VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

Fakulta elektrotechniky
a komunikačních technologií

DIPLOMOVÁ PRÁCE

Brno, 2021 Bc. Antonín Bohačík

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

MANAGEMENT POLYGONU ENERGETICKÉ PŘENOSOVÉ SOUSTAVY
MANAGEMENT OF THE ENERGY TRANSMISSION SYSTEM POLYGON

DIPLOMOVÁ PRÁCE
MASTER'S THESIS

AUTOR PRÁCE — **Bc. Antonín Bohačík**
AUTHOR

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

BRNO 2021

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
FAKULTA ELEKTROTECHNIKY A KOMUNIKAČNÍCH TECHNOLOGIÍ

Diplomová práce

magisterský navazující studijní program **Informační bezpečnost**

Ústav telekomunikací

Student: Bc. Antonín Bohačík ***ID:*** 195149
Ročník: 2 ***Akademický rok:*** 2020/21

NÁZEV TÉMATU:

Management polygonu energetické přenosové soustavy

POKYNY PRO VYPRACOVÁNÍ:

Cílem práce je realizace ovládacího rozhraní pro polygon simulující datovou komunikaci v energetické přenosové soustavě. Nastudujte problematiku standardu IEC 60870 a IEC 61850, které slouží v datové komunikaci v rámci energetické přenosové soustavy a jednotlivých rozvoden. V rámci standardu IEC 61850 se zaměřte na část 80-1, která popisuje výměnu informací mezi protokoly z výše uvedených standardů. Dílčím cílem práce bude implementace standardu IEC 61850-80-1 do vytvořeného polygonu. Dále budou vytvořeny a otestovány scénáře (minimálně šest) simulující standardní provoz, kritické stavy v rozvodných stanicích a útoky na infrastrukturu.
Výstupem diplomové práce bude rozhraní, které bude umožňovat správu jednotlivých rozvoden v rámci energetické přenosové soustavy s možností simulace standardního provozu, kritických stavů a vybraných útoků. Dále budou jednotlivé rozvodny rozšířeny o modul implementující IEC 61850-80-1 pro výměnu informací mezi standardy IEC 61850 a IEC 60870.

DOPORUČENÁ LITERATURA:

[1] MATOUŠEK Petr. Description and analysis of IEC 104 Protocol. FIT-TR-2017-12, Brno: Faculty of Information Technology BUT, 2017.

[2] MATOUŠEK Petr. Description of IEC 61850 Communication. FIT-TR-2018-01, Brno: Fakulta informačních technologií VUT v Brně, 2018.

Termín zadání: 1.2.2021 ***Termín odevzdání:*** 24.5.2021

Vedoucí práce: Ing. Petr Blažek

doc. Ing. Jan Hajný, Ph.D.
předseda rady studijního programu

ABSTRAKT

Diplomová práce je zaměřena na vytvoření ovládacího rozhraní pro polygon simulující datovou část rozvodné sítě České republiky, kde je komunikace mezi jednotlivými rozvodnami realizována protokolem IEC 60870-5-104. Teoretická část práce detailně vysvětluje základní principy, vlastnosti a možnosti komunikačních standardů IEC 60870 a IEC 61850. Další část je zaměřena na samotnou realizaci a následnou implementaci ovládacího rozhraní včetně implementace modulu IEC 61850-80-1 pro převod dat mezi zmíněnými standardy. Poslední část popisuje vytvořené scénáře chování či samotný rozbor komunikace.

ABSTRACT

The diploma thesis is focused on the creation of a control interface for a polygon simulating the electrical distribution network of the Czech Republic, where communication between substations is realized by IEC 60870-5-104 protocol. The theoretical part of the thesis explains the basic principles, properties and possibilities of communication standards IEC 60870 and IEC 61850. The next part is focused on the actual implementation and subsequent implementation of the control interface, including the implementation of the IEC 61850-80-1 module for data transfer between the mentioned standards. The last part describes the created behavior scenarios or the analysis of communication itself.

KLÍČOVÁ SLOVA

Elektrárna, emulace, IEC 60870, IEC 61850, polygon, RaspberryPi, rozvodna, rozvodná síť, SCADA, scénáře chování, simulace, transformátor, webová aplikace

KEY WORDS

Behavior scenario, distribution network, emulation, IEC 60870, IEC 61850, polygon, power station, RaspberryPi, SCADA, substation, simulation, transformer, web application

Citace práce:

BOHAČÍK, Antonín. *Management polygonu energetické přenosové soustavy.* Brno, 2021. Dostupné také z: <`https://www.vutbr.cz/studenti/zav-prace/detail/133561`>. Diplomová práce. Vysoké učení technické v Brně, Fakulta elektrotechniky a komunikačních technologií, Ústav telekomunikací. Vedoucí práce Petr Blažek.

PROHLÁŠENÍ

Prohlašuji, že jsem diplomovou práci na téma „Management polygonu energetické přenosové soustavy“ vypracoval samostatně s použitím odborné literatury a pramenů uvedených na seznamu, který tvoří přílohu této 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 jsem si plně vědom následků porušení ustanovení § 11 a následujících autorského zákona č. 121/2000 Sb., včetně možných trestněprávních důsledků vyplývajících z ustanovení části druhé, hlavy VI. Díl 4 Trestního zákoníku č. 40/2009 Sb.

Datum: ..... Podpis autora: .....

PODĚKOVÁNÍ

Děkuji vedoucímu mé diplomové práce **Ing. Petru Blažkovi** za velmi užitečné konzultace, cenné rady, profesionální přístup a trpělivost při zpracování této práce. Dále bych chtěl poděkovat **Bc. Honzovi Klečkovi** za užitečné rady při vytváření webové aplikace a také **Bc. Jiřímu Dřímalovi** za konzultace spojené s pokročilým programováním.

