VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

Fakulta elektrotechniky
a komunikačních technologií

DIPLOMOVÁ PRÁCE

Brno, 2020 Bc. Lukáš Rusz

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
BRNO UNIVERSITY OF TECHNOLOGY

FAKULTA ELEKTROTECHNIKY A KOMUNIKAČNÍCH TECHNOLOGIÍ
FACULTY OF ELECTRICAL ENGINEERING AND COMMUNICATION

ÚSTAV TELEKOMUNIKACÍ
DEPARTMENT OF TELECOMMUNICATIONS

SIMULAČNÍ PROSTŘEDÍ STANDARDU IEC 61850
IEC 61850 SIMULATION ENVIRONMENT

DIPLOMOVÁ PRÁCE
MASTER'S THESIS

AUTOR PRÁCE — **Bc. Lukáš Rusz**
AUTHOR

VEDOUCÍ PRÁCE — **Ing. Petr Blažek**
SUPERVISOR

BRNO 2020

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
FAKULTA ELEKTROTECHNIKY A KOMUNIKAČNÍCH TECHNOLOGIÍ

Diplomová práce

magisterský navazující studijní obor **Telekomunikační a informační technika**

Ústav telekomunikací

Student: Bc. Lukáš Rusz ***ID:*** 213504
Ročník: 2 ***Akademický rok:*** 2019/20

NÁZEV TÉMATU:

Simulační prostředí standardu IEC 61850

POKYNY PRO VYPRACOVÁNÍ:

Práce je zaměřena na vytvoření softwarového nástroje pro simulování komunikace protokolů ze standardu IEC 61850. Student provede analýzu komunikačního standardu IEC 61850. Bude proveden výběr softwarového prostředí pro simulaci (např. NS3/NS2, OPNET, OMNET++ a další). Následně budou implementovány protokoly (MMS, SMV, GOOSE, SNTP a další) do simulačního prostředí a realizace celé průmyslové komunikační infrastruktury. Výsledkem práce bude prostředí, které bude simulovat komunikaci od koncových prvků až po dohledové centrum SCADA dle standardu IEC 61850. Dílčím cílem práce bude analýza zranitelností standardu IEC 61850 a návrh mitigačních opatření, která budou ověřena v simulovaném prostředí. V neposlední řadě bude umožněno nahrávání komunikace ve formátu *.pcap souborů (např. integrací přes Wireshark či jiným vybraným způsobem).

DOPORUČENÁ LITERATURA:

[1] W. Huang, "Learn IEC 61850 configuration in 30 minutes," 2018 71st Annual Conference for Protective Relay Engineers (CPRE), College Station, TX, 2018, pp. 1-5.doi: 10.1109/CPRE.2018.8349803

[2] CHAMBERLAIN, Thomas. Learning OMNeT++. Birmingham: Packt Publishing, 2013. ISBN 978-1849697149.

Termín zadání: 3.2.2020 ***Termín odevzdání:*** 1.6.2020

Vedoucí práce: Ing. Petr Blažek

prof. Ing. Jiří Mišurec, CSc.
předseda oborové rady

ABSTRAKT

Práce se zabývá komunikačními protokoly standardu IEC 61850. Jsou popsány protokoly GOOSE (Generic Object Oriented Substation Events),SMV (Sampled Measured Values) a MMS (Manufacturing Message Specification). Protokoly jsou použity pro vytvoření simulační sítě, která je popsána v této práci. Simulační síť je vytvořená v programu OMNeT++, instalovaném ve virtuálním prostředí Ubuntu.

KLÍČOVÁ SLOVA

SCADA, GOOSE, SMV, IED, OMNeT++, simulace, simulační prostředí

ABSTRACT

The work deals with communication protocols of the IEC 61850 standard. The protocols GOOSE (Generic Object Oriented Substation Events), SMV (Sampled Measured Values) and MMS (Manufacturing Message Specification) are described. The protocols are used to create a simulation network, which is described in this work. The simulation network is created in the OMNeT ++, program installed in the Ubuntu virtual environment.

KEYWORDS

SCADA, GOOSE, SMV, IED, OMNeT++, simulation, simulation environment

RUSZ, Lukáš. *Simulační prostředí standardu IEC 61850* . Brno, 2020, 58 s. Diplomová práce. Vysoké učení technické v Brně, Fakulta elektrotechniky a komunikačních technologií, Ústav telekomunikací. Vedoucí práce: Ing. Petr Blažek

PROHLÁŠENÍ

Prohlašuji, že svou diplomovou práci na téma „Simulační prostředí standardu IEC 61850 “ jsem vypracoval samostatně pod vedením vedoucího diplomové práce a s použitím odborné literatury a dalších informačních zdrojů, které jsou všechny citovány v práci a uvedeny v seznamu literatury na konci práce.

Jako autor uvedené diplomové práce dále prohlašuji, že v souvislosti s vytvořením této diplomové práce jsem neporušil autorská práva třetích osob, zejména jsem nezasáhl nedovoleným způsobem do cizích autorských práv osobnostních a/nebo majetkových a jsem si plně vědom následků porušení ustanovení § 11 a následujících autorského zákona č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon), ve znění pozdějších předpisů, včetně možných trestněprávních důsledků vyplývajících z ustanovení části druhé, hlavy VI. díl 4 Trestního zákoníku č. 40/2009 Sb.

Brno ....

podpis autora

PODĚKOVÁNÍ

Rád bych poděkoval vedoucímu diplomové práce panu Ing.Petru Blažkovi, za odborné vedení, konzultace, trpělivost a podnětné návrhy k práci.

Obsah

Seznam obrázků

Seznam tabulek

Seznam výpisů

Úvod

Elektrická síť čelí v dnešní době bezprecedentní poptávce a snaží se vyhovět novým požadavkům v distribuci elektrické energie. Faktory dnešní doby, které mění povahu a požadavky elektrické sítě, jsou například zvýšená poptávka po energii, výroba z obnovitelných zdrojů nebo vznik elektrických vozidel. Mnoho energetických společností hledá řešení inteligentních měření a inteligentních sítí, která jim pomohou tyto výzvy řešit.

Nasazují se proto nové systémy, kterým je například SCADA (Supervisory Control And Data Acquisition). Jedná se o systém pro řízení a sběr dat, který je zaměřen na dispečerský dohled, monitoring a případnou parametrizaci sítě. Systém je provozován nad úrovni hardwaru a zprostředkovává sběr dat z měřičů, čidel, ale i z celých technologických procesů. SCADA systémy již v dnešní době používají ke komunikaci počítačové sítě a masivně integrují Web technologie. Díky tomu jsou v dnešní době možné vzdálené přístupy a dohled prostřednictvím internetu.

Cílem této práce je obecné seznámení s pojmem inteligentní síť. Dále je popsán systém SCADA, který je důležitý ke správě a řízení rozvoden elektrické energie. Podrobně je zde popsán standard IEC 61850, který je stěžejní pro komunikaci mezi zařízeními v rozvodnách. Součástí tohoto standardu jsou komunikační protokoly GOOSE, SV a MMS které jsou zahrnuty v této práci.

V praktické části této práce je vybrán vhodný simulační nástroj a rozšiřující knihovny, potřebné k simulaci komunikace mezi protokoly ze standardu IEC 61850. Následně je popsaná instalace samotného simulačního prostředí a potřebných frameworků k realizaci celé simulace. Výstupem praktické části je funkční simulační prostředí, s vytvořenou sítí a následná simulace přenosu a zasílání kritických zpráv dle standardu 61850.

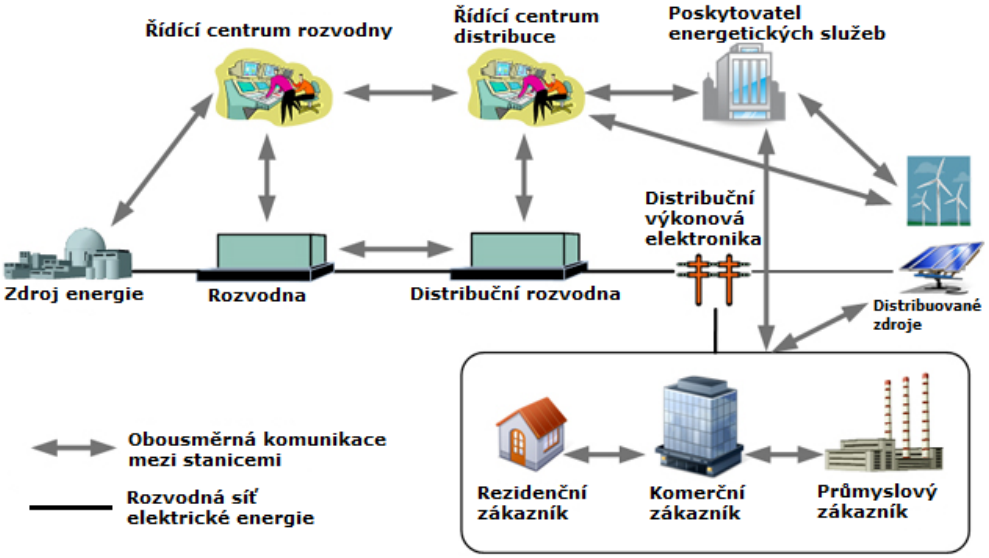
1 Inteligentní síť (Smart grid)

Inteligentní síť [1] je systém, který využívá informační a komunikační technologie z hlediska výroby, distribuce a spotřeby elektrické energie, aby zlepšila spolehlivost a služby, snížila náklady a zvýšila účinnost a stabilitu rozvodné sítě. Inteligentní síť má tři základní znaky, kterými jsou plná automatizace, plná integrace koncových zákazníku a adaptace na různé způsoby výroby elektrické energie.

Plná automatizace znamená zapojení řídícího a kontrolního systému společně se senzory monitorujícími chování sítě a automatické obnovování provozu po případné poruše. Zásluhou plné automatizace jsou v reálném čase k dispozici informace o zatížení sítě, kvalitě dodávky elektřiny, přerušení dodávky apod.

Plná integrace koncových zákazníků spočívá ve vybavení zákazníků takzvanými inteligentními elektroměry (Smart meter), které umožňují obousměrný přenos informací v reálném čase. Řešení umožňuje tvorbu cenových tarifů podle aktuální situace v elektrické síti. Plná integrace koncových zákazníků umožňuje odběratelům elektrické energie efektivně řídit spotřebu. Mohou například vytápět, prát prádlo nebo ohřívat vodu v době s volnou výrobní kapacitou.

Třetím základním znakem inteligentních sítí je adaptace na různé zdroje výroby elektrické energie. Umožňuje to zapojení dalších zdrojů elektrické energie, kterými jsou například solární, vodní a větrné elektrárny. Díky této technologii je možné, aby přebytky elektrické energie vyrobené zákazníky z vlastních zdrojů, byly prodávány zpět do sítě. Pro princip komunikace byl vytvořen konceptuální model tvořen stanicemi, mezi kterými je komunikační nebo elektrické spojení (viz obrázek 1.1).

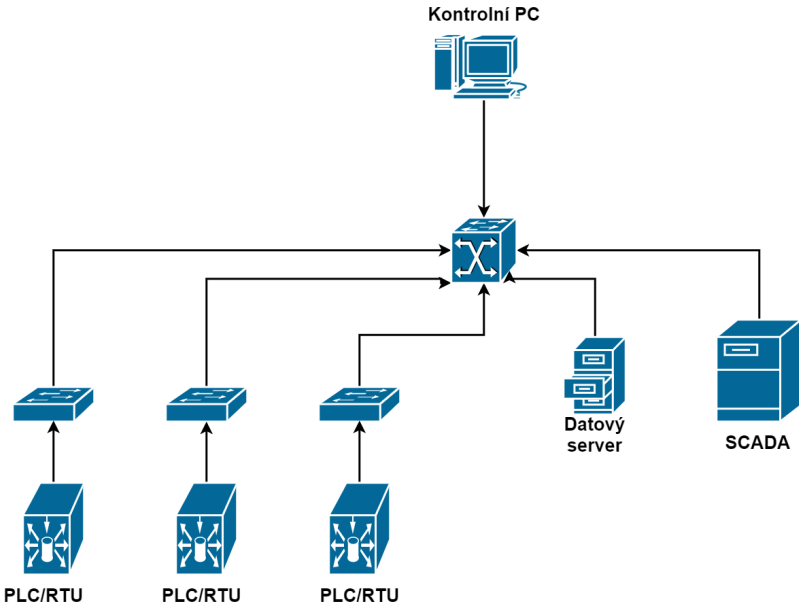


Obr. 1.1: Konceptuální model Smart Grid sítí, převzato z [2].

1.1 SCADA

SCADA (Supervisory Control And Data Acquisition) neboli dispečerské řízení a sběr dat. Jedná se o typ softwarového aplikačního programu pro řízení procesů. SCADA je centrální řídicí systém spojující více technologií k zajištění monitorování, sběru, zpracování dat, zasílaní řídících příkazů zařízením. Systém provádí automatický sběr dat a v pravidelných intervalech kontroluje stav senzorů. Systém SCADA může být použit jak u jednoduchých konfigurací, tak zejména u velkých průmyslových zařízeních a složitých komplexech. Ve velkých průmyslových zařízeních dochází k velkému počtu procesů, kde každý proces je nutné zaznamenávat a sledovat. Vše je velmi složité, neboť každé zařízení, senzor atd. poskytuje jiný výstup. Systém SCADA slouží ke shromažďování těchto dat, které počítač následně zpracovává a včas prezentuje. Dojde-li například ke zvýšení napětí na zařízení, je tato informace odeslána do systému, přičemž upozorňuje, že došlo k události, a zobrazuje tyto informace logickým a organizovaným způsobem.[3]

Stanice SCADA se odkazuje na datové servery komunikujícími se zařízeními prostřednictvím procesních kontrolérů, jako jsou PLC (Programmable Logic Controller) nebo RTU (Remote terminal unit). PLC jsou připojeny k datovým serverům buď přímo nebo prostřednictvím sítě. Systém SCADA využívá sítě WAN (Wide Area Network) a LAN (Local Area Network). Síť LAN je využita pro komunikaci mezi hlavní stanicí a zařízeními, což jsou senzory připojené k PLC nebo RTU. RTU je elektronické zařízení využívající mikroprocesor, který propojuje fyzická zařízení s řídícím systémem přenosem telemetrických dat. Na základě zpráv z řídícího systému může ovládat připojená fyzická zařízení. Většinu monitorovacích a kontrolních operací provádějí RTU nebo PLC, jak je vidět na obrázku 1.2.



