizaci rozvoden. Moxa [online]. 2010 [cit. 2017-03-13]. Dostupné z: http://www.moxa.cz/zpravodaj/2010/01/Certifikace-podle-IEC-61850-3-je-dulezitym-faktorem-pri-vyberu-zarizeni-pro-automatizaci-rozvoden.htm

[24] RONEŠOVÁ, Andrea. Přehled protokolu MODBUS. 2005, , 20. Dostupné také z: http://home.zcu.cz/~ronesova/bastl/files/modbus.pdf

[25] VOJÁČEK, Antonín. Modbus. 2004, 20. Dostupné také z: http://automatizace.hw.cz/clanek/2004070701

[26] ZEZULKA, František a Ondřej HYNČICA. Průmyslový Ethernet IX: EtherNet/IP, EtherCAT. Automa. 2008, (10), 5. Dostupné také z: http://automa.cz/cz/casopis-clanky/prumyslovy-ethernet-ix-ethernet/ip-ethercat-2008_10_37910_6510/

[27] SCHIFFER, Viktor, VANGOMPEL, David J., Raymond A. ROMITO a Katherine VOSS, ed. The Common Industrial Protocol (CIP™) and the Family of CIP Networks. Brno: ODVA, 2016.

[28] Profinet Technology. Profinet [online]. [cit. 2017-03-19]. Dostupné z: http://www.profibus.com/technology/profinet/

[29] PROFINET - Standard pro průmyslový Ethernet v automatizaci. 2005, , 16. Dostupné z: http://stest1.etnetera.cz/ad/current/content/data_files/automatizacni_systemy/prumyslova_komunikace/profinet/profinet_04_2005_cz.pdf

[30] ZEZULKA, František a Ondřej HYNČICA. Průmyslový Ethernet VIII: Ethernet Powerlink, Profinet. Automa. 2008, (5), 5. Dostupné také z: http://automa.cz/Aton/FileRepository/pdf_articles/37288.pdf

[31] IEC 61850: Soubor norem pro komunikaci v energetice. Pandatron.cz [online]. 2011 [cit. 2017-03-23]. Dostupné z: https://pandatron.cz/?2663&iec_61850:_soubor_norem_pro_komunikaci_v_energetice

[32] Enhanced protection functionality with IEC 61850 and GOOSE [online prezentace]. In: . 2008, s. 38 [cit. 2017-03-21]. Dostupné z: http://www02.abb.com/global/sgabb/sgabb005.nsf/bf177942f19f4a98c1257148003b7a0a/e81bb489e5ae0b68482574d70020bf42/$FILE/B5_G2_Enhanced+protection+functionality+with+IEC+61850+and+GOOSE.pdf

[33] ZHANG Jianqing a Carl A. GUNTER. IEC 61850 - Communication Networks and Systems in Substations:An Overview of Computer Science [online prezentace]., Illinois security lab [cit. 2017-03-22]. Dostupný z: http://www.ics.muni.cz/mba/eiz/eiz11c-6.pdf

[34] KRIGER, Carl, Shaheen BEHARDIEN a John-Charly RETONDA-MODIYA. Enhanced protection functionality with IEC 61850 and GOOSE [online]. 2008, s. 14 [cit. 2017-03-22]. ISSN 841-9836. Dostupné z: http://univagora.ro/jour/index.php/ijccc/article/viewFile/329/pdf_66

[35] International Standard. : IEC 61850-5 [online]. International Electrotechnical Commission, c2003 [cit. 2017-03-22]. Dostupné z: http://www.normservis.cz/download/view/iec/info_iec61850-5%7Bed1.0%7Den.pdf

[36] ČESKÁ TECHNICKÁ NORMA. : IEC 61850-7-3 [online]. 2004 [cit. 2017-03-22]. Dostupné z: http://csnonlinefirmy.unmz.cz/html_nahledy/33/69596/69596_nahled.htm

[37] International Standard. : IEC 61850-9-3 [online]. International Electrotechnical Commission, 2016 [cit. 2017-03-22]. Dostupné z: https://webstore.iec.ch/preview/info_iecieee61850-9-3%7Bed1.0%7Den.pdf

[38] ČESKÁ TECHNICKÁ NORMA. : IEC 61850-10 [online]. 2006 [cit. 2017-03-22]. Dostupné z: http://csnonlinefirmy.unmz.cz/html_nahledy/33/74981/74981_nahled.htm

[39] Designing Non-Deterministic PAC Systems to Meet Deterministic Requirements. PAC World magazine [online]. New York, USA, 2015 [cit. 2017-03-23]. Dostupné z: https://www.pacw.org/no-cache/issue/june_2015_issue/deterministic_system/designing_nondeterministic_pac_systems_to_meet_deterministic_requirements.html