Datum: ..... Podpis autora: .....

Obsah

Seznam obrázků

Seznam tabulek

Seznam výpisů

Úvod

S nástupem moderní technologie se začal rozvíjet trend dálkového řízení. K tomuto účelu byly navrženy softwary a standardy jako SCADA[1], které informace nejen shromažďují, ale také podporují vzdálenou regulaci a řízení. Vytvoření plně funkčního systému na bázi dálkového řízení není levná záležitost, a tak si mnozí výrobci chrání detailnější informace o svých systémech.

Zde nastává problém vývoje nových technologií, neboť výrobci mnohdy nemají s kým spolupracovat na vývoji zařízení či nemají kde si tato nová zařízení otestovat. Další problém tkví v samotném školení zaměstnanců. Jedná se o časově náročný proces, kde není rozumné tyto nedostatečně zkušené zaměstnance připouštět k reálnému systému dálkového řízení. Proto vznikají simulátory či celé polygony.

Cílem diplomové práce je seznámení se se standardy IEC 60870 a IEC 61850, na základě těchto znalostí vytvořit programové řešení reprezentující jednotlivé stanice polygonu energetické přenosové soustavy, včetně samotného ovládacího a kontrolního rozhraní pro vzdálenou správu. V neposlední řadě také definovat a realizovat scénáře chování stanic polygonu, které odpovídají nejběžnějším stavům reálných elektráren a rozvoden včetně scénářů útoků na infrastrukturu polygonu.

Součástí práce je i detailní rozbor programového řešení stanic polygonu a způsobu simulování komunikačních dat. Rovněž je rozebrána implementace webového rozhraní, které zajišťuje správu nad stanicemi polygonu přenosové soustavy včetně detailního popisu všech vytvořených ovládacích funkcí. Dále je popsán návrh a implementace standardu IEC 61850-80-1 sloužící k převodu dat mezi standardy IEC 61850 a IEC 60870.

Poslední část je věnována testování definovaných scénářů chování, včetně vizuálního znázornění průběhů. Ukázána a rozebrána je i samotná komunikace, navazování a ukončování spojení mezi prvky polygonu či řídicí komunikace mezi webovým serverem a stanicemi polygonu.

[1] Supervisory Control And Data Acquisition

1 Elektrická soustava ČR

Elektrická soustava je systém zařízení, která zajišťují přenos elektrické energie od výrobců k odběratelům. Slouží k přenosu a rozvodu elektrické energie z místa výroby (elektrárny či rozvodny) do místa spotřeby (domácnosti či firmy). Elektrickou soustavu tvoří elektrické stanice, výrobny elektrické energie a elektrické sítě. V České republice se aktuálně nachází přes 36 000 zdrojů vyrábějících elektřinu. Vedle jaderných, uhelných, paroplynových a vodních elektráren jde také o elektrárny solární, větrné nebo na biomasu. Elektrickou soustavu ČR dělíme na přenosovou a distribuční soustavu. [1, 2]

- Přenosová soustava – Je sestavena ze sítí 400 a 220 kV a tvoří páteř elektrické soustavy. Slouží k přenosu výkonů na velké vzdálenosti, zajištění propojení elektrických soustav se soustavami zahraničními či pro vyvedení výkonu z velkých systémových elektráren. S okolními státy je česká PS[1] propojena 11 vedeními 400 kV a 6 vedeními 220 kV. Do PS ČR spadá 12 elektráren a 43 rozvoden. [2, 3]
- Distribuční soustava – Slouží k distribuci výkonu ke konkrétním odběratelům. V ČR je tvořena sítěmi 110 kV a všech nižších napěťových úrovní. Přenáší výkon na kratší vzdálenosti a také jsou do ní připojeny elektrárny nižších výkonů. V některých případech zajišťuje přeshraniční propojení, které však slouží pouze pro napájení určitých oblastí. [1]

Mezi hlavní rozdíly mezi distribuční a přenosovou soustavou patří kromě velikosti napětí jednotlivých prvků sítí také zapojení a způsob provozu sítí PS. V PS jsou až na drobné provozní výjimky všechna vedení a transformátory mezi úrovněmi 400 a 220 kV. Jedná se o propojenou síť, ve které lze kterýkoliv prvek této sítě v případě poruchy okamžitě nahradit jiným. Při odstavení jednoho, nebo více vedení, či transformátorů převezmou jejich zátěž ostatní prvky, které zůstaly v provozu. Systém zálohy se odborně nazývá bezpečnostní kritérium N-1. Tento způsob je použit i při návrhu a provozu rovněž distribuční sítě na napěťové úrovni 110 kV. [1, 2, 3]

V rámci rozvodné sítě ČR je použit komunikační protokol IEC 60870-5, ovšem v praxi (převážně tedy v zahraničí) můžeme narazit na spoustu komunikačních protokolů, mezi které patří např. Modbus, Modbus X, Profibus, Spabus, DNP3[2] nebo IEC 61850. [4]

[1] Přenosová Soustava

[2] Distributed Network Protocol 3

1.1 Supervisory Control And Data Acquisition

Supervisory Control And Data Acquisition zkráceně SCADA, je souhrnné označení pro sadu softwaru a zařízení, která slouží k dispečernímu (dálkovému) řízení z centrálního pracoviště. Používána je převážně k monitorování a řízení průmyslových či jiných technických zařízení a sběru dat. Tento systém je tvořen řídicími a podřízenými stanicemi. Podřízené stanice vykonávají příkazy od nadřazených stanic, jako například řídicí příkazy, nastavování výstupů, či poskytování informací o vstupech. Podřízené stanice slouží pouze ke sběru dat, ale samotný význam těchto dat je zpracováván již řídicí stanicí. [5, 6]