Obr. 1.2: Základní architektura SCADA sítě.

1.2 IEC 61850

IEC 61850 je soubor norem, který upřesňuje metody komunikace a komunikační protokoly v oblasti energetiky. Dle těchto norem lze vytvářet flexibilní komunikační systémy, které vyhovují současným požadavkům energetického průmyslu. Určuje pravidla pro vzájemnou komunikaci mezi zařízeními v rozvodnách a stanovuje požadavky, které jsou kladeny na rozvodny a jejich zařízení z hlediska komunikace.

1.2.1 Důvod zavedení standardu IEC 61850

Pro komunikaci v rozvodnách po celém světe se používá více než padesát různých protokolů. Soubor norem IEC 61850 představuje standardizovanou, jednotnou, na dodavateli nezávislou metodu pro tvorbu komunikační sítě a integraci jednotlivých zařízení rozvodny. Cílem tvorby tohoto souboru norem bylo umožnit vytváření systémů, v nichž budou komunikovat zařízení od různých výrobců. Zařízení spojená komunikační sítí se označují zkratkou IED (Intelligent Electronic Devices), česky inteligentní elektronická zařízení.

Zařízení IED nacházející se v rozvodnách nebo jinde v rozvodné sítí, komunikují mezi sebou z důvodu sběru provozních dat, nastavování parametrů regulace, vzdálenému ovládání a konfigurace jednotlivých zařízení. Systém umožňuje realizovat nové funkce pro distribuovanou ochranu rozvoden, jejich regulaci a automatizaci provozu.[4]

1.2.2 Struktura standardu IEC 61850

Struktura standardu IEC 61850 má 10 hlavních částí, z nichž některé jsou vícedílné. Stručné seznámení s obsahem těchto částí bylo vypracováno na základě článku [6].

IEC 61850-1 (Úvod a přehled)

První část standardu specifikuje důvod jeho vzniku. Dále popisuje jeho základní principy a výhody proti starším standardům.

IEC 61850-2 (Výklad zvláštních výrazů)

Druhá část vysvětluje význam zvláštních výrazů. Zejména speciálních zkratek, které se v tomto standardu značně využívají.

61850-3 (Všeobecné požadavky)

Třetí část standardu určuje základní požadavky na komunikaci mezi IED v rozvodně a požadavky na systémy, které jsou na rozvodnu vázány.

IEC 61850-4 (Systémové a projektové řízení)

Čtvrtá část definuje požadavky na správu systémů, řízení projektů a na speciální podpůrné nástroje pro inženýrské práce a systém zkoušek rozvoden.

IEC61850-5 (Požadavky na komunikaci pro funkce a modely zařízení)

Pátá část definuje komunikaci mezi IED. Těmi jsou ochrany, odpojovače nebo transformátory a systémem rozvodny.

IEC 61850-6 (Konfigurační popisový jazyk pro komunikaci v elektrických stanicích týkající se IED)

Šestá čast se týká IED a specifikuje formáty souborů pro popis konfigurace jednotlivých IED a souborů parametrů spojených s komunikací a konfigurací komunikačního systému.

IEC 61850-7-1 (Základní komunikační struktura pro podřízené stanice a napájecí zařízení: Zásady a modely)

Standard obsahuje přehled o architektuře komunikačních systémů a interakcích mezi zařízeními rozvoden. Dále stanovuje, jak dosáhnout vzájemné součinnosti zařízení.

IEC 61850-7-2 (Základní komunikační struktura pro podřízené stanice a napájecí zařízení: Abstraktní rozhraní pro komunikační služby (ACSI))

Standard popisuje rozhraní pro komunikaci mezi klientem a vzdáleným serverem. Dále pro přenos informací o časově kritických událostech a pro přenos souborů vzorkovaných hodnot.

IEC 61850-7-3 (Základní komunikační struktura pro podřízené stanice a napájecí zařízení: Obecné třídy dat)

Standard upřesňuje třídy dat pro přenos informací (např. o stavu zařízení, vzorkovaných veličinách, o analogových žádaných veličinách, o konfiguraci zařízení.

IEC 61850-7-4 (Základní komunikační struktura pro podřízené stanice a napájecí zařízení: Třídy kompatibilních logických uzlů a třídy dat)

Standard stanovuje jednotné názvy kompatibilních logických uzlů a názvy dat pro komunikaci mezi zařízeními IED.

IEC 61850-8-1 (Mapování specifických komunikačních služeb (SCSM))

Osmá část upřesňuje metody pro výměnu časově kritických i nekritických dat po místních sítích pomocí mapování na MMS a na ethernetové rámce z ISO/IEC 8802-3 (IEEE 802.3). Norma upřesňuje výměnu dat v reálném čase, řídicí činnosti a sdělování zpráv.

IEC 61850-9-1 (Mapování specifických komunikačních služeb (SCSM))

Devátá část definuje mapování specifických komunikačních služeb pro komunikaci na úrovni pole rozvodny – proces pro přístroje podle IEC 60044-8. Norma platí pro přenos vzorkovaných hodnot po sériovém jednosměrném (neorientovaném) vícebodovém spoji bod-bod.

IEC 61850-9-2 (Mapování specifických komunikačních služeb (SCSM))

Předposlední část doplňuje normu IEC61850-9-1 tak, aby se do SCSM zahrnulo kompletní mapování modelu vzorkovaných hodnot, získávaných po ethernetové procesní sběrnici definované standardem ISO/IEC 8802.3

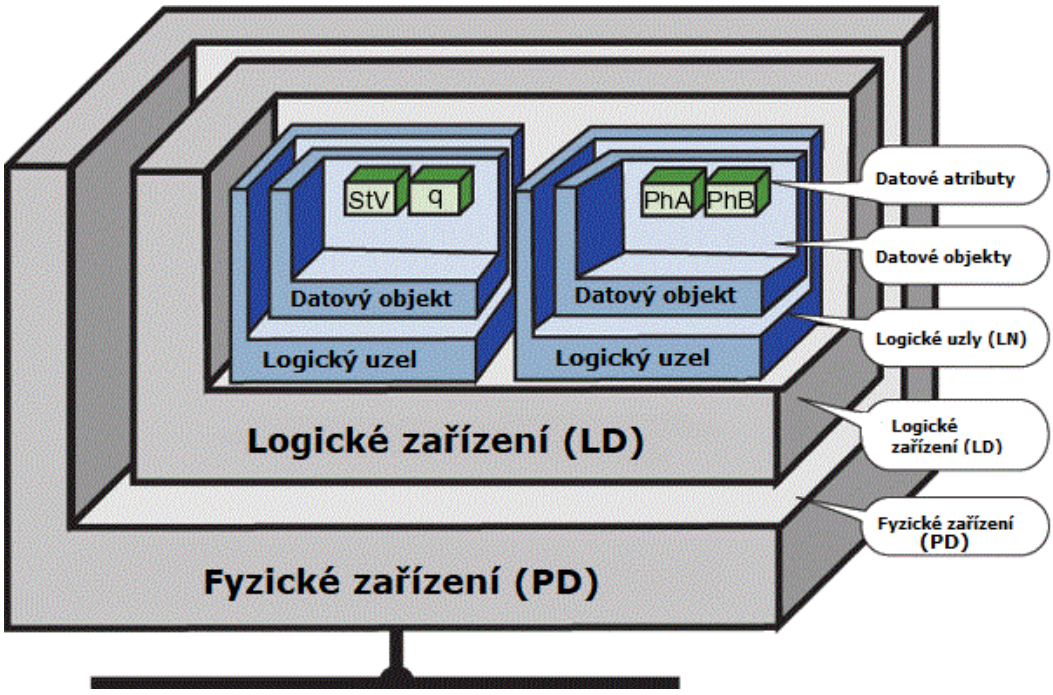
61850-10 (Zkoušky shody)

Poslední část standardu určuje metody a popisuje abstraktní případy zkoušek pro zkoušení shody zařízení používaných v automatizovaných systémech rozvoden.

Výše popsané normy slouží hlavně výrobcům zařízení IED, komunikačních komponent a dalšího SW vybavení, které musí vyhovovat těmto standardům pro získání certifikace.

1.2.3 Datový model standardu IEC 61850

Publikace [8],[9] popisují datový model, který se skládá z fyzického a logického zařízení, logického uzlu, datového objektu a atributu, jak znázorňuje obrázek 1.3.



Obr. 1.3: Datový model IEC 61850, převzato z [7].

Fyzické zařízení

Na prvním místě datového modelu se nachází fyzické zařízení, také označováno jako PD (Physical Device). Fyzické zařízení je též nazýváno IED (Inteligentní elektronické zařízení). Jedná se o ochranný terminál, který má v rozvodném zařízení svou unikátní IP adresu. IED je také definováno jedinečným názvem. Firma ABB u svých IED používá tzv. Technical Key. Jde o jedinečný název s maximální délkou deset znaků. Jinou firmou je například Siemens, který u svých zařízení používá „IED Name“ kde je maximální počet znaků omezen na 8. Pokud se na jednom projektu podílí více výrobců, musí se počet znaků technického klíče IED vždy shodovat.

Logické zařízení

V rámci fyzických zařízení může být definováno jedno nebo více logických zařízení LD (Logical Device). Logické zařízení soustřeďuje data z více zařízení do jednoho fyzického zařízení. Logické zařízení může být například ovládací prvek, poruchový zapisovač nebo ochranná či řídící funkce. Na základě standardu IEC 61850-7-1 musí každé logické zařízení obsahovat minimálně tři logické uzly kterými jsou:

LPHD – zahrnuje informace o fyzickém zařízení (Název PD, stav zařízení, reset zařízení),
LLN0 – zahrnuje informace o všech logických uzlech (provozní režim, datové sady, objekty pro řízení zasílání událostí),
LN – zahrnuje ochranou funkci popsanou ve standardu IEC 61850-7-4.

Logický uzel

Podstrukturu logických zařízení tvoří logické uzly LN (Logical Node). Jedná se o seskupení dat a služeb, které se vztahují na specifickou funkci rozvodny. Díky tomu je možné veškeré údaje, které jsou v rozvodně generovány, přiřadit k určitému logickému uzlu. Logické uzly jsou například pro automatickou regulaci, měření, řízení atd.

Datové objekty

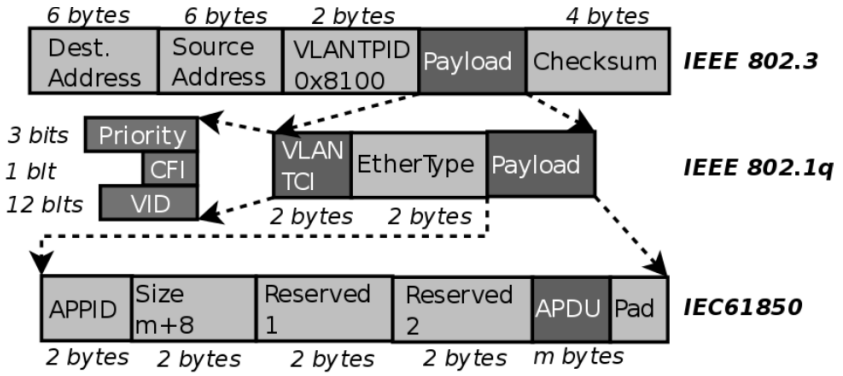
Datové objekty , jeden čí více, obsahuje každý logický uzel. Logické uzly si datové objekty můžou vzájemně předávat. Datové objekty představují základní stavební prvek modelu IEC 61850. Název každého datového objektu je určen obecnou datovou třídou. Ta stanovuje jakou formou jsou data klientovi poskytována. Třídy jsou rozděleny dle jednotlivých významů (informace o stavu, měřené nebo nastavené hodnoty, časové údaje a další).
V datových objektech se dále nachází datové atributy.

Datové atributy

Nejmenší funkční část datového modelu IEC 61850 zastupují datové atributy (Data Atributte (DA). Datové atributy jsou například měřené hodnoty, logické stavy vypínačů, parametry nastavení ochran nebo povely.

1.2.4 Komunikace

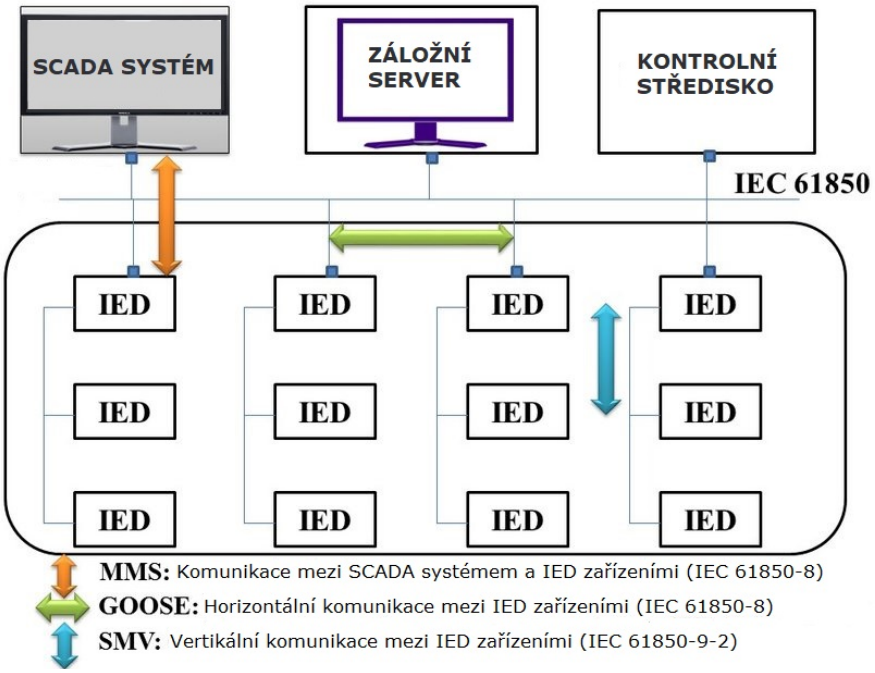
IEC 61850 používá pro přenos zpráv standard IEEE 802.1q a IEEE 802.3. Aby bylo možné zajistit deterministickou komunikaci v reálném čase, je nutné mít ethernetové přepínače kompatibilní se standardem IEEE 802.1q. Standard umožňuje rozesílání zpráv se zásadami plánování podle priorit a dále rozdělení lokálních sítí (LAN) na virtuální sítě (VLAN). Základní struktura SMV a GOOSE zprávy s ohledem na IEEE 802.3 a IEEE 802.1q standardy jsou zobrazeny na obrázku 1.4. Velmi důležité je pole VLAN TCI, které obsahuje pole VID (VLAN ID) o velikosti 12 bitů k určení cíle VLAN a pole Priority o velikosti tři bity, označující úroveň priority, se kterou musí příjemce zprávu zpracovat.