[40] ČESKÁ TECHNICKÁ NORMA. : IEC 61850-6 [online]. 2006 [cit. 2017-03-22]. Dostupné z: http://csnonlinefirmy.unmz.cz/html_nahledy/33/74942/74942_nahled.htm

[41] ČESKÁ TECHNICKÁ NORMA. : IEC 61850-7 [online]. 2005 [cit. 2017-03-22]. Dostupné z: http://csnonlinefirmy.unmz.cz/html_nahledy/33/72570/72570_nahled.htm

[42] MMS Objects and Services. The Net is the Automation [online]. 2015 [cit. 2017-03-25]. Dostupné z: http://www.nettedautomation.com/standardization/ISO/TC184/SC5/WG2/mms_intro/intro4.html

[43] FORGUE, Bruno a Pavel VLADYKA. IEC 61850 : soubor norem pro komunikaci v energetice s velkým potenciálem výhod. Automa [online]. 2010, (3), 1-3 [cit. 2017-03-23]. Dostupné z: http://automa.cz/Aton/FileRepository/pdf_articles/40771.pdf

[44] International Standard. : IEC 61850-9-3 [online]. International Electrotechnical Commission, 2016 [cit. 2017-03-22]. Dostupné z: http://www.teias.gov.tr/IEC/iec60870-5-101%7Bed2.0%7Den.pdf

[45] IEC 60870-5-101. IPCOM GmbH [online]. [cit. 2017-03-22]. Dostupné z: http://www.ipcomm.de/protocol/IEC101/en/sheet.html

[46] IEC 60870-5-104. IPCOM GmbH [online]. [cit. 2017-03-22]. Dostupné z: http://www.ipcomm.de/protocol/IEC104/en/sheet.html

[47] Overview of the DNP3 Protocol. DNP [online]. 2011 [cit. 2017-03-23]. Dostupné z: https://www.dnp.org/pages/aboutdefault.aspx

[48] Modbus and DNP3 Communication Protocols [online]. [cit. 2017-03-24]. Dostupné z: https://scadahacker.com/library/Documents/ICS_Protocols/Triangle%20Microworks%20-%20Modbus-DNP3%20Comparison.pdf

[49] BOUŠKA, Petr. Začínáme s monitoringem sítě. Connect [online]. 2009, (09) [cit. 2017-03-24]. Dostupné z: http://www.samuraj-cz.com/clanek/zaciname-s-monitoringem-site/

[50] SNMP objekty a MIB. Svět sítí [online]. [cit. 2017-03-24]. Dostupné z: http://www.svetsiti.cz/clanek.asp?cid=SNMP-objekty-a-MIB-1362000

[51] BOUŠKA, Petr. SNMP - Simple Network Management Protocol. Samuraj [online]. 2006 [cit. 2017-03-25]. Dostupné z: http://www.samuraj-cz.com/clanek/snmp-simple-network-management-protocol/

[52] RFC 1157 – Simple Network Management Protokol [online]. [cit. 2017-03-20]. Dostupné z: https://tools.ietf.org/html/rfc1157

[53] OREBAUGH, Angela. Wireshark a Ethereal: kompletní průvodce analýzou a diagnostikou sítí. Brno: Computer Press, 2008. ISBN 978-80-251-2048-4.

[54] GOOSER. TMV SS [online]. [cit. 2017-03-26]. Dostupné z: http://www.tmvss.cz/vyrobci/programma-megger/gooser

[55] Cisco networking Academy: CCNA 4: Chapter 8 - Monitoring the Network [online]. San Jose, USA: Cisco Systems, c2015 [cit. 2017-03-27]. Dostupné z: www.netacad.com

[56] VOREL, David. Bezpečnostní monitoring – SIEM [online prezentace]. [cit. 2017-03-25]. Dostupné z: https://www.nic.cz/public_media/IT14/prezentace/David_Vorel.pdf

[57] SCADA – The Brain of the Smart Grid. Remote Site and Equipment Management [online]. 2014 [cit. 2017-03-27]. Dostupné z: http://www.remotemagazine.com/main/articles/scada-the-brain-of-the-smart-grid/

[58] GooseAir v. 1.5.1. GridSoftware [online]. [cit. 2017-03-27]. Dostupné z: http://www.gridsoftware.com/docs/pdf/gooseAir_Manual.pdf

[59] GosoerMeter One IEC 61850 message monitor. ELECTRICAL TESTING EQUIPMENT - SMCint [online]. [cit. 2017-03-28]. Dostupné z: http://smcint.com/product/goosemeter-one-iec-61850/

[60] BALDA, Pavel. SCADA a HMI systémy [online prezentace]. Plzeň, 2007 [cit. 2017-03-29]. Dostupné z: http://vendulka.zcu.cz/Download/Free/IRS1/IRS1-08_SCADA_HMI.pdf