Systém SCADA obecně nezastává funkci plnohodnotného řídicího systému dané technologie, ale je zaměřen převážně na dispečerský dohled, monitorování či případnou parametrizaci. Software typu SCADA je provozován na vyšší úrovni, tj. nad hardwarem (měřiče, PLC[3], senzory atd.), který zprostředkovává konektivitu a sběr dat z dohledových technologických procesů. [5, 7]

Systémy na principu SCADA mohou komunikovat s okolím prostřednictvím specializovaných průmyslových linek či sítí. Ovšem v dnešní době jsou stále častěji využívány počítačové sítě typu ethernet, na kterých probíhá komunikace zpravidla prostřednictvím standardizovaných komunikačních protokolů. SCADA systémy jsou vysoce škálovatelné a umožnují zpracovávat vstupní proměnné v počtu od několika jednotek do stovek tisíců, a to v závislosti na složitosti a rozsahu dohledové technologie. [5, 6]

1.2 IEC 60870

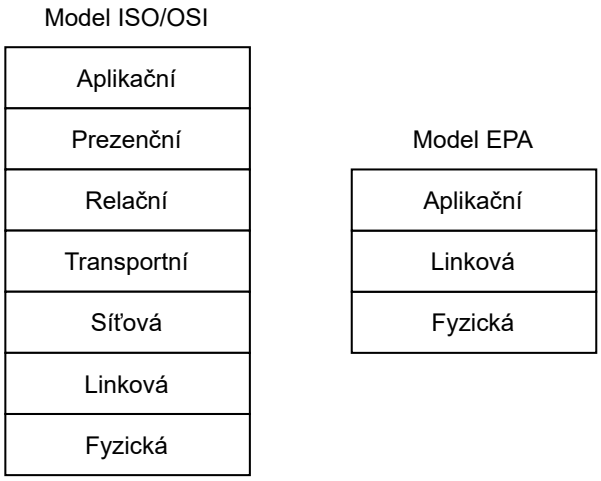
Protokol IEC 60870 byl vytvořen technickou komisí 57 v roce 1995. Jedná se o standard pro dohledové řízení, komunikaci elektronických napájecích systémů a ochranu. Je využíván především v energetice. Stejně jako například protokol DNP3 je postaven na architektuře EPA[4]. Obrázek 1.1 zobrazuje model ISO/OSI a EPA. [8, 9]

Základním faktem k pochopení adresování podle IEC 60870-5 je rozdíl mezi řídicími a monitorovacími směry. Předpokládá se, že celkový systém má hierarchickou strukturu zahrnující centralizovanou kontrolu. Dle tohoto protokolu je každá stanice buď řídicí nebo kontrolovanou stanicí. [8, 10]

Při tomto způsobu komunikace, řídicí stanice odesílá požadavky všem svým podřízeným stanicím, kde každá podřízená jednotka reaguje individuálně. Postup dotazování může být přizpůsoben individuálním požadavkům systému. [10, 11]

[3] Power Line Communication

[4] Enhanced Performance Architecture



Obr. 1.1: Model ISO/OSI v porovnání s modelem EPA.

1.2.1 Normy IEC 60870

Normy IEC 60870 jsou u nás označovány jako ČSN EN 60870. Jedná se o označení celé skupiny norem nazvanou „Systémy a zařízení pro dálkové ovládání“. Tento soubor je rozdělen do 6 částí. [8, 11, 12]

- IEC 60870-1 (Všeobecné ustanovení)
- IEC 60870-2 (Provozní podmínky)
- IEC 60870-3 (Elektrické charakteristiky rozhraní)
- IEC 60870-4 (Požadavky na vlastnosti)
- IEC 60870-5 (Komunikační protokoly)
- IEC 60870-6 (Protokoly dálkového řízení)

První dvě se zabývají všeobecnými zásadami této normy. Třetí z nich pojednává o elektrických charakteristikách rozhraní. Další se zabývá požadavky na vlastnosti dálkového ovládání. Část IEC 60870-5 (Komunikační protokoly) se zabývá samotnými komunikačními protokoly. Ty specifikují funkce užitečné pro systémy dálkového ovládání, mezi které patří dvě nejdůležitější z nich Report By Exception a mechanismus přiřazování časových značek. [8, 11]

Poslední částí je IEC 60870-6, která definuje systémy používané pro dálkové ovládání v aplikacích elektrotechniky a automatizace energetických systémů. Byla vyvinuta, aby poskytla komunikační profily pro odesílání základních kontrolních zpráv mezi dvěma systémy, které jsou kompatibilní s normami ISO a doporučeními ITU-T. [8, 12]

Report by Exception

Tato funkcionalita umožňuje podřízeným stanicím požádat o komunikaci s řídicí stanicí. Podřízená stanice je schopna inicializovat komunikaci i bez dotázání, jinak by se o daných proměnných (většinou kritických pro systém) dozvěděla až v okamžiku, kdy by na danou podřízenou stanici došlo podle pravidelného dotazování. [8, 9]