Obr. 1.4: Základní struktura SMV a GOOSE zprávy s ohledem na IEEE 802.3 a IEEE 802.1q standardy, převzato z [10].

Horizontální a vertikální komunikace

Komunikace mezi různými zařízeními v rozvodně probíhá jak horizontálně tak vertikálně. Grafické znázornění je na obrázku 1.5. Horizontální komunikace znamená výměnu dat mezi zařízeními na stejné úrovni z hlediska hierarchie sítě. Horizontálně se přenáší GOOSE zprávy. Vertikální komunikace umožňuje výměnu dat mezi zařízeními umístěných na různých úrovních. Přenášeny jsou MMS (Manufacturing Message Specification) zprávy. Vertikální komunikace používá komunikační model klient - server, zatímco horizontální komunikace používá komunikační model vydavatel - odběratel.



Obr. 1.5: Schéma komunikace ve standardu IEC 61850, převzato z [11].

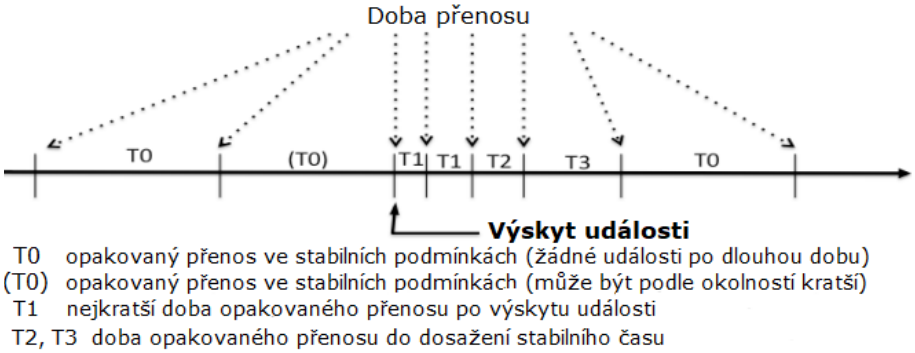
1.2.5 GOOSE Protokol

Protokol GOOSE, který je popsán normou IEC 61850-8-1, je jedním z nejznámějších protokolů poskytovaných standardem IEC 61850. Zkratku GOOSE (Generic Object-Oriented Substation Event)lze přeložit jako "obecnou objektově orientovanou událost v rozvodnách". GOOSE protokol je klíčový při realizaci inteligentní rozvodny. GOOSE zprávy se využívají pro přenos kritických zpráv s vysokou prioritou (např.: blokační signály mezi ochranami). Zprávy jsou vysílány multicastingem a slouží především ke komunikaci mezi IED zařízeními. Data o události v rozvodnách pocházejí z datové sady každého logického uzlu. Aby byla zaručena spolehlivost a včasnost přenosu, je ve zprávě GOOSE použit mechanismus opakovaného přenosu,

který je založený na multicast technologii. V porovnání se zprávami MMS (Manufacturing Message Specification), obsahuje GOOSE protokol dvě zásadní výhody. První je její vynikající včasnost a vysoká účinnost. Druhou výhodou je, že GOOSE zprávy podporují funkci jednoho vysílání a vícenásobného příjmu. Možnost vícenásobného příjmu umožňuje sdílet odpojovače, napětí nebo proud. Veškerá komunikace GOOSE zpráv probíhá horizontálně na internetové vrstvě L2.

Interval přenosu zpráv

Spolehlivost a včasnost GOOSE zpráv zajišťuje cyklický přenos dat. Jedná se o přenos, který probíhá v určitých časových intervalech. Standardní interval přenosu je v rozmezí 5-100ms, označován jako T0 nebo Tmax. Jestliže v rozvodně nastane nějaká událost (překročení hraničních hodnot), je vytvořena nová GOOSE zpráva. Interval přenosu se sníží na 0,5–5ms (označován jako T1 nebo Tmin) a zpráva je ihned přednostně odeslána. Poté se intervaly odesílání zpráv zdvojnásobují k intervalu Tmax.



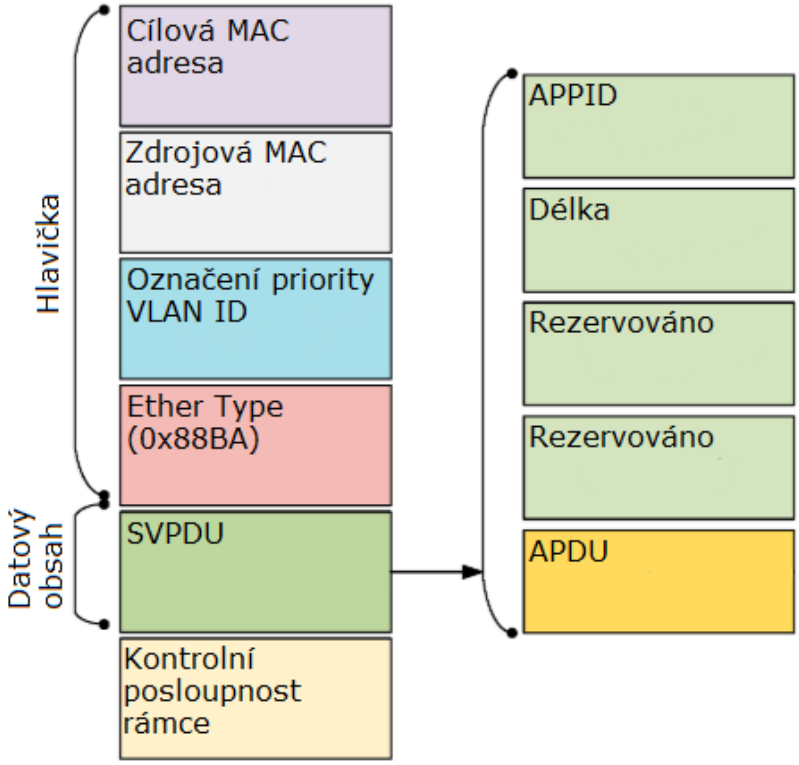
Obr. 1.6: Časový interval přenosu GOOSE zpráv, převzato z [12].

1.2.6 Sampled Values protkol

Protokol SV (Sampled Values) neboli vzorkované hodnoty se používá k přenosu digitalizovaných okamžitých hodnot veličin energetických systémů, zejména primárních proudů a napětí. Hodnoty se přenášejí pomocí procesní sběrnice. Jedná se o komunikační datovou sběrnici, ke které jsou připojena zařízení na úrovni pole rozvodny (přepínací zařízení, měřicí transformátory). K procesní sběrnici lze připojit měřící převodníky, spínače, odpojovače a jiné zařízení. Hlavním úkolem procesní sběrnice je okamžitý přenos hodnot z měřících zařízení.

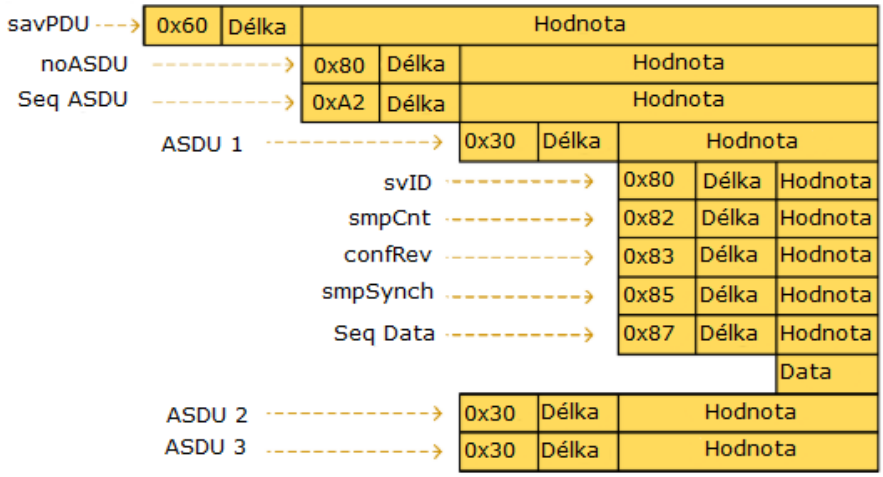
Struktura SMV datagramu

Na obrázku 1.7 je znázorněna struktura SMV datagramu, který je popsán v publikaci [13] a skládá se ze dvou částí. První část, nazvaná záhlaví, obsahuje cílovou a zdrojovou MAC adresou. Cílová MAC adresa je jedna z všesměrových MAC adresu, které jsou uvedeny ve standardu IEC 61850 a začínají 01 0C CD 04. Datagram obsahuje také službu VLAN (Virtual Lan), která slouží k určování priorit na základě standardu IEEE 802.1Q. Poslední část záhlaví je pole Ether Type, které obsahuje hodnotu 0x88BA. Hodnota určuje, že se jedná o SMV zprávy.



Obr. 1.7: Struktura SMV datagramu

Druhou částí datagramu je datový obsah. Datová jednotka SVPDU (Samled Value Protocol Data Unit) obsahuje více datových polí. Prvním je APPID (Application ID), což je jedinečný identifikátor používaný pro rozlišení a klasifikaci SMV zpráv. Pole Délka, je hexadecimální číslo určující délku celého SVPDU. Následující dvě pole jsou vyhrazená pro budoucí použití a poslední je pole APDU (Application Protocol Data Unit). APDU může obsahovat několik ASDU (Application Service Data Units) jak je zobrazeno na obrázku 1.8.



Obr. 1.8: Detail APDU pole

Jedná se o objekty obsahující důležité informace pro jednotlivé uzly. Použití několika ASDU umožňuje jedinému zařízení odesílat nebo přijímat data fyzických senzorů z několika uzlů v rámci energetického systému v jedné SMV zprávě. Počet jednotlivých objektů ASDU je uložen v poli noASDU. Všechna ASDU poté obsahují sedm následujících podpolí.

svID – ID hodnoty vzorku,

SmpCnt – Počítadlo, které zvyšuje počet vždy, když je odebrána nová vzorkovací hodnota,

ConfRev – Hodnota, která označuje počet změn konfigurace,

SmpSynch – Booleovská hodnota, která je pravdivá, pokud je SV synchronizován hodinovým signálem, a false, pokud není,

Seq Data – Sekvence dat,

Data – Aktuální dataset.

1.2.7 MMS protokol

MMS je protokol pro přenos dat pomocí technologie klient – server a je standardizován jako ISO/IEC 9506. Kapitola IEC 61850-8-1 popisuje pouze postup přiřazování datových služeb popsaných v IEC 61850 k protokolu MMS, který je definován jako ISO / IEC 9506. Hlavním účelem protokolu MMS je shromažďování údajů o IED a jejich následné přeposílání do SCADA systému.

V článku [14] je popsáno, že IEC 61850 definuje dva typy zpráv, kterými jsou zprávy s vyrovnávací pamětí a bez vyrovnávací paměti. Hlavním rozdílem je, že při použití vyrovnávací paměti budou zprávy doručeny klientovi i v případě, kdy je zpráva připravena, ale nedojde k žádné komunikaci z důvodu výpadku komunikačního kanálu. Všechny vygenerované zprávy se ukládají do paměti zařízení. Pře-

nos těchto zpráv je zahájen po obnovení spojení. Neodeslané zprávy se ukládají do vyrovnávací paměti na serveru. Jestliže během výpadku dojde k událostem, které vygenerovaly mnoho zpráv a vyrovnávací paměť se zaplní, jsou starší zprávy přemazávány novými. Server ale po navázání spojení klientovi sděluje, že vyrovnávací paměť byla vyčerpána a došlo ke ztrátě starších dat. Pokud je spojení mezi klientem a serverem v pořádku, může být přenos obou typu zpráv okamžitý při vzniku alarmující události. Přenos proběhne za předpokladu, že časový interval, pro který jsou události zaznamenány, je roven nule.

1.2.8 Zranitelnost standardu IEC 61850

Standard IEC 61850 má mnoho výhod, ale použití komunikace pomocí Ethernetu je důvodem k obavám o zabezpečení, které je publikováno v článku [15], protože norma neobsahuje žádná bezpečnostní opatření. Podobně jako většina běžných standardů komunikačních technologií, které jsou v současné době implementovány v energetických sítích, je standard IEC 61850 náchylný k různým typům útoků. Jedná se například o odepření služby, útoky k prolomení hesla nebo odposlouchávání paketů.

Odepření služby

Útok odmítnutí služby, známý také jako DoS (Denial of Service) nastává, když se útočník pokusí cílovou službu znefunkčnit a znepřístupnit ostatním uživatelům. Způsobem jak toho dosáhnout, může být narušení nebo využití služby zařízení IED. Narušení provozu IED nastane, pokud útočník vysílá škodlivý kód na cílené zařízení IED. Kód náhodně zapisuje nadměrně velká data, což způsobí zahlcení vyrovnávací paměti.