[61] KUBÍN, Roman a Michal BOHÁČ. Rapid Spanning Tree Protocol (802.1w). Remote Site and Equipment Management [online]. VŠB Ostrava, 2005 [cit. 2017-04-10]. Dostupné z: http://www.cs.vsb.cz/grygarek/SPS/projekty0405/RSTP-Kubin-Rohac.pdf

[62] Spanning Tree Protocol: RSTP Proposal/Agreement Process. Be The Packets - CCIE Study Blog [online]. [cit. 2017-04-13]. Dostupné z: https://bethepacketsite.wordpress.com/2016/02/29/spanning-tree-protocol-rstp-proposalagreement-process/

[63] SNMP response processing. IBM Knowledge Center [online]. [cit. 2017-04-25]. Dostupné z: https://www.ibm.com/support/knowledgecenter/en/ssw_aix_61/com.ibm.aix.networkcomm/snmpv1_daemon_respnsprcess.htm

[64] HOLMAN, Jan. SNMP a monitoring sítě [online]. [cit. 2017-04-25]. Dostupné z: http://www.fi.muni.cz/~kas/pv090/referaty/2015-podzim/snmp.html

[65] KLAŠKA, Luboš. Model Manager - Agent. Svět sítí [online]. 2000 [cit. 2017-04-25]. Dostupné z: http://www.svetsiti.cz/clanek.asp?cid=Model-Manager-Agent-1262000

[66] SNMP Protocol Basic Request/Response Information Poll Using GetRequest and (Get)Response Messages. The TCP/IP Guide [online]. 2005 [cit. 2017-04-25]. Dostupné z: http://www.tcpipguide.com/free/t_SNMPProtocolBasicRequestResponseInformationPollUsi.htm

[67] Using the SNMP GetBulk request for data retrieval. *IBM: DeveloperWorks* [online]. [cit. 2017-04-25]. Dostupné z: https://www.ibm.com/developerworks/ibmi/library/i-snmp-getbulk-data-retrieval/

[68] Projekt Smart Region ve Vrchlabí. *ČEZ Distribuce* [online]. [cit. 2017-04-26]. Dostupné z: http://www.cezdistribuce.cz/cs/pro-media/smart-region.html

Univerzita Hradec Králové
Fakulta informatiky a managementu
Akademický rok: 2015/2016

Studijní program: Aplikovaná informatika
Forma: Prezenční
Obor/komb.: Aplikovaná informatika (ai3-p)

Podklad pro zadání BAKALÁŘSKÉ práce studenta

PŘEDKLÁDÁ:	ADRESA	OSOBNÍ ČÍSLO
Hájek Vojtěch	Dolení 168, Jilemnice	I1301270

TÉMA ČESKY:

Monitoring průmyslových sítí v energetice

TÉMA ANGLICKY:

Monitoring of Industrial Networks in Energetics

VEDOUCÍ PRÁCE:

Ing. Ondřej Hornig - KIT

ZÁSADY PRO VYPRACOVÁNÍ:

Cílem práce je podrobně představit komunikační mechanismy v průmyslových sítích používaných řídícími systémy v energetickém průmyslu. Přiblíží základní principy a funkce IP sítí s protokoly Ethernet a IEC 61850, které se standardně používají v energetických řídících sítích. Pro klíčové služby, které práce v takových sítích identifikuje, navrhne ve své praktické části řešení za pomocí standardizovaných protokolů v IP sítích.

Osnova:
1. Uvod
2. Průmyslové datové sítě
3. Protokoly průmyslového Ethernetu
4. Nástroje monitoringu
5. Měření konvergence v heterogenních přepínaných sítích
6. Shrnutí výsledků
7. Závěr

SEZNAM DOPORUČENÉ LITERATURY:

DOSTÁLEK, Libor.; KABELOVÁ, Alena. Velký průvodce protokoly TCP/IP a systémem DNS. 5. aktualizované vydání, Brno: Computer Press, a.s., 2008. 488 s. ISBN 978-80-251-2236-5.

HICKS, Michael. Optimizing Applications on Cisco Networks. 1. vydání. Indianapolis: Cisco Press, 2004. 384 s. ISBN: 978-1-58705-153-1.

HUCABY, David. CCNP SWITCH 642-813 Official Certification Guide. 1. vydání. Indianapolis: Cisco Press, 2011, 533 s. ISBN 978-1-58720-243-8.

RANJBAR, Amir. Troubleshooting and Maintaining Cisco IP Networks (TSHOOT). 1. vydání. Indianapolis: Cisco Press, 2010. 392 s. ISBN: 978-1-58705-876-9.

Podpis studenta: .....

Datum: 26. 4. 2017

Podpis vedoucího práce: .....

Datum: 26. 4. 2017