Časové značky

Časové značky slouží ke zjištění času konkrétní události. Tato značka bývá automaticky připojena k dané zprávě. Tato zpráva zpravidla obsahuje informace o tom, kdy nastala daná událost a co bylo její příčinou, typicky ve formátu rok-týden-den a sekundy. Ovšem nejedná se o pravidlo a může se měnit dle dané implementace a potřeb. Pro správné fungování je nezbytné také udržovat přesnou časovou synchronizaci mezi řídicí a podřízenými stanicemi. [8, 10]

Formát CP56Time2a

Jedná se strukturovaný formát času, který je využíván protokolem IEC 60870-5 k vytváření časových razítek. Využíván je především sedmi bajtový formát, neboť tří bajtový formát není v protokolu IEC 60870-5-104 povolen. [8, 11]

1.2.2 Struktura zpráv

Protokol IEC 60870-5 je založen na redukovaném referenčním modelu EPA. Tento model obsahuje tři vrstvy modelu ISO/OSI, a to aplikační, linkovou a fyzickou vrstvu. Tabulka 1.1 ukazuje jednotlivé části normy IEC 60870-5 při dosazení do modelu EPA. [8, 10, 11]

Tab. 1.1: Normy IEC 60870-5 v modelu EPA.

Vybrané aplikační funkce podle IEC 60870-5-5	Uživatelský proces
Vybrané informační aplikační prvky podle IEC 60870-5-4	Aplikační vrstva
Vybrané datové jednotky aplikačních služeb podle IEC 60870-5-3	
Vybrané postupy přenosu podle IEC 60870-5-2	Linková vrstva
Vybrané formáty přenosových rámců podle IEC 60870-5-1	
Vybrané doporučení ITU-T	Fyzická vrstva

- Aplikační vrstva – definuje informační prvky pro strukturování aplikačních dat a funkce komunikačních služeb. Definuje celkovou strukturu zpráv, strukturu ASDU[5], informační prvky, adresování a směrování zpráv atd.

[5] Application-layer Service Data Unit

- Linková vrstva – určuje formáty rámců či bitové pořadí.
- Fyzická vrstva – definuje hardwarově závislé specifikace komunikačních rozhraní IEC 60870-5-101 a IEC 60870-5-104. Zahrnuje definici komunikačních rozhraní a konfigurace sítě.

1.2.3 Přenos dat

Protokol IEC 60870-5-101 poskytuje komunikační profil pro odesílání zpráv o dálkovém řízení mezi centrální řídicí stanicí a dálkově ovládanými stanicemi. Pro tyto účely využívá přímo propojené datové okruhy mezi centrální stanicí a jednotlivými výstupy. Tento protokol umožňuje dva způsoby přenosu komunikace, a to na vyvážený a nevyvážený. Protokol IEC 60870-5-104 kombinuje aplikační vrstvu IEC 60870-5-101 a přenosové funkce poskytované protokolem TCP/IP[6]. [8, 10]

1. Balanced (Vyvážený přenos) – V tomto režimu může každá stanice iniciovat přenos zpráv. Stanice mohou pracovat současně v řídícím a řízeném stavu. Vyvážený přenos je omezen na konfiguraci bodového přenosu point-to-point a vícebodového přenosu multiple point-to-point. [8, 10]
2. Unbalanced (Nevyvážený přenos) – V tomto režimu řídicí stanice řídí datovou komunikaci postupným dotazováním. Zahajuje veškeré přenosy zpráv, zatímco řízené stanice mohou pouze reagovat na tyto zprávy. Využíván je převážně pro globální, cyklické, ovládací příkazy či příkazy nastavení. [8, 10]

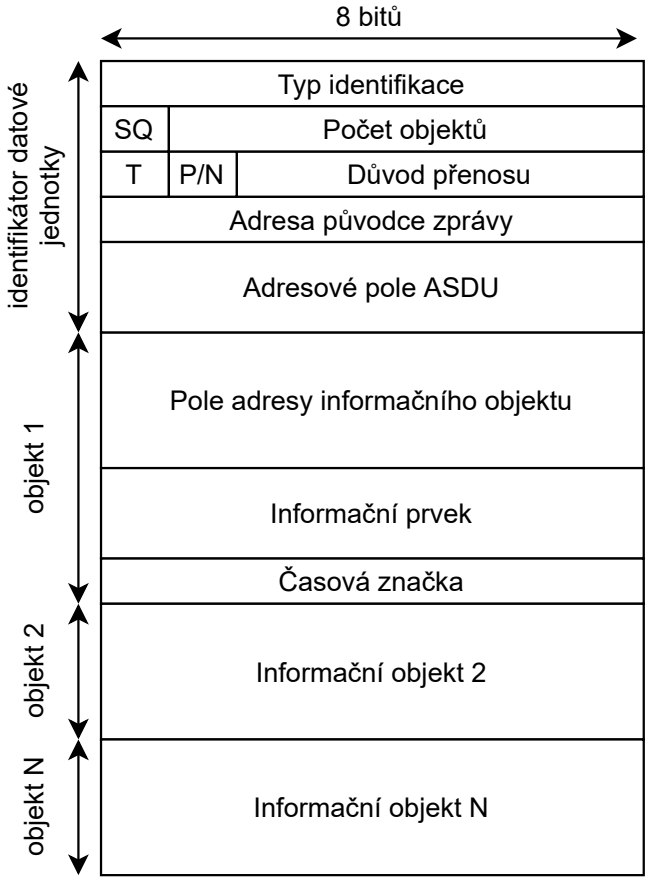
1.2.4 Datový objekt

Norma IEC 60870-5 obsahuje informace o sadě informačních objektů, které vyhovují jak obecným aplikacím SCADA, tak zejména aplikacím energetických rozvodných systémů. Uvnitř ASDU jednotek jsou přenášena aplikační data v rámci jednoho nebo více informačních objektů viz obr. 1.2. [8, 9, 13]