Otrava GOOSE zprávy

GOOSE poisoning neboli otrava GOOSE, je další formou útoků odmítnutí služeb. Odesílatel zpráv GOOSE se nazývá vydavatel a příjemce zpráv GOOSE se nazývá předplatitel, což je obvykle zařízení IED. Každá GOOSE zpráva má pole stavu značených stNum a pořadového čísla sqNum. Při výskytu události, začne IED vysílat zprávu s novým stNum. Zpráva se opakuje s proměnným časovým zpožděním, kde každá opakovaná zpráva má zvýšený sqNum. Aby se předešlo opakovaným útokům, předplatitel zahodí jakoukoli zprávu mající stNum menší nebo rovnou předchozí zprávě. Zde se útočník pokouší přimět předplatitele, aby přijímal zprávy s vyšším číslem než zprávy odeslané vydavatelem. Výsledkem tohoto útoku bude, že všechny zprávy GOOSE od autentického vydavatele budou zařízením IED považovány za zastaralé. IED nyní bude přijímat a zpracovávat pouze GOOSE zprávy odeslané

útočníkem. Cílem takového útoku je zablokovat jakýkoli kontrolní příkaz určen napadenému IED. To zabrání IED v reakci na kritické události.

Útok k prolomení hesla

Prolomením hesla se útočník snaží získat neoprávněný přístup k systému nebo zařízení, kterým může být například IED. Útok lze provést dvěma způsoby, kterými jsou útok hrubou silou nebo slovníkový útok. Útok hrubou silou je založen na zkoušení všech možných kombinací hesla, dokud není nalezeno správné. Způsob tohoto útoku by ale mohl trvat moc dlouho. Slovníkové útoky používají pouze vytvořená slova, která jsou obsažena ve slovníku k uhádnutí hesla. Typy hesel jsou v tomto případě pravděpodobnější a jejich výsledkem je méně času na jejich uhodnutí.

Odposlouchávání komunikace

Odposlouchávám síťové komunikace se útočník snaží o čtení a odcizení paketů přenášených sítí. Útoky tohoto typu musí být spuštěny z vnitřní sítě LAN, proto musí útočník buď napadnout počítač v síti rozvodny kde je použit standard IEC 61850, nebo mít fyzický přístup k zařízení v síti. Útoky bývají úspěšné, protože služby na které cílí, včetně FTP, HTTP a Telnet, nešifrují své zprávy, a po jejich zachycení je lze snadno přečíst.

Jedním ze způsobů, jak útočník může odposlouchávat sítovou komunikaci, je provedení podvržení odpovědi na ARP (Address Resolution Protocol)dotaz. ARP je základní komunikační protokol, který převádí IP adresy na MAC adresy. Při tomto útoku jsou na ostatních počítačích v síti LAN nainstalovány falešné adresy IP a mapování MAC adres. IP adresa zařízení je pak spojena s nesprávnou adresou MAC, což má za následek přeposílání všech paketů adresovaných na tuto Ip adresu, na zařízení útočníka.

2 Simulační nástroje

Síťové simulátory umožňují intuitivně modelovat složité chování protokolů a inovovat sítě. Simulátory jsou schopné efektivně analyzovat výkon těchto protokolů a technologií v modelech síťové infrastruktury v reálném měřítku.

2.1 Network simulator 3

NS3 (Network Simulator 3) je síťový simulátor určený pro vzdělávací a výzkumné účely. NS-3 je software s otevřeným kódem licencován pod GNU GPLv2 (General Public Licence), což umožňuje stálý vývoj tohoto softwaru. Simulační nástroj je napsán v jazyce C++, Python a nahrazuje předchozí verzi programu NS-2. Hlavním cílem NS3 je dle publikace [16] vytvoření pevného simulačního jádra, které je dobře zdokumentované, snadno použitelné, laditelné, a které vyhovuje potřebám celého pracovního postupu konfigurace simulace, její následné spuštění a sběr výsledných dat.

Simulační nástroj NS-3 umožňuje vývoj simulačních modelů, dostatečně realistických na to, aby umožnily použití NS-3 jako síťového emulátoru v reálném čase, propojeného se skutečným světem. Software podporuje také interakci s reálnými systémy pomocí plánovače v reálném čase, kde simulace běží ve smyčce. Díky tomuto řešení mohou uživatelé přijímat data generované NS-3 na fyzických zařízeních v sítí a NS-3 může sloužit jako propojovací prvek mezi virtuálními stroji.

2.1.1 Vytváření simulace v NS-3

Základním krokem je definice topologie sítě, kde vytváříme zařízení, která mezi sebou mají komunikovat. Dalším krokem je definování vztahů a vzájemného propojení zařízení. Konfigurace zařízení a nastavování jejich parametrů je dalším krokem pro spuštění simulace. Spuštění simulace umožní generování dat a události na základě nastavených parametrů sítě. Po úspěšném ukončení simulace se data ukládají s časovou značkou a detaily události. Data vytvořené simulací lze zobrazit také do grafické vizualizace. Průběh komunikace mezi zařízeními lze zaznamenávat také programem Wireshark.

2.2 Riverbed Modeler

Simulační nástroj Riverbed Modeler je nástupcem simulačního nástroje OPNET a je složen ze sady protokolů a technologií doplněných o propracované vývojové prostředí. Nabízí možnost modelování mnoha typů a technologií sítě (včetně VoIP,

TCP, OSPFv3, MPLS, IPv6 a dalších). Riverbed Modeler [17] umožňuje testovat a předvádět technologické návrhy před uvedením do reálného provozu na síti. Díky tomuto simulátoru je možné zvýšit produktivitu výzkumu a vývoje síťových technologií.

V rámci vytváření projektu můžeme použít předdefinované prvky sítě, kterými jsou například přepínače, routery, servery a propojit je pomocí linek. Následně nastavit parametry komunikace. Podporováno je také automatické vytváření standardních síťových topologií. Náhodný provoz lze automaticky generovat z algoritmů zadaných uživatelem nebo importovat z dostupných balíčku simulujících skutečný provoz. Výsledky simulace a získaná data jsou zobrazena v grafech. Simulační nástroj může generovat také statistiky síťového provozu a animace.

Riverbed modeler je na rozdíl od předchozího softwaru OPNET zpoplatněn. Nabízí ale verzi Riverbed Modeler Academic Edition, která poskytuje prostředí pro modelování, analýzu a předpovídání výkonu síťových infrastruktur. Academic Edition je navržen tak, aby splňoval základní požadavky pro výuku vytváření a testování sítí. Obsahuje nástroje pro návrhy modelů, simulací, sběr a následnou analýzu získaných dat.

2.3 OMNeT ++

OMNeT++ (Objective Modular Network Testbed in C++) popsán na stránkách [18], je objektově orientovaný modulární simulátor diskrétních událostí, který je napsán v programovacím jazyce C++. Je určen zejména pro simulace počítačových sítí, ale vzhledem k jeho flexibilní architektuře je využíván v různých oblastech IT. Simulátor lze použít pro modelování komunikačních protokolů, počítačových sítí a modelování provozu. Lze modelovat i víceprocesorové a distribuované systémy a administrativní systémy.

Program OMNeT++ umožnuje provádět simulace v grafickém rozhraní nebo v příkazovém řádku. Grafické rozhraní zobrazuje jednotlivé rozmístění potřebných modulů a jejich vzájemné propojení. Nastavení použitých modulů se provádí pomocí příkazové řádky, kde lze nastavovat jak jednotlivé moduly, tak veškeré parametry simulace.

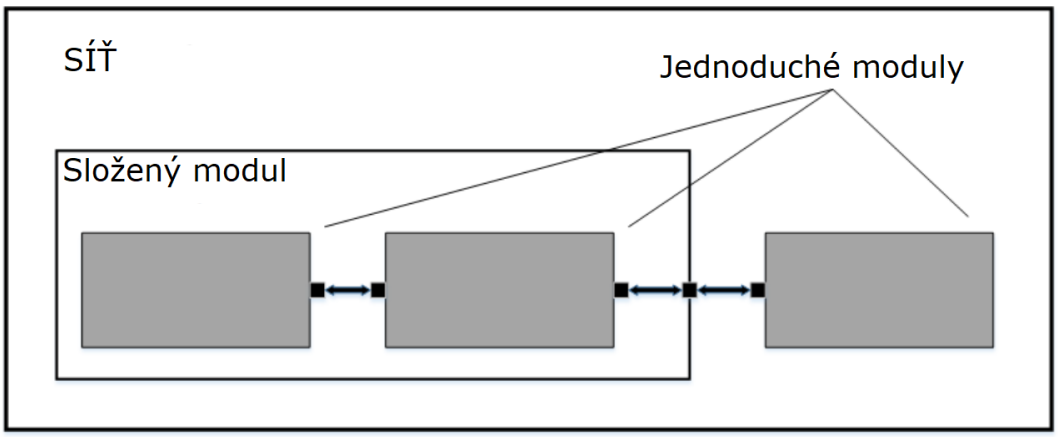
Simulátor beží na nejběžnějších operačních systémech, kterými jsou: Linux, Mac OS, Windows. OMNeT++ je zdarma pouze pro akademické a neziskové účely. Pro komerční použití je potřeba získat licenci OMNEST, kterou nabízí společnost Simulcraft Inc.

2.3.1 Moduly

OMNeT ++ používá pro vytváření modelů hierarchicky vnořených modulů, což uživateli umožňuje odrážet logickou strukturu skutečného systému ve struktuře modelu. Modul, který je v hierarchii postaven nejvýše, se nazývá systémový a skládá se z jednoduchých a složených modulů. Složené moduly lze dále dělit, ale základním stavebním prvkem každého složeného modulu je modul jednoduchý.

Jednoduchý a složený modul

Jednoduché moduly jsou nedělitelné prvky, které jsou naprogramovány v jazyce C++. Jsou to funkční prvky, které generují a reagují na události. Složené moduly slouží pouze k logickému uspořádání systému a mohou mít stejné parametry jako jednoduché moduly, negenerují však žádné události. Na obrázku je zobrazen rozdíl mezi jednoduchým a složeným modulem.



Obr. 2.1: Jednoduchý a složený modul

Moduly mezi sebou komunikují pomocí zpráv, které mohou obsahovat libovolná data. Zprávy jsou odesílány pomocí bran, které jsou rozděleny na vstupní a výstupní. Spojení mezi nimi jsou vytvářena v rámci jedné úrovně hierarchie modulů. Spojení přesahující úrovně hierarchie nejsou povoleny, protože by bránily opětovnému použití modelu. Komunikaci mezi jednoduchými modely na více úrovních, zajišťují složené moduly. Spojením mezi složenými moduly lze přiřadit parametry, jako je zpoždění, přenosová rychlost a bitová chybovost. Lze také definovat typy připojení se specifickými vlastnostmi. Tato spojení se nazývají kanály a mohou být znovu použity na několika místech.

Složené moduly mohou obsahovat parametry, které se používají hlavně pro předávání konfiguračních dat do jednoduchých modulů a pro definování topologie simulačního modelu. Složené moduly mohou předávat parametry nebo výrazy parametrů

svým submodulům.

2.3.2 Jazyk NED

K popisu topologie rozdělení jednotlivých modulů a specifikaci struktury sítě používá OMNeT++ jazyk NED (Network Description). Výstupem jsou soubory s koncovkou .ned. Soubory tohoto typu lze převádět na XML a zpět bez toho, aniž by jsme ztratili nějaká data, což umožňuje generovat NED z informací, které jsou uloženy v jiných systémech (například databáze SQL). NED umožnuje deklarovat jednoduché moduly a sestavovat je do modulů složených. Jazyk NED se přispůsobí i velkým projektům, neboť obsahuje následující funkce:

Hierarchie

Zavedení hierarchií umožnuje jakýkoliv modul, který je příliž složitý jako jeden celek, rozdělit na menší moduly a použít je jako složený modul.

Komponenty

Jednoduché a složené moduly jsou opakovaně použitelné, což nejen snižuje kopírování kódu, ale také umožňuje vytváření knihoven komponent (jako jsou INET Framework, MiXiM, Castalia atd.).

Rozhraní

Rozhraní modulů a kanálů lze použít jako zástupný symbol, pokud by se normálně použil modul nebo typ kanálu a konkrétní modul nebo typ kanálu je určován v době nastavení sítě parametrem. Konkrétní typy modulů musí implementovat rozhraní, které mohou nahradit. Například vzhledem k tomu, že typ složeného modulu s názvem MobileHost obsahuje submodul mobility typu IMobility (kde IMobility je rozhraní modulu), skutečný typ mobility může být vybrán z typů modulů, které implementovaly IMobility (RandomWalkMobility , TurtleMobility atd.)

Dědictví

Odvozené moduly a kanály mohou přidávat nové parametry, dílčí moduly a připojení. Dokážou nastavit původní parametry na přesnou hodnotu, což umožňuje převzít například modul GenericTCPClientApp a vytvořit z něho FTPClientApp nastavením určitých parametrů na pevnou hodnotu.

Anotace metadat

Metadata nepoužívá simulační jádro programu přímo, ale mohou nést další informace pro různé nástroje, běhové prostředí nebo další moduly v modelu. Například grafické znázornění modulu (ikona) nebo měřící jednotka (miliwatt). Parametry jsou tedy zadány jako anotace metadat.

2.3.3 Knihovny pro rozšíření OMNeT++

Pro simulační nástroj OMNeT++ jsou k dispozici rozšiřující knihovny (Frameworky). Každá knihovna se zaměřuje na určitou oblast, jako například na počítačové sítě nebo na práci se souborovými systémy. Při vytváření jednoho projektu je možné mít přiřazeno více knihoven.

2.4 Porovnání simulačních nástrojů

Tabulka 2.1 porovnává tři vybrané simulační nástroje z hlediska možnosti simulace protokolu IEC 61850.

Tab. 2.1: Porovnání popsaných simulačních nástrojů

	NS 3	Riverbed Modeler	OMNeT++
Licence	Zdarma	Zdarma po registraci	Zdarma
Grafické vývojové prostředí	Ne	Ano	Ano
Vizualizace topologie sítě	Ano	Ano	Ano
Propojení s reálnou sítí	Ano	Ne	Ano
Rozšiřování pomocí knihoven	Ano	Ano	Ano

Simulační nástroj NS3 byl zamítnut z důvodu absence grafického vývojového prostředí. Riverbed Modeler není možné propojit do reálného síťového provozu a proto jsem zvolil Simulační nástroj OMNeT++. Velkou výhodou je možnost naimportovat framework, který podporuje komunikaci standardu IEC 61850.