Každá datová jednotka má jedinečné typově identifikační číslo. V každé jednotce ASDU je zahrnut pouze jeden datový typ nacházející se v prvním poli ASDU jednotky. Typy informačních objektů jsou normou definovány a seskupeny podle směru, a to na směr monitorování či řízení, a podle typu informací, které přenáší. Mezi ně patří informace o procesu, informace o systému, parametry přenosu souborů. Kompletní výpis všech typově identifikačních čísel jsou uvedeny v příloze E. [8, 12, 13]

Dále pak můžeme jednotlivé zprávy dělit podle samotného důvodu, který způsobil poslání dané zprávy neboli COT[7]. Toto značení je určeno ke zlepšení transparentnosti při zpracovávání přijatých zpráv. Všechny typy COT a jejich významy jsou uvedeny v příloze F. [8, 12, 13]

[6] Transmission Control Protocol/Internet Protocol
[7] Cause Of Transmission



Obr. 1.2: Struktura ASDU jednotky.

Další položkou v záhlaví ASDU zprávy je sekvenční číslo SQ[8], které určuje pořadí přijatých zpráv, adresu původce zprávy OA[9] či informační prvek, který je základním prvkem a slouží k přenosu informací. [8, 12, 13]

1.2.5 IEC 60870 TLS spojení

Komunikační protokol TLS[10] podle normy IEC 608070-5-7 kapitoly 9 lze použít tak, aby umožňoval bezpečnou komunikaci se zařízením na bázi protokolu IEC 60870-5-104. Pro šifrování lze použít kryptografii veřejného klíče nebo asymetrické šifrování. Proto potřebuje každý účastník tohoto systému (klient/server), certifikát a soukromý klíč. Podporovaný protokol v IEC 60870-5-104 s použitím TLS je založen na certifikátech X.509. [8, 11, 14]

- Režim serveru – Pokud má být zařízení provozováno jako server, musí být definován zabezpečený port serveru (tlsServerPort). Tento port je ve výchozím

[8]Sequence Number
[9]Originator Adress
[10]Transport Layout Security

nastavení 0, což znamená, že režim serveru je deaktivován a žádný klient se nemůže připojit. Dále můžeme definovat port serveru (tcpServerPort) pro nezabezpečená připojení. Nastavení nenulového čísla pro tlsServerPort a tcpServerPort umožňuje paralelně zabezpečené a nezabezpečené spojení. [11, 14]

- Klientský režim – Pro každé spojení, které zařízení vytvoří jako klient k jinému serveru, existuje interní datový bod (_IecConnection). Prvek datového bodu (_IecConnection.Config.Flags) definuje, zda musí být připojení šifrováno. Pokud je aktivováno šifrování, klient naváže spojení TLS a odpovídajícím způsobem zašifruje veškerou komunikaci IEC 60870. [11, 14]

Certifikát X.509

V kryptografii je X.509 standard definující formát certifikátů veřejného klíče. Certifikáty X.509 se používají v mnoha internetových protokolech, včetně TLS/SSL[11], což je základ pro HTTPS[12], bezpečný protokol pro procházení webu. Používají se také při vytváření elektronických podpisů. Certifikát X.509 obsahuje veřejný klíč a identitu (název hostitele, organizace nebo jednotlivce) a je podepsán certifikační autoritou, nebo sám sebou. [8, 14, 15]

Poté, co je certifikát podepsán důvěryhodnou certifikační autoritou, nebo ověřen jinými prostředky, se může tento držitel certifikátu spolehnout na obsažený veřejný klíč při navazování zabezpečené komunikace s jinou stranou nebo k ověřování dokumentů digitálně podepsaných odpovídajícím soukromým klíčem. [8, 14, 15]

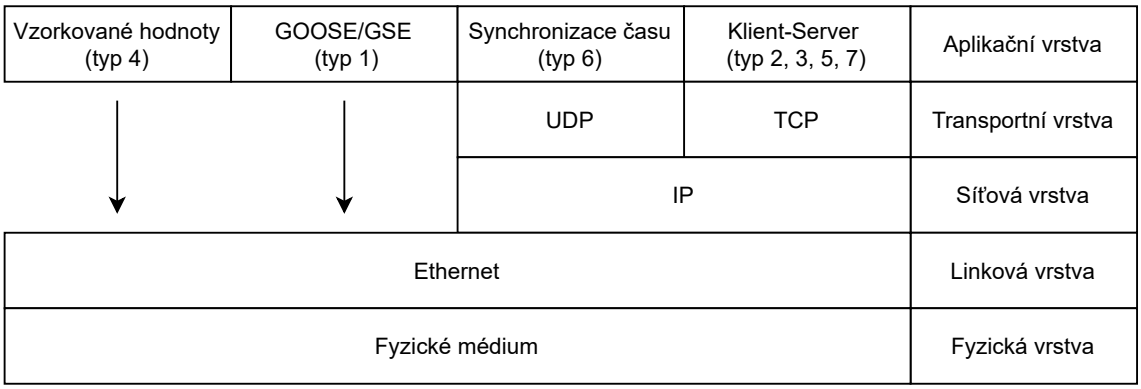
Tento standard také definuje revokační seznamy certifikátů, které jsou prostředkem k distribuci informací o certifikátech, které byly podepisujícím orgánem považovány za neplatné stejně jako algoritmus ověření cesty certifikace, který umožňuje podepisování certifikátů zprostředkovanými certifikáty CA[13], které jsou zase podepsány jinými certifikáty. [8, 14, 15]