3 Virtuální prostředí

Pro lepší přenositelnost byl nástroj OMNET++ nainstalován ve virtuálním prostředí. Jako virtualizační nástroj byl zvolen VM VirtualBox verze 6.0.12, kde byl nainstalován operační systém Ubuntu 18.04. Instalovat OMNeT ++ je možné i na operační systém Windows, tato možnost nebyla zvolena z důvodu, že Windows pracuje v OMNeT++ jen s knihovnami do velikosti 65 536 záznamů a knihovny, které budou potřeba jsou větší.

Po instalaci Ubuntu byl nainstalován OMNeT++ verze 5.4.3 a potřebné knihovny pro otestování funkčnosti programu. Po spuštění základní simulace se program jevil v pořádku. Problém nastal u spuštění simulace rozsáhlejší sítě, kde se program zasekával a selhával. Problém nastal také při importu potřebné knihovny s názvem INETMANET, která se po importu nezobrazovala v simulačním nástroji a tedy nebylo možné dále pracovat na modelu SCADA sítě. Z tohoto důvodu byl proveden přechod na starší verzi OMNeT++ 4.6, kde již funkčnost simulačního nástroje spolu s knihovnou INETMANET byla otestována a nevykazovala žádné chyby během simulace. Celková instalace musela být provedena znovu. Postup této instalace je popsán níže.

3.1 Instalace OMNET++

Všechny distribuce Linux obsahují pouze zdrojové kódy, a je proto nutné je před prvním spuštěním OMNeT++ zkompilovat. Věškeré příkazy se v prostředí Linux zadávájí do terminálu.

Sytém Linux Ubuntu 18.04 má implementovanou Javu OpenJDK-11. Pro správnou instalaci a fungování simulačního nástroje je zapotřebí OpenJDK-8. Pro instalaci požadované verze OpenJDK je zapotřebí zadat do terminálu následující příkazy:

```
sudo apt update
sudo apt install openjdk-8-jdk
```

Správnost instalace zjistíme na výpisu, který je na obrázku 3.1. Výpis dostaneme zadáním příkazu:

```
update-java-alternatives -l
```

```
lukas@lukas-VirtualBox:~$ update-java-alternatives -l
java-1.11.0-openjdk-amd64      1111       /usr/lib/jvm/java-1.11.0-openjdk-amd64
java-1.8.0-openjdk-amd64       1081       /usr/lib/jvm/java-1.8.0-openjdk-amd64
lukas@lukas-VirtualBox:~$
```

Obr. 3.1: Výpis verze JDK

Verzi OpenJDK-8 je nutné nastavit jako výchozí. Zadáním následujícího příkazu dostaneme možnost výběru výchozí verze, jak je zobrazeno na obrázku 3.2.

```
sudo update-alternatives –config java
```

```
lukas@lukas-VirtualBox:~$ update-alternatives --config java
Existují 2 možnosti pro alternativu java (poskytující /usr/bin/java).

  Výběr      Cesta                                          Priorita   Stav
------------------------------------------------------------
  0            /usr/lib/jvm/java-11-openjdk-amd64/bin/java      1111      automatický režim
  1            /usr/lib/jvm/java-11-openjdk-amd64/bin/java      1111      ruční režim
* 2            /usr/lib/jvm/java-8-openjdk-amd64/jre/bin/java   1081      ruční režim

Pro aktuální možnost[*] stiskněte <enter>, jinak zadejte číslo:
```

Obr. 3.2: Nastavení výchozí verze OpenJDK

Před instalací simulačního softwaru OMNeT++ zadáme do terminálu příkaz pro aktualizaci repozitářů:

```
sudo apt-get update
```

Před instalací samotného OMNeT++ je potřeba nainstalovat balíčky souborů, které jsou potřebné ke spuštění simulačního nástroje příkazem:

```
sudo apt-get install build-essential gcc g++ bison flex perl tcl-dev tk-dev libxml2-dev zlib1g-dev default-jre doxygen graphviz libwebkitgtk-1.0-0 openmpi-bin libopenmpi-dev libpcap-dev
```

Z oficiálních stránek [18] si stáhneme OMNeT++ verze 4.6 a následně jej rozbalíme pomocí příkazu:

```
tar xvfz omnetpp-4.6-src.tgz
```

Abychom mohli pokračovat v instalaci, je potřeba se přemístit do složky s programem pomocí příkazu:

```
cd /omnetpp/omnetpp-4.6
```

Dalším krokem je sestavení konfiguračních souborů pro spuštění programu. Sestavení proběhne zadáním příkazu:

```
./configure
```

Před sestavením OMNeT++ je potřeba zadat cestu umístění programu do souboru /.bashrc, který otevřeme pomocí příkazu:

```
gedit /.bashrc
```

Otevřel se nám textový editor, ve kterém je potřeba na konci dokumentu zadat následující text:

```
export PATH=$PATH:/home/omnet/omnetpp-4.6/bin
```

Po uložení souboru je už možné sestavit OMNeT++ do spustitelné podoby, zadáním příkazu:

```
make
```

Jakmile se sestavení dokončí, je možné spustit program zadáním příkazu:

```
omnetpp
```

Po spuštění programu máme na výběr, zda chceme importovat vzorové příklady a framework INET. Vzorové příklady si necháme naimportovat, abychom mohli vyzkoušet funkčnost programu. Framework INET není potřeba importovat, jelikož bude nahrazen frameworkem INEMANET, který obsahuje moduly potřebné k vytvoření simulace. Framework je dostupný na stránkách GITHUB [20], který po stažení rozbalíme pomocí příkazu:

```
tar xvfz inetmanet-master-src.tgz
```

Po rozbalení souboru je zapotřebí přejít do složky inetmanet-master pomocí příkazu:

```
cd inetmanet-master
```

Adresář neobsahuje soubor pro sestavení frameworku, a proto jej vytvoříme příkazem:

```
make makefile
```

Vytvoření souboru pro sestavení nám umožní sestavit framework inetmanet příkazem:

```
make
```

Po sestavení knihovny INETMANET sputíme OMNeT++, kde INETMANET naimportujeme: Pro import zvolíme v menu programu: File→ Import→ Genereal→ Existing projekt into Workspace a zde zadáme cestu k adresáři inetmanet-master. Zaškrtnutím volby Copy project into workspace a jeho potvrzením se nám naimportuje potřebný framework do simulačního nástroje OMNeT++.

Nakonec je potřeba nainstalovat program Wireshark, aby bylo možné otevřít vytvořené *.pcap soubory. Použijeme příkaz:

```
sudo apt-get install wireshark
```

3.1.1 INETMANET

Framework INETMANET je rozšíření framworku INET o SCADA prvky, které budeme používat při návrhu sítě. Níže jsou popsány jednoprvkové a složené moduly, které budou použity při vytváření testovací sítě.

EtherAppGoose

Jedná se o jednoprvkový modul, který umí generovat a zpracovávat GOOSE zprávy.

EtherAppSv

Jedná se o jednoprvkový modul, který umí generovat a zpracovávat SMV zprávy.

EtherEncap

Jedná se o jednoprvkový modul, který provádí zapouzdření zprávy z vyšší vrstvy do ethernetového rámce a předání na rozhraní EtherMACFullDuplex. Pracuje i v opačném směru, kdy zprávu z ethernetového rámce předává vyššímu rozhraní.

EtherMACFullDuplex

Jedná se o jednoprvkový modul, který obsahuje rozhraní s podporou plně duplexního provozu při rychlostech 10 Mb/s, 100 Mb/s, 1 GB/s, 10 GB/s, 40 GB/s, a 100 GB/s. Prvek provádí přenos rámců a podle MAC adresy rozhoduje, zda bude rámec zahozen nebo přijat a předán rozhraní EtherEncap.

EtherQoSQueue

Jedná se o víceprvkový modul, který má na starost rozpoznávat důležitost zpráv. Obsahuje dva moduly, kterými jsou DataQueue a pauseQueue. DataQueue přenáší zprávy s vyšší prioritou a pauseQueue slouží k uložení dat s nižší prioritou a čeká na vyřízení dat s prioritou vyšší.

SCADA

Jedná se o víceprvkový modul složený z EtherMACFullDuplex, EtherEncap, EtherQoSQueue a EtherTrafGen. SCADA má za úkol generovat a přijímat zprávy ze sítě s určením priority. Generování zpráv obstarává jednoprvkový modul EtherTrafGen.

Pc

Jedná se o víceprvkový modul složený z EtherMACFullDuplex, EtherAppSv, EtherEncap a EtherAppGoose. Jeho funkcí je shromažďování informací od zařízení MU (Merge Unit) pomocí Sampled Values zpráv.

IecNportFifoSwitch, IecNportSwitch

Jedná se o víceprvkové moduly, které slouží jako moduly přepínačů s předem nedefinovaným počtem účastníků. Moduly dále obsahují modul Gate, který slouží pro příjem a odesílání zpráv. Obsahují ještě modul Relay Unit, který přepíná zprávy na správný port.

Inter

Jedná se o víceprvkový modul, který reaguje na zprávy typu GOOSE od modulu Pc. Skládá se z jednoprvkových modulů EtherMACFullDuplex, EtherEncap a EtherAppGoose.

Com

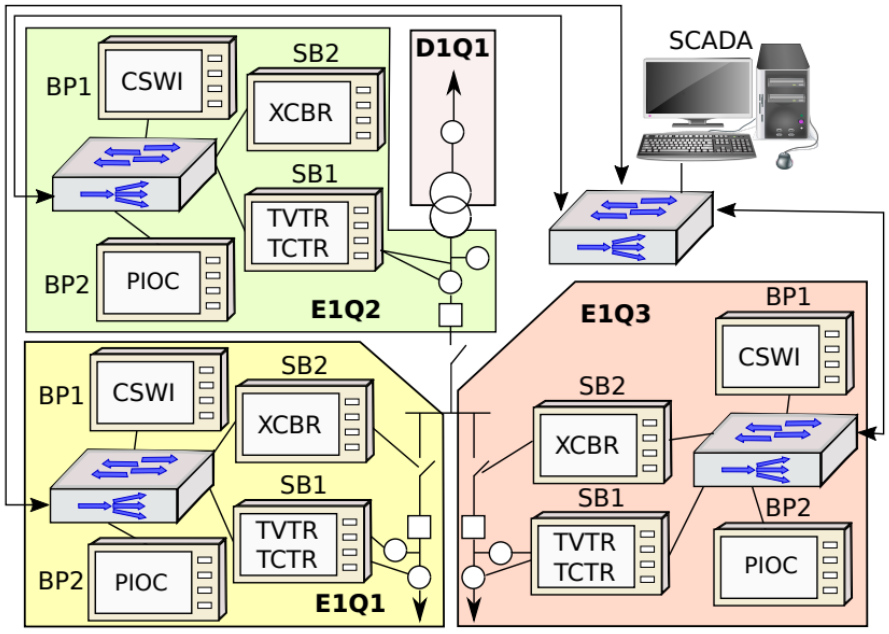
Jedná se o víceprvkový modul složen z EtherMACFullDuplex, EtherEncap a EtherAppGoose. Jeho úkolem je reakce na GOOSE zprávy od modlu PC.

Merge Unit

Jedná se o víceprvkový modul složen z EtherMACFullDuplex, EtherAppSv a EtherEncap. Umožňuje implementovat procesní sběrnici převedením analogových signálů z běžných proudových a napěťových transformátorů na hodnoty podle normy IEC 61850.

3.2 Síť pro testování komunikace

V rámci praktické části byla vytvořena sít pro simulaci datové komunikace, která probíhá mezi zařízeními v rámci rozvodny typu T1-1. Jedná se o typ rozvodny, která transformuje napětí 220kV na 132kV. Schéma tohoto typu rozvodny je zobrazeno na obrázku 3.3.



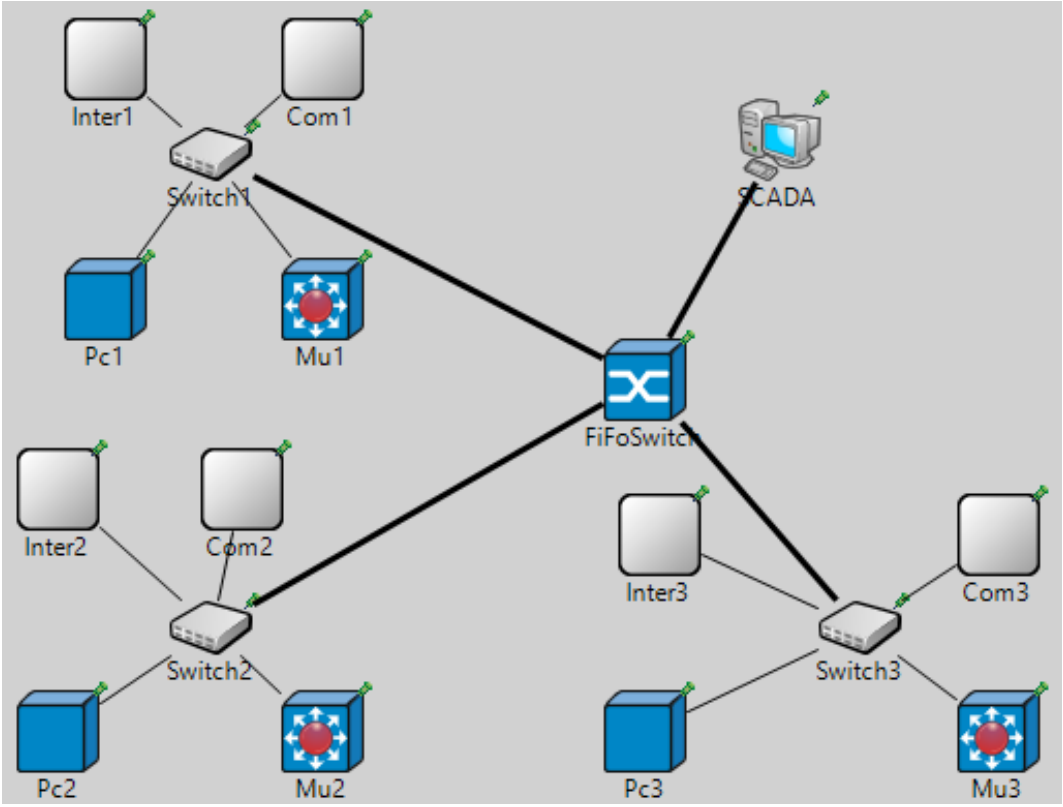
Obr. 3.3: Schéma rozvodny T1-1

Schéma zobrazuje tři samostatné části rozvodny, které jsou navzájem propojeny switchem. Tento switch podporuje standard IEEE 802.1Q, díky čemuž je schopen vytvářet VLANy za účelem logického oddělení každé z těchto částí. Díky tomu probíhá datový přenos jen mezi potřebnými zařízeními. Každá část obsahuje čtyři zařízení, která jsou vzájemně propojena pomocí switche. Zařízení SB1 je IED, které dokáže generovat zprávy SV. Zbylá tři zařízení (BP1, BP2, SB2) jsou IED pro ochranu a kontrolu rozvodny, generující GOOSE zprávy.