1.3 IEC 61850

Standard IEC 61850, který je u nás definován normami ČSN EN 61850, byl zaveden, aby sjednotil komunikační standardy v energetice, neboť zde existuje mnoho vzájemně nekompatibilních protokolů. Během vývoje standardu byl kladen zvlášť důraz na spolehlivost a stabilitu. Je tvořen několika normami, které jsou zaměřeny na samotnou terminologii, řízení, komunikaci, či samotnými zkouškami a shodami zařízení použitých v automatických rozvodnách. Dále stanovuje požadavky, které

[11] Secure Sockets Layer
[12] Hypertext Transfer Protocol
[13] Certification Authority

jsou na rozvodny a jejich zařízení z hlediska komunikace kladeny. Jde tedy o standardizovaný datový model, který využívá všechny vrstvy referenčního modelu ISO/OSI viz obr. 1.3. [16, 17, 18]



Obr. 1.3: Porovnání TCP/IP a IEC 61850.

Jedná se o standard, který splňuje všechny nároky a požadavky pro energetiku a společnosti zaměřené na dálkové řízení po celém světě. Dle standardu je každý uzel připojen jako řídicí zařízení, a tak může řídit provoz sítě a komunikovat se všemi podřízenými stanicemi. Podobně jako standard IEC 60870 komunikuje na principu žádost–odpověď. Také je zde implementována funkce nevyžádaných zpráv, ovšem standard definuje i další typy zpráv, aby umožnil klientským stanicím řídit přenos dat. [16, 18, 19]

Normy standardu IEC 61850

Soubor norem je rozdělen do 10 částí. [16, 18, 19]

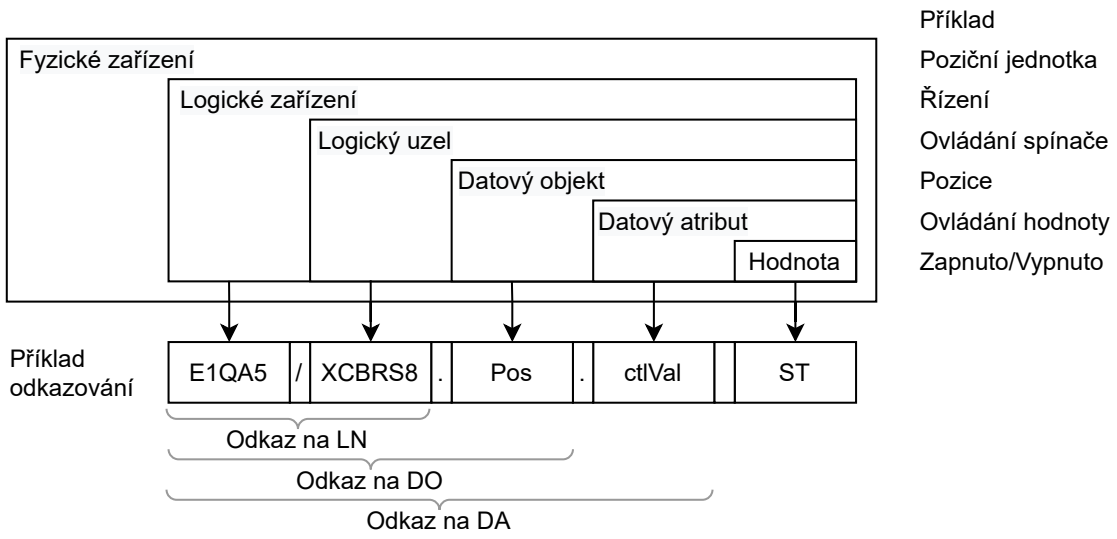
- IEC 61850-1 – Úvod a přehled
- IEC 61850-2 – Výklad zvláštních výrazů
- IEC 61850-3 – Všeobecné požadavky
- IEC 61850-4 – Systémové a projektové řízení
- IEC 61850-5 – Požadavky na komunikaci pro funkce a modely zařízení
- IEC 61850-6 – Konfigurační jazyk pro komunikaci v elektrických stanicích
- IEC 61850-7 – Komunikační struktura pro rozvodná a napájecí zařízení
  1. část: Zásady a modely
  2. část: Abstraktní rozhraní pro komunikační služby (ACSI[14])
  3. část: Obecné třídy dat
  4. část: Třídy kompatibilních logických uzlů a třídy dat
- IEC 61850-8 – Mapování specifických komunikačních služeb (SCSM[15])

[14] Abstract Communications Service Interface
[15] System Center Service Manager

1. část: Mapování na MMS[16] a na ISO/IEC 8802-3
- IEC 61850-9 – Mapování specifických komunikačních služeb (SCSM)
  1. část: Přenos vzorkovaných hodnot po sériovém jednosměrném vícebodovém spoji bod-bod
  2. část: Vzorkované hodnoty
- IEC 61850-10 – Zkoušky shody

1.3.1 Datový model IEC 61850

Data v terminálech jsou organizována podle objektově orientovaného přístupu. Pro vzájemnou kompatibilitu mezi zařízeními od různých výrobců musí být objekty jasně definovány. Fyzické zařízení (PD nebo také IED[17]) obsahuje různé funkční moduly, které jsou modelovány jako logická zařízení (LD). Každé logické zařízení může poskytovat různé operace definované jako logické uzly (LN). Logické uzly obsahují datové objekty (DO), které představují služby aplikace. Proměnné logických uzlů jsou reprezentovány jako běžné datové třídy (CDC). Norma IEC 61850-7-3 definuje 40 různých CDC. Každý datový objekt obsahuje sadu základních datových atributů (DA), které spadají do 12 kategorií funkčního omezení (FC). Atributy obsahují hodnoty definované pomocí běžných datových atributů (CDA). Struktura informačního modelu standardu IEC 61850 je zobrazena na obr. 1.4 včetně znázorněného způsobu odkazování se na jednotlivé prvky. [16, 17]



Obr. 1.4: Datový model IEC 61850.