Zařízení mají uvnitř názvy, které označují přidělení LN (Logical node) neboli Logický uzel. Dle publikace [21] je zařízení SB1 určeno výhradně k měření elektrických parametrů, proto obsahuje logický uzel TVTR (Voltage transformer) neboli napěťový transformátor a TCTR (Current transformer) neboli proudový transformátor. Dalším zařízením je BP1 obsahující logický uzel s názvem CSWI (Switch controller). Slouží jako ovládací prvek, který vysílá příkazy k zapnutí nebo vypnutí jističe. BP2 obsahuje logický uzel s názvem PIOC (Over current protection). Zařízení je popsáno v publikaci [22] jako ochranný prvek, který analyzuje data z logického uzlu TCTR a určuje zda nedošlo k překročení hodnoty měřeného proudu. Posledním zařízením je SB2 obsahující logický uzel XCBR (Circuit Breaker). Slouží pro vypnutí jističe v případě poruchy a jeho opětovné zapnutí. Příkazy k zapnutí nebo vypnutí jsou přijímány od logického uzlu CSWI.

3.3 Simulace komunikace dle standardu IEC 61850

Na základě schématu rozvodny zobrazeném na obrázku 3.3 byla vytvořena síť pro otestovaní komunikace dle standardu IEC 61850. Rozvržení modulů simulace je zobrazeno na obrázku 3.4. Obsahuje tři moduly Merge unit pro generování hodnot a zastupuje zařízení SB1, tři moduly Com zastupující zařízení SB2 a Inter zastupující zařízení BP1. Dále jsou zde tři moduly PC sloužící zastupující zařízení BP2, tři přepínače IecNportSwitch, jeden přepínač IecNportFifoSwitch a zařízení SCADA.



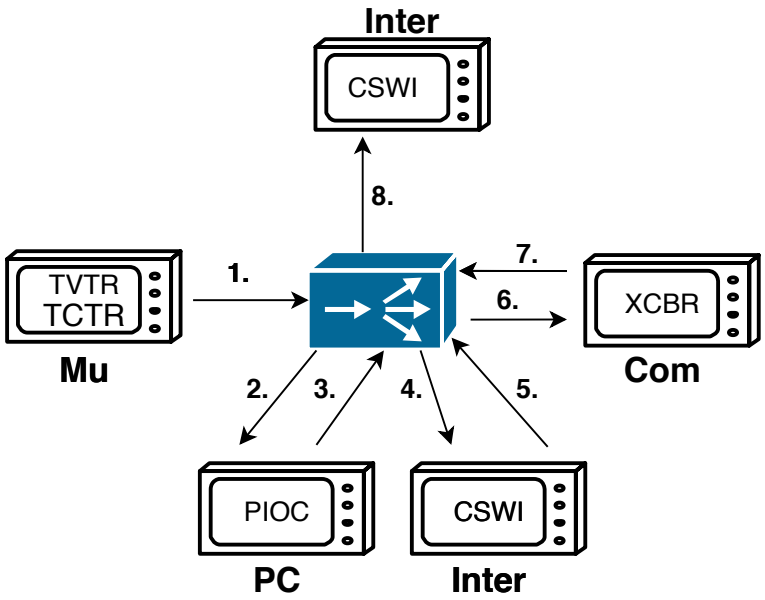
Obr. 3.4: Schéma vytvořené simulace

Zařízení Inter, Com, Mu, a Pc jsou propojená s přepínači ethernetovým kabelem s omezenou rychlostí na 100 Mb/s a ztrátovostí packetu 0,01%. Switche jsou připojeny k FIFO Switchi pomocí optického kabelu s rychlostí 40 Gb/s a ztrátovostí packetu 0,001%. Stejným způsobem jako jsou propojeny switche, je propojená i SCADA se zařízením FIFO Switch.

3.3.1 Průběh simulace

V následující části je popsán průběh vytvořené simulace. Na obrázku 3.5 je grafické znázornění posloupnosti událostí při výskytu alarmové hodnoty.

Za normálních podmínek, kdy není zjištěna alarmová hodnota, odesílá zařízení Merge unit hodnoty napětí a proudu pomocí všesměrových SV zpráv. Událost 1 zobrazuje odeslání informace o poruše vyskytující se v rozvodně. Logický uzel PIOC v zařízení PC přijme a vyhodnotí zprávu s nouzovou hodnotou, kterou obdržel od zařízení Mu. Tato situace je označena číslem 2. Po vyhodnocení a zjištění, že se jedná o alarmovou zprávu,vzniká situace 3, kde začne zařízení PC zasílat sekvenci zpráv GOOSE k zařízení Inter. Logický uzel CSWI v zařízení Inter, v události 4, příjme tyto zprávy. Po zpracování dat vytváří logický uzel další posloupnost zpráv GOOSE, v události 5, pro zařízení Com. V případě události 6 jsou tyto zprávy zpracovávány logickým uzlem XCBR v zařízení Com, aby se aktivoval jistič systému v zasažené oblasti. Jakmile se aktivace provede, generuje Com sekvenci GOOSE zpráv o změně stavu jističe (událost 7). V události 8 CSWI zpracuje zprávy a pamatuje si, že jistič byl aktivován.



Obr. 3.5: Posloupnost událostí rozvodny

3.3.2 Nastavení simulace

Nastavení sítě a simulace se provádí v souboru *.ini, výpisy z nastavení zařízení jsou součástí této kapitoly. V prvním výpisu 3.1 je nastavení intervalu odeslání první zprávy, kterou se zařízení mezi sebou identifikují. Dále je zde určení skupiny zařízení a jejich typ.

Výpis 3.1: Nastavení simulace

```
**. Pc *. goMod . startTime = 0s
**. Pc *. goMod . iedType = default
**. Pc *. goMod . goID = "GOOSEIDPC"
**. Pc *. subs . sendInterval = 0s
**. Inter *. cli . startTime = 0s
**. Inter *. cli . iedType = "inter"
**. Inter *. cli . goID = "GOOSEIDINTER"
**. Com *. cli. startTime = 0s
**. Com *. cli. iedType = "com"
**. Com *. cli. goID = "GOOSEIDCOM"
**. Mu *. cli. startTime = 0s
**. Mu *. cli. iedType = "mu"
```

Výpis 3.2 zobrazuje nastavení zařízení Pc. Je zde nastavení MAC adresy zařízení, multicastové adresy sloužící k rozesílání SMV a GOOSE zpráv, ID zařízení a aplikací, na které má zprávu rozesílat. Nastavení zbylých dvou zařízení je v tabulce 3.1.

Výpis 3.2: Základní nastavení zařízení Pc1

```
**. Pc1 .mac. address = "B8:89:B9:20:02:01"
**. Pc1 .mac. multiCastGroupAddr0 = "01:0C:CD:01:01:FF"
**. Pc1 .mac. multiCastGroupAddr1 = "01:0C:CD:04:01:FF"
**. Pc1 . goMod . myAppID = 0 x0001
**. Pc1 . goMod . interAppID0 = 0 x0002
```

Tab. 3.1: Nastavení dalších zařízení Pc

Zařízení	MAC adresa	Multicast pro GOOSE	Multicast pro SMV	ID
Inter1	B8:89:B9:20:02:01	01:0C:CD:01:01:FF	01:0C:CD:04:01:FF	0x0001
Inter2	B8:89:B9:21:02:01	01:0C:CD:01:02:FF	01:0C:CD:04:02:FF	0x0011
Inter3	B8:89:B9:22:02:01	01:0C:CD:01:03:FF	01:0C:CD:04:03:FF	0x0021

Výpis 3.3 obsahuje nastavení zařízení Inter1, kde je nastavena MAC adresa zařízení Inter,multicastové adresy pro příjem a rozesílání zpráv GOOSE. Natavení dalších zařízení je v tabulce 3.2.

Výpis 3.3: Základní nastavení zařízení Inter1

```
**. Inter1 . mac . address = "B8:89:B9:20:02:02"
**. Inter1 . mac . multiCastGroupAddr0 ="01:0C:CD:01:
01:FF"
**. Inter1 . cli . destAddress = "01:0C:CD:01:01:FF"
**. Inter1 . cli . cbRef = "IEDINTER1/LLN0$GO$EVal"
**. Inter1 . cli . dataSetRef = "IEDINTER1/LLN0$Eval
$Eval_DataSet"
**. Inter1 . cli . myAppID = 0 x0002
**. Inter1 . cli . pcAppID0 = 0 x0001
**. Inter1 . cli . comAppID0 = 0 x0003
```

Tab. 3.2: Nastavení dalších zařízení Inter

Zařízení	MAC adresa	Multicast pro GOOSE zprávy	ID Zařízení
Inter1	B8:89:B9:20:02:02	01:0C:CD:01:01:FF	0x0002
Inter2	B8:89:B9:21:02:02	01:0C:CD:01:02:FF	0x0012
Inter3	B8:89:B9:22:02:02	01:0C:CD:01:03:FF	0x0022

Výpis 3.4 obsahuje nastavení zařízení Com1, kde je nastavena MAC adresa zařízení Com, multicastové adresy pro příjem a rozesílání zpráv GOOSE. Nastavení dalších zařízení je v tabulce 3.3.

Výpis 3.4: Základní nastavení zařízení Com1

```
**. Com1 .mac. address = "B8:89:B9:20:02:03"
**. Com1 .mac. multiCastGroupAddr0 = "01:0C:CD:01:01:FF"
**. Com1 .cli. destAddress = "01:0C:CD:01:01:FF"
**. Com1 .cli. cbRef = "IEDCOM1/LLN0$GO$EVal"
**. Com1 .cli. dataSetRef = "IEDCOM1/LLN0$Eval
$Eval_DataSet"
**. Com1 .cli. myAppID = 0 x0003 # APPID do com
**. Com1 .cli. interAppID0 = 0 x0002 # APPID do inter1
```

Tab. 3.3: Nastavení dalších zařízení Com

Zařízení	MAC adresa	Multicast pro GOOSE	Multicast pro SMV	ID
Com1	B8:89:B9:20:02:03	01:0C:CD:01:01:FF	01:0C:CD:04:01:FF	0x0003
Com2	B8:89:B9:21:02:03	01:0C:CD:01:02:FF	01:0C:CD:04:02:FF	0x0013
Com3	B8:89:B9:22:02:03	01:0C:CD:01:03:FF	01:0C:CD:04:03:FF	0x0023

Výpis 3.5 obsahuje nastavení zařízení Mu1, kde je nastavena MAC adresa zařízení Mu1 ,multicastové adresy pro rozesílání SMV zpráv. Nastavení dalších zařízení je v tabulce 3.4.

Výpis 3.5: Základní nastavení zařízení Mu1

```
**. Mu1 .mac. address = "B8:89:B9:20:02:04"
**. Mu1 .cli. destAddress = "01:0C:CD:04:01:FF"
```

Tab. 3.4: Nastavení dalších zařízení Mu

Zařízení	MAC adresa	Multicast pro SMV
Mu1	B8:89:B9:20:02:04	01:0C:CD:04:01:FF
Mu2	B8:89:B9:21:02:04	01:0C:CD:04:02:FF
Mu3	B8:89:B9:22:02:04	01:0C:CD:04:03:FF

Výpis 3.6 obsahuje nastavení zařízení Scada, kde je nastavena MAC adresa zařízení Scada ,cílová MAC adresa a velikost paketu.

Výpis 3.6: Základní nastavení zařízení Scada

```
**. SCADA . csmacdSupport = false
**. SCADA .mac . address = "B8:89:B9:20:FF:FF"
**. SCADA .app . destAddress = "01:0C:CD:01:01:FF"
**. SCADA .app . packetLength = 150B
```

Po nastavení zařízení je potřeba importovat a nastavit modul „pcapecorder“ sloužící k zachytávání komunikace. Importování se provádí pomocí příkazu „import“ v programovatelné části modulu, kterou zachycuje výpis 3.7. Nastavení modulu je zobrazeno ve výpisu3.8

Výpis 3.7: Nastavení modulu PcapRecorder v modulu IecFifoSwitch

```
import inet.util.PcapRecorder;
module IecFifoSwitch
{
    parameters:
        @node();
        @labels(node,ethernet-node);
        @display("bgb=406,276;i=abstract/switch");
        bool hasStatus = default(false);
        int numPcapRecorders = default(0);
    gates:
        inout ethg[] @labels(EtherFrame-conn);
    submodules:
          pcapRecorder[numPcapRecorders]: PcapRecorder {
            @display("p=291,60");
        }
```

Výpis 3.8: Nastavení modulu pcaprecorder

```
**.numPcapRecorders=1
**.FiFoSwitch.pcapRecorder[0].pcapFile = "results/fifo.
   pcap"
**.SCADA.pcapRecorder[0].pcapFile = "results/SCADA.pcap"
**.Com1.pcapRecorder[0].pcapFile = "results/Com.pcap"
```

Výpis 3.9 zobrazuje nastavení jednoduchého modulu s názvem EtherAppSv, který je součástí složeného modulu MergeUnit. Stára se o generování SV zpráv v daném intervalu, pro ostatní zařízení. Tyto zprávy obsahují hodnoty napětí a proudu.

Výpis 3.9: Základní nastavení jednoduchého modulu EtherAppSv

```
simple EtherAppSv
{
    parameters:
       string pcIed = default(".^.goMod");
       string destAddress = default("");
       double startTime @unit(s) = default(this.
          sendInterval);
       double stopTime @unit(s) = default(-1s);
       double sendInterval @unit(s) = default(208333e-9s)
          ;
```

```
        double sampleInterval @unit(s) = default(208333e-9
           s);
        double samplingRate = default(4800);
```

Důležitým prvkem celé simulace je jednoduchý modul s názvem EtherAppGoose. Nachází se v složených modulech Inter, Com, Pc a jeho zakladní nastavení je ve výpisu 3.10. Dle nastavení plní tyto funkce (ochranu, blokování a ovládání)

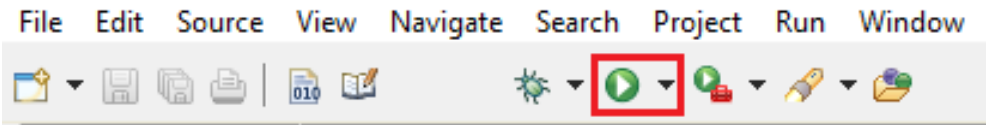
Výpis 3.10: Základní nastavení jednoduchého modulu EtherAppGoose

```
simple EtherAppGoose
{
    parameters:

        string destAddress = default("");
        double startTime @unit(s) = default(this.
           sendInterval);
        double stopTime @unit(s) = default(-1s);
        double sendInterval @unit(s) = default(16400e-3s);
        string iedType = default("pc");
```

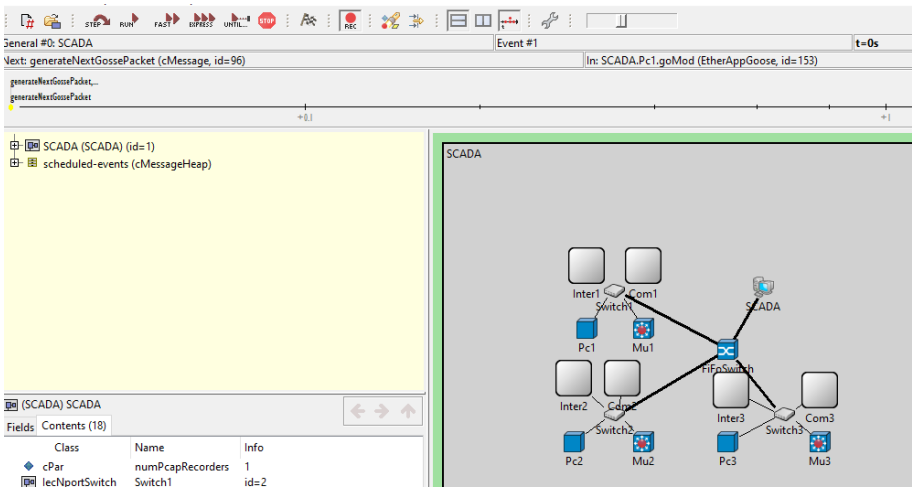
3.4 Spuštění simulace

Připravenou a nastavenou síť si můžeme spustit tlačítkem play vyznačeném na obrázku 3.6 .



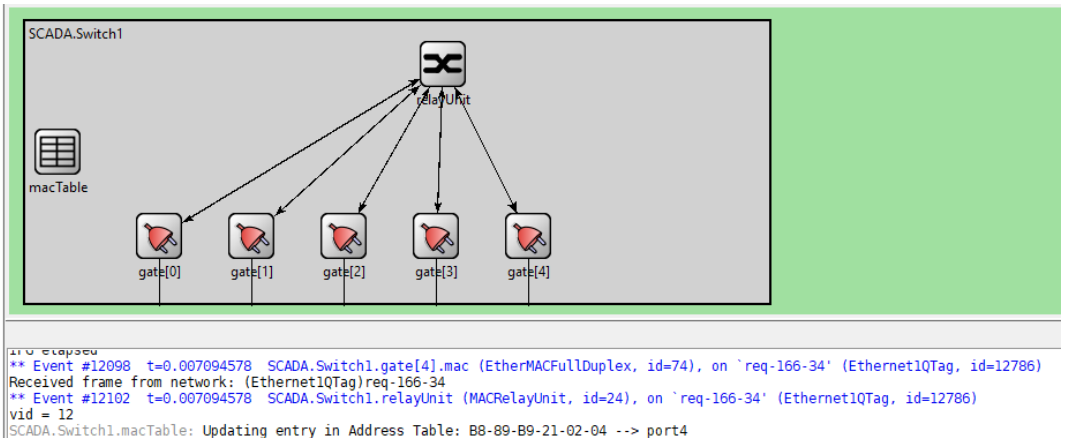
Obr. 3.6: Tlačítko pro spuštění simulace

Po spuštění se nám otevře simulační prostředí OMNeT++, zobrazeno na obrázku 3.7, ve kterém probíhá samotná simulace. Zahájení simulace se provede kliknutím na play.



Obr. 3.7: Simulačni prostředí programu OMNeT++

Simulační prostředí neumožnuje pouze spuštění, ale je možné simulaci zrychlit nebo zpomalit, krokovat nebo nastavit pouze časový úsek, ve kterém má simulace probíhat. Nespornou výhodou je možnost pozorování komunikace každého zařízení v reálném čase, jak je zobrazeno na obrázku 3.8



Obr. 3.8: Průběh komunikace v reálném čase v zařízení Switch1

3.4.1 Zahájení komunikace

Prvotní komunikace, v čase nula, je zobrazena na obrázku 3.9. Každé zařízení naváže spojení s lokálním přepínačem, aby přepínač zjistil, které zařízení má na kterém portu připojené a tyto hodnoty si zapíše do tabulky adres. Následně začíná vzájemná komunikace mezi všemi zařízeními. Zařízení Mu odesílá SMV zprávy o velikosti 136 bajtů, zařízení Pc GOOSE zprávy o velikosti 147 bajtů, zařízení Com GOOSE zprávu o velikosti 150 bajtů a zařízení Inter GOOSE zprávu o velikosti 156 bajtů. Rozdílné velikosti zpráv jsem nastavil proto, aby bylo možné ve výpisu identifikovat, od kterého zařízení zprávy pochází. Standardní velikosti zpráv dle standardu IEC 61850 jsou 160 bajtů pro GOOSE a 140 bajtů pro SV.

Time	Src/Dest	Name
0	Pc1 --> Switch1	req-155-
0	Pc2 --> Switch2	req-159-
0	Mu1 --> Switch1	req-165-
0	Mu2 --> Switch2	req-168-
0	Inter1 --> Switch1	req-171-
0	Inter2 --> Switch2	req-174-
0	Com1 --> Switch1	req-177-
0	Com2 --> Switch2	req-180-
0	Com3 --> Switch3	req-183-
0	Inter3 --> Switch3	req-186-
0	Mu3 --> Switch3	req-189-
0	Pc3 --> Switch3	req-190-

Obr. 3.9: Zahájení komunikace mezi zařízeními a přepínači

3.4.2 Průběh komunikace

Obsahem této kapitoly je ověření průběhu komunikace, která je zobrazena na obrázku 3.5. V simulačním prostředí bylo nahlíženo do potřebných zařízení v reálném čase a byly zaznamenány průběhy komunikace.

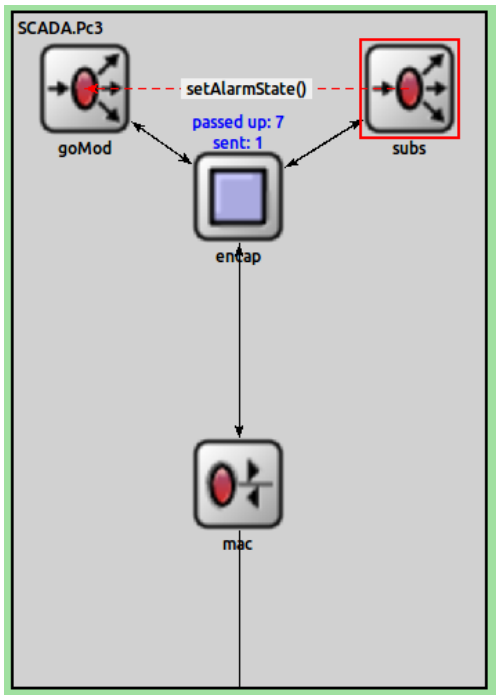
První zařízení které jsem testoval, je Merge unit (Mu). Zařízení odesílá SV zprávy v pravidelném intervalu, který je dle standardu IEC 61850 nastaven na 4800 zpráv za sekundu. O generování těchto zpráv se v zařízení Mu stará jednoduchý modul s názvem EtherAppSv. Pro ověření generování zpráv je na obrázku 3.10 zobrazen výpis z modulu EtherAppSv. Je zde vidět i časová pravidelnost vytváření zpráv v intervalu 0,208 ms (milisekund).

```
Generating SV packet `req-163-346'
** Event #113246  t=0.072291551  SCADA.Mu1.cli (EtherAppSv, id=163),
** Event #113247  t=0.072291551  SCADA.Mu1.cli (EtherAppSv, id=163),
Generating SV packet `req-163-347'
** Event #113573  t=0.072499884  SCADA.Mu1.cli (EtherAppSv, id=163),
** Event #113574  t=0.072499884  SCADA.Mu1.cli (EtherAppSv, id=163),
Generating SV packet `req-163-348'
** Event #113900  t=0.072708217  SCADA.Mu1.cli (EtherAppSv, id=163),
** Event #113901  t=0.072708217  SCADA.Mu1.cli (EtherAppSv, id=163),
Generating SV packet `req-163-349'
** Event #114227  t=0.07291655  SCADA.Mu1.cli (EtherAppSv, id=163),
** Event #114228  t=0.07291655  SCADA.Mu1.cli (EtherAppSv, id=163),
Generating SV packet `req-163-350'
```

Obr. 3.10: Záznam komunikace v modulu EtherAppSv v reálném čase

Dalším zařízením je Pc. Má na starost příjem a vyhodnocování zpráv s hodnotami napětí a proudu, které dostáva od zařízení Mu. V čase 0,833 ms je vyslána SMV zpráva zařízením Mu, která obsahuje informace o překročení mezní hodnoty napětí

nebo proudu. Zprávu obdrží zařízení Pc v čase 0,87 ms. Přijeti alarmové zprávy s požadavkem na poslání GOOSE zprávy je na obrázku 3.11.



Obr. 3.11: Přijetí alarmové zprávy v zařízení Pc3

Po přijetí alarmové zprávy je vygenerována GOOSE zpráva o události pro zařízení Inter. Průběh komunikace po přijetí alarmové zprávy je na obrázku 3.12. Modul mac přijal zprávu, kterou následně poslal na zařízení encap, které zprávu zasílá na modul subs. Modul zjistí alarmovou hodnotu a vyžádá zaslání GOOSE zprávy modulem goMod. Na obrázku 3.12 lze vidět, že zprávy, které nejsou určeny zařízení Pc3, jsou modulem mac zahazovány.

```
0.000844212       ---> mac          req-189-4   EtherSvData:106 bytes   ETH: B8-89-B9-22-02-04 > 01-0C-CD-04-03-FF (136 bytes)
0.000855092       mac --> encap     req-189-4   EtherSvData:106 bytes   ETH: B8-89-B9-22-02-04 > 01-0C-CD-04-03-FF (128 bytes)
0.000855092       encap --> subs    req-189-4   EtherSvData:106 bytes
0.000855092       goMod --> encap   req-190-2   EtherGooseData:117 bytes
0.000855092       encap --> mac     req-190-2   EtherGooseData:117 bytes   ETH: 00-00-00-00-00-00 > 01-0C-CD-01-03-FF (139 bytes)
0.000855092       mac --->          req-190-2   EtherGooseData:117 bytes   ETH: B8-89-B9-22-02-01 > 01-0C-CD-01-03-FF (147 bytes)
0.000856051999    ---> mac          req-165-4   EtherSvData:106 bytes   ETH: B8-89-B9-20-02-04 > 01-0C-CD-04-01-FF (136 bytes)
0.000867891998    ---> mac          req-168-4   EtherSvData:106 bytes   ETH: B8-89-B9-21-02-04 > 01-0C-CD-04-02-FF (136 bytes)
```

Obr. 3.12: Průběh komunikace po přijetí alarmové zprávy

Na obrázku 3.12 je zobrazen také model komunikace Publisher-Subscriber. Jedná se o druh komunikace, kdy Publisher neboli vydavatel vysílá předem určené skupiny dat bez ohledu na to, komu mají být data doručena. Subscriber neboli odběratel ze sběrnice odebírá nastavenou sadu dat, nehledě na to, kterým vydavatelem byla zaslána.