[16]Multimedia Messaging Service
[17]Intelligent Electronic Devices

Fyzické zařízení

Fyzické zařízení představuje terminál (např. relé či rozvodnu), který je definovaný jedinečnou IP adresou. Fyzické zařízení je identifikováno unikátním názvem, maximálně však 10 znaků dlouhým. [16, 17]

Logické zařízení

Logické zařízení je podskupina fyzických zařízení. V rámci jednoho fyzického zařízení jich může být definováno několik. Každé logické zařízení obsahuje následující atributy:

- Název logického zařízení (LDName) – Jednoznačně definuje logické zařízení v síti.
- Seznam logických uzlů (LogicalNode[1...n]) – Seznam všech logických uzlů, které jsou součástí logického zařízení.
- Službu vracející seznam objektů (GetLogicalDeviceDirectory) – Vrací seznam všech logických uzlů, ke kterým má klient přístup.

Každé logické zařízení obsahuje jeden nebo více logických uzlů. [16, 17]

Logický uzel

Logický uzel je virtuální reprezentace zařízení. Jedná se o seskupení dat a služeb souvisejících s určitou funkcí zařízení (např. rozvodny). Všechna data generovaná zařízením lze proto přiřadit určitému logickému uzlu. Ve standardu IEC 61850 je logický uzel definován jako nejmenší entita pro výměnu dat. Představují tedy logické znázornění konkrétních prvků (např. vypínač, odpojovač, přepínač atd.). Logické uzly jsou kombinovány do skupin na základě funkčnosti. Existují logické uzly pro automatické řízení, pro měření a správu, dohledovou kontrolu atd. Norma IEC 61850-7-4 definuje 159 jedinečných tříd logických uzlů. [16, 17]

Datový objekt

Logický uzel obsahuje datové objekty, které představují objekty aplikace (rozvodny). Každý datový objekt má jedinečný název. Tyto názvy jsou určeny standardem a jsou funkčně související s účelem energetické soustavy. Soubor datových objektů souvisejících s daným logickým uzlem je definován normou IEC 61850-7-3. Jak již bylo zmíněno, standard popisuje 40 běžných datových tříd (CDC), které přiřazují kolekci datových objektů konkrétní třídě. Datový objekt je tedy základním stavebním kamenem datového modelu standardu IEC 61850. [16, 17]

Datový atribut

Jedná se o nejmenší část datového modelu a může reprezentovat logické stavy vypínačů, přepínačů, parametrů atd. Tyto atributy spadají do 12 kategorií funkčního omezení. Jedná se o vlastnost datového atributu, která charakterizuje konkrétní použití atributu. Označuje služby použitelné pro konkrétní datový atribut. Z aplikačního hlediska jsou datové atributy klasifikovány podle jejich konkrétního použití. Některé atributy se používají pro řízení, jiné pro hlášení a protokolování, nebo pro skupiny měření či nastavování, nebo pro popis konkrétních datových atributů. Funkční omezení slouží jako datový filtr ve smyslu definování služeb použitelných pro specifické datové atributy běžných datových tříd definovaných v IEC 61850-7-3. [16, 17]

1.3.2 IEC 61850-80-1

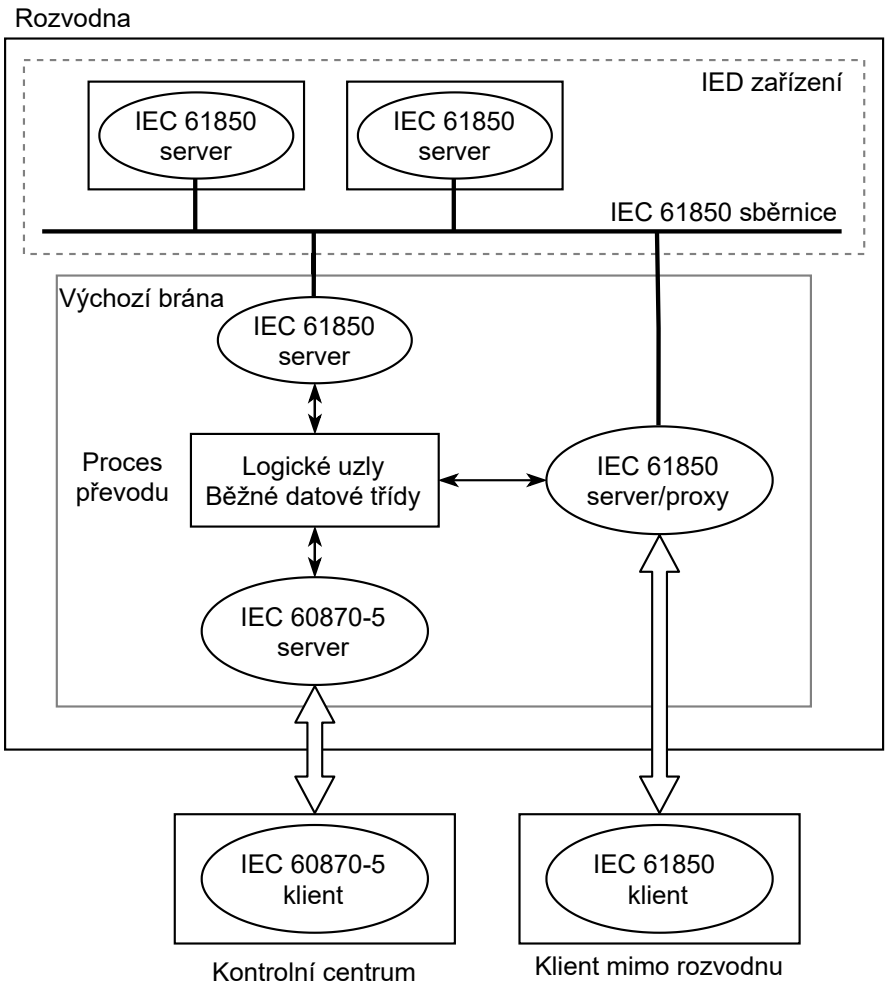
Jedná se o normu, která rozšiřuje původní standard IEC 61850 za účelem zlepšení propojitelnosti s ostatními standardy. Směrnice poskytuje pokyny, jak vyměňovat informace z datového modelu založeného na CDC[18] (např. IEC 61850) pomocí IEC 60870-5-101, nebo IEC 60870-5-104 mezi rozvodnou a řídicím centrem. [16, 19, 20]