Dalším krokem komunikace je příjetí GOOSE zprávy od zařízení Pc zařízením Inter. Na základě přijatých dat vygeneruje jednoduchý modul EtherAppGoose posloupnost GOOSE zpráv pro zařízení Com. Záznam této komunikace je na obrázku 3.13.

```
** Event #338945  t=0.218087585  SCADA.Inter3.cli (EtherAppGoose, id=189), on
Received packet `req-194-6'
** Event #338955  t=0.218101104997  SCADA.Inter3.cli (EtherAppGoose, id=189),
Generating GOOSE packet `req-189-6'
Next 0.466101104997 SendInterval 0.248
Next 0.466101104997 SendInterval 0.496
** Event #339422  t=0.218184330997  SCADA.Inter3.cli (EtherAppGoose, id=189),
```

Obr. 3.13: Přijetí GOOSE zprávy a následné generování zprávy GOOSE

Posledním zařízením obsaženém v simulaci je Com. Vyhodnocuje GOOSE zprávy od zařízení Inter. Na základě těchto zpráv zasílá příkazy k otevření nebo uzavření jističe v postižené oblasti rozvodny. Vytváření těchto požadavků v zařízení Com je ověřeno na obrázku 3.14.

```
** Event #2222  t=0.000917731997  SCADA.Com1.cli (EtherAppGoose, id=177),
Received packet `req-169-2'
ZMENA STAVU JISTICE_ PUVODNI HODNOTA0
ZMENA STAVU JISTICE_ NOVA HODNOTA 1
Generating GOOSE packet `req-177-2'
Next 0.031917731997 SendInterval 0.031
Next 0.031917731997 SendInterval 0.062
** Event #2693  t=0.001101104997  SCADA.Com1.cli (EtherAppGoose, id=177),
Received packet `req-153-3'
** Event #2765  t=0.001126064997  SCADA.Com1.cli (EtherAppGoose, id=177),
Received packet `req-169-3'
ZMENA STAVU JISTICE_ PUVODNI HODNOTA1
ZMENA STAVU JISTICE_ NOVA HODNOTA 0
Generating GOOSE packet `req-177-3'
Next 0.032126064997 SendInterval 0.031
Next 0.032126064997 SendInterval 0.062
```

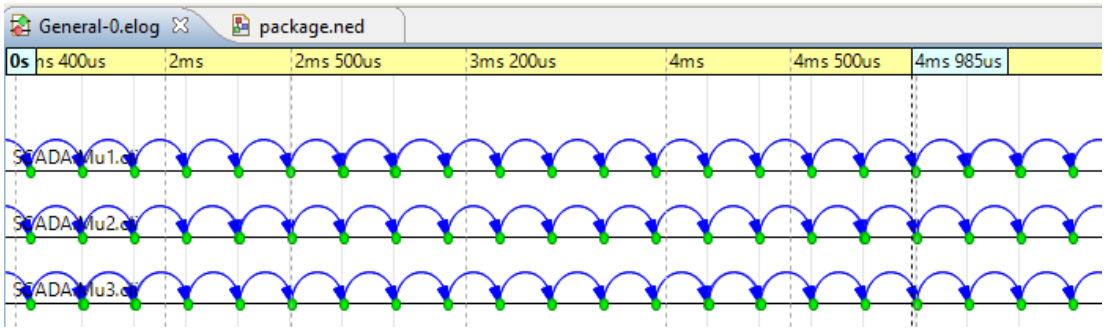
Obr. 3.14: Vytvoření požadavku pro změnu stavu jističe

Na výše zobrazených výpisech ze zařízení lze vidět, že vytvořená simulace komunikuje dle schématu a standardu IEC 61850.

3.4.3 Výsledky simulace

Simulační program OMNeT++ umožnuje záznam veškeré komunikace do časové osy, na které je možné si pomocí filtrů nastavit záznamy, které potřebujeme. Výsledky se ukládají do složky results umístěné v projektu. Dále program ukládá skalární a vektorové veličiny, díky kterým je možné vytvářet grafy. Na obrázku 3.15 je

vidět časová osa pro zařízení Mu. Byla odfiltrována ostatní zařízení, aby bylo vidět intervaly vytváření SV zpráv s hodnotami napětí a proudu.



Obr. 3.15: Záznam časové osy pro vytváření SV zpráv v zařízeních Mu

Doplňující knihovna inet umožňuje nahrávání také do .pcap souborů. Jedná se o jednoduchý modul s názvem PcapRecorder. V rámci mé simulace jsem provedl implementaci tohoto modulu do zařízení FIFOSwitch, SCADA a Com, viz nastavení ve výpisu 3.8. Po spuštění a ukončení simulace se vytvořily .pcap soubory ve složce results. Soubory však byly prázdné, proto jsem modul otevřel v reálném čase, kde jsem zjistil, že modul PcapRecorder podporuje pouze packety IPv4/6. Na obrázku je vidět, že modul packety zachytává, ale pokud packet nepatří do IPv4/6 datagramu je zahozen.

```
DA.FiFoSwitch.mac[0] (EtherMACFullDuplex, id=269), on selfmsg `EndTransmission' (cMessage, id=84)
pRecorder::recordPacket(SCADA.FiFoSwitch.mac[0].req-193-1100, 1)
ket Ethernet1QTag 'req-193-1100': Packet EtherSvData 'req-193-1100': CANNOT DECODE, packet doesn't contain either IPv4 or IPv6 Datagram
DA.FiFoSwitch.mac[1] (EtherMACFullDuplex, id=270), on selfmsg `EndTransmission' (cMessage, id=87)
pRecorder::recordPacket(SCADA.FiFoSwitch.mac[1].req-166-1100, 1)
ket Ethernet1QTag 'req-166-1100': Packet EtherSvData 'req-166-1100': CANNOT DECODE, packet doesn't contain either IPv4 or IPv6 Datagram
DA.FiFoSwitch.mac[2] (EtherMACFullDuplex, id=271), on selfmsg `EndTransmission' (cMessage, id=90)
```

Obr. 3.16: Záznam z modulu PcapRecorder

Vytvořená simulace umožňuje zkoumat rychlosti přenosu zpráv potřebných ke správnému fungovaní rozvodny,vytváření alarmových a řídících zpráv. Veškeré síťové prvky se dají detailně nastavit a tím dosáhnout vytvoření potřebné testovací sítě. Díky instalaci ve virtuálním prostředí, je dobře přenositelná a vhodná ke studijním účelům.

Závěr

Cílem diplomové práce bylo provést analýzu standardu IEC 61850, seznámit se se simulačním prostředím a vytvořit simulaci obsahující síť, komunikující dle tohoto standardu.

Tato práce je rozdělena na tři hlavní kapitoly. První kapitola přibližuje technologii Inteligentních sítí. Na tuto technologii je vázaná SCADA, která je v dnešní době využívána stále častěji a proto je popsána v první části práce. Je zde popsán standard IEC 61850 který je velmi důležitý z hlediska komunikace v energetickém průmyslu. Součásti standardu jsou protokoly MMS, GOOSE a SMV,které jsou popsány v této kapitole. Konec první kapitoly je věnován zranitelnosti standardu a jsou zde popsány možné typy útoků.

Druhá kapitola je zaměřena na výběr vhodného simulačního nástroje. Jsou popsány tři simulační nástroje které jsou porovnány v přehledné tabulce. Na základě srovnání byl vybrán simulační nástroj OMNeT++. Jeho nespornou výhodou je možnost importu knihoven, které plně podporují standard IEC 61850. Tyto knihovny obsahují moduly, které byly použity v simulaci a v práci jsou jednotlivě popsány.

Poslední část je věnována kompletní instalaci, nastavení a spuštění simulace. Virtuální prostředí pro instalaci OMNeT++ jsem zvolil VM Virtual box s operačním systémem Linux Ubuntu. Instalace OMNeT++ je podrobně popsána po jednotlivých příkazech. V simulaci byla použita jednotlivá zařízení, která mezi sebou komunikují pomocí standardem IEC 61850. Cílem bylo dokázat přítomnost a funkčnost zpráv SMV,GOOSE a MMS. Vytvořená simulace ověřuje funkčnost pouze dvou protokolů, kterými jsou GOOSE a SMV. V závěru jsou výpisy z různých zařízení, které prokazují funkčnost zasílání SMV a GOOSE zpráv. Protokol MMS, který využívá komunikaci klient-server, se z časových důvodů nepodařilo zprovoznit. Jedná se o protokol, který by ze stanice Server, zasílal informace o množství zaslaných zpráv, množství kritických zpráv a změn stavu jističe, do zařízení SCADA. Komunikace by probíhala v určených intervalech a každá zpráva by měla pevnou velikost.

Literatura

[1] *Jak funguje a co je smart grid* [online]. [cit. 4. 11. 2019]. Dostupné z URL: <http://www.proelektrotechniky.cz/vzdelavani/22.php>

[2] *An Introduction to Smart Grid* [online]. [cit. 05. 11. 2019]. Dostupné z URL: «<https://www.ecomena.org/smart-grid/>

[3] *How SCADA Systems Work?* [online]. [cit. 4. 11. 2019]. Dostupné z URL: <https://www.elprocus.com/scada-systems-work/>

[4] *IEC 61850: soubor norem pro komunikaci v energetice s velkým potenciálem výhod* [online]. [cit. 4. 11. 2019]. Dostupné z URL: <https://www.allaboutcircuits.com/technical-articles/quadrature-phase-shift-keying-qpsk-modulation/>

[5] *Structure of the standard* [online]. [cit. 05. 11. 2019]. Dostupné z URL: «<https://www.researchgate.net/publication/281770126_An_Autonomic_and_Ubiquitous_Framework_for_Smart_Grid_Management>

[6] *Soubor norem IEC 61850* [online]. [cit. 4. 11. 2019]. Dostupné z URL: <http://www.controlengcesko.com/index.php?id=47&no_cache=1&tx_ttnews[tt_news]=3564&cHash=5b883560c4&type=98>

[7] Petr MATOUŠEK. *Description of IEC 61850 Communication* Fakulta informačních technologií VUT v Brně, 2018 . [cit. 4. 11. 2019].>

[8] STODŮLKA, Ivo. *Model elektrické stanice s komunikačním protokolem IEC 61850* [online] Vysoké učení technické v Brně. Fakulta elektrotechniky a komunikačních technologií. Ústav elektroenergetiky. [cit. 4. 11. 2019]. Dostupné z URL: <http://hdl.handle.net/11012/3566>

[9] ŠIKULA, Jiří. *Převod standardu IEC 61850 na komunikační protokol ModBus* [online] Vysoké učení technické v Brně. Fakulta elektrotechniky a komunikačních technologií. Ústav elektrotechnologie. [cit. 4. 11. 2019]. Dostupné z URL: <https://www.vutbr.cz/www_base/zav_prace_soubor_verejne.php?file_id=125516>

[10] *Simulation models for IEC 61850 communication in electrical substations using GOOSE and SMV time-critical messages* [cit. 4. 11. 2019].> Dostupné z URL: <https://www.researchgate.net/publication/304456800_Simulation_models_for_IEC_61850_communication_in_electrical_substations_using_GOOSE_and_SMV_time-critical_messages>

[11] *Securing restricted publisher-subscriber communications in smart grid substations* [cit. 4. 11. 2019].> Dostupné z URL: <https://www.researchgate.net/publication/324179255_Securing_restricted_publisher-subscriber_communications_in_smart_grid_substations>

[12] *Exploiting the GOOSE protocol* [cit. 4. 11. 2019].> Dostupné z URL: <https://www.semanticscholar.org/paper/Exploiting-the-GOOSE-protocol%3A-A-practical-attack-Hoyos-Dehus/e63fda4f86b8355c0b794e75f81c25c73e33c3fa>

[13] *The IEC 61850 Sampled Measured Values Protocol: Analysis, Threat Identification, and Feasibility of Using NN Forecasters to Detect Spoofed Packets* [online] [cit. 4. 11. 2019]. Dostupné z URL: <https://www.mdpi.com/1996-1073/12/19/3731/htm>

[14] *Protocol MMS* [online] [cit. 4. 11. 2019]. Dostupné z URL: <http://digitalsubstation.com/blog/2013/04/12/protokol-mms/>

[15] *IEC 61850: Technology standards and cyber-threats* [online] [cit. 4. 11. 2019]. Dostupné z URL: <https://ieeexplore.ieee.org/document/7555647>

[16] *What is ns-3* [online] [cit. 4. 11. 2019]. Dostupné z URL: <https://www.nsnam.org/about/what-is-ns-3/>

[17] *RIVERBED MODELER* [online] [cit. 4. 11. 2019]. Dostupné z URL: <https://www.riverbed.com/gb/products/steelcentral/steelcentral-riverbed-modeler.html>

[18] *OMNET++* [online] [cit. 4. 11. 2019]. Dostupné z URL: <https://omnetpp.org/>

[19] *Inetmanet knihovna* [online] [cit. 4. 11. 2019]. Dostupné z URL: <https://github.com/hectordelahoz/ProcessBusIec61850/tree/master/iec61850InetV2.6/inet>

[20] *On Automatic Generation of IEC61850/IEC61499 Substation Automation Systems Enabled by Ontology* [online] [cit. 20. 4. 2020]. Dostupné z URL: <http://vyatkin.org/publ/2014/IECON%20eSWRL.pdf>

[21] *Real-Time Analysis of Time-Critical Messages in IEC 61850 Electrical Substation Communication Systems* [online] [cit. 20. 4. 2020]. Dostupné z URL: <https://www.researchgate.net/publication/333760965_Real-Time_Analysis_of_Time-Critical_Messages_in_IEC_61850_Electrical_Substation_Communication_Systems>

[22] *On Automatic Generation of IEC61850/IEC61499 Substation Automation Systems Enabled by Ontology* [online] [cit. 20. 4. 2020]. Dostupné z URL: <http://vyatkin.org/publ/2014/IECON%20eSWRL.pdf>

Seznam symbolů, veličin a zkratek

APDU	Application Protocol Data Unit
APPID	Application ID
ASDU	Application Service Data Units
ARP	Address Resolution Protocol
DoS	Denial of Service
GNU	General Public Licence
FTP	File Transfer Protocol
GOOSE	Generic Object Oriented Substation Event
HTTP	Hypertext Transfer Protocol
IED	Inteligent Electronic Device
IT	Information Technology
LAN	Local Area Network
MAC	Media Access Control
MMS	Manufacturing Message Specification
MPLS	Multiprotocol Label Switching
MU	Merge Unit
NED	Network Description
OSPF	Open Shortest Path First
PLC	Programmable Logic Controller
RTU	Remote Terminal Unit
SCADA	Supervisory Control And Data Acquisition
SVPDU	Samled Value Protocol Data Unit
TCP	Transmission Control Protocol
VLAN	Virtual Local Area Network
VoIP	Voice over Internet Protocol
WAN	Wide Area Network
XML	eXtensible Markup Language

Seznam příloh

A Zdrojové kódy simulace

V elektronické podobě je dostupný soubor Workspace, který obsahuje veškerá nastavení simulace a topologie sítě. Součásti soboru jsou také veškeré výsledky vytvořené simulace. Soubor lze importovat do programu OMNeT++ jako existující projekt.