Specifikace se zaměřuje hlavně na definování pravidel a funkcí zařízení brány jako součásti rozvodny. Pravidla a funkce jsou však platné také v případě připojení zařízení IED přímo k WAN[19] síti kompatibilní s IEC 60870-5-101, nebo IEC 60870-5-104, a proto musí být mapování provedeno uvnitř IED. Cílem této normy je popsat standardizované mapování datových modelů orientovaných na zařízení s již definovanými atributy CDC, službami na již definované ASDU (například IEC 61850-7) a službami IEC 60870-5-104 nebo IEC 60870-5-101. [8, 16, 20]

Příklad možné architektury hraničního zařízení je zobrazen na obr. 1.5. Schéma popisuje koncepční architekturu zařízení brány v rozvodně. Zařízení brány odděluje sběrnici stanic IEC 61850 od protokolu IEC 60870-5-101/104 prostřednictvím procesu převodu. Výhodou tohoto přístupu je, že není potřeba mapovat pouze služby pro interakci s řídícím modelem. Proces převodu je organizován podle datového modelu IEC 61850 (LD, LN, CDC viz kapitola 1.3.1). [8, 16, 20]

[18] Change Data Capture – Přístup k integraci dat, který je založen na identifikaci, zachycení a doručení změn provedených ve podnikovém zdroji dat.

[19] Wide Area Network – Počítačová síť pokrývající rozlehlé geografické území.



Obr. 1.5: Koncepční schéma hraničního zařízení.

Mapování informačního modelu zařízení IEC 61850 do IEC 60870-5

Mapování mezi informačním modelem založeném na standardu IEC 61850 využívá existující funkcionality protokolu IEC 60870-5-101/104, a to konkrétně obecnou adresu ASDU (CASDU[20]) a adresu informačního objektu (IOA). Tyto funkcionality jsou využity k přizpůsobení zařízení využívající LD, LN a přenos informací (dat) v reálném čase pomocí standardizovaných ASDU zpráv. Totéž platí pro služby a základní aplikační funkce. [16, 20]

Odkaz na logické zařízení (LD) je mapováno na adresu CASDU, ta může být jak strukturovaná, tak i nestrukturovaná. Např. CASDU může identifikovat ID stanice a ID instance logického zařízení. Doporučuje se ovšem vytvořit schéma adresování tak, aby konkrétní stanice měla jedinečnou adresu. Maximální počet CASDU pro jeden odkaz je 65 534. [20]

[20]Common adress of ASDU

Identifikátor instance logického uzlu (LN) a odkaz na datový atribut se mapují na adresu informačního objektu (IOA). Všechny atributy třídy LN jsou implicitně definované a viditelné. IOA může být strukturované nebo nestrukturované. V obou případech se pro definování adres IOA doporučuje desítkový přístup, kde maximální počet adres IOA na CASDU je 65 536. [20]

Mapování běžných datových tříd

Každá běžná datová třída (CDC) se skládá z jednoho nebo více atributů dat konkrétního datového typu. Každý atribut dat musí být namapován na jednu konkrétní IOA. V protokolech IEC 60870-5-101/104 je každý IOA přímo spojen s konkrétním typem ASDU (s časem nebo bez času). Požadavky mapování LD/LN na CASDU/IOA se mohou lišit v různých oblastech použití. Nejvhodnější způsob definice mapování je na základě užitku v závislosti na konkrétních potřebách. [8, 20]

Mapování zobrazené v příloze G bylo definováno normou IEC 61850-80-1 jako výchozí mapování z různých možností mapování. Tato příloha obsahuje všechny typy CDC definované normou IEC 61850-7-3:2010 a IEC 61400-25-2, ovšem některé typy není možné přímo namapovat na konkrétní typ ASDU (jako např. zprávy typu VSS, ORG, či TSG). [8, 16, 20]

1.4 Porovnání IEC 60870 a IEC 61850

Oba standardy stojí na osvědčených řešeních a poskytují alespoň základní úroveň (first level) interoperability získávání dat, ovšem standard IEC 61850 poskytuje i aplikační úroveň interoperability. Dále také oba poskytují informace v reálném čase s tím, že IEC 61850 poskytuje výměnu informací v reálném čase pro vzorkované hodnoty včetně vypínacích příkazů. [8, 16, 21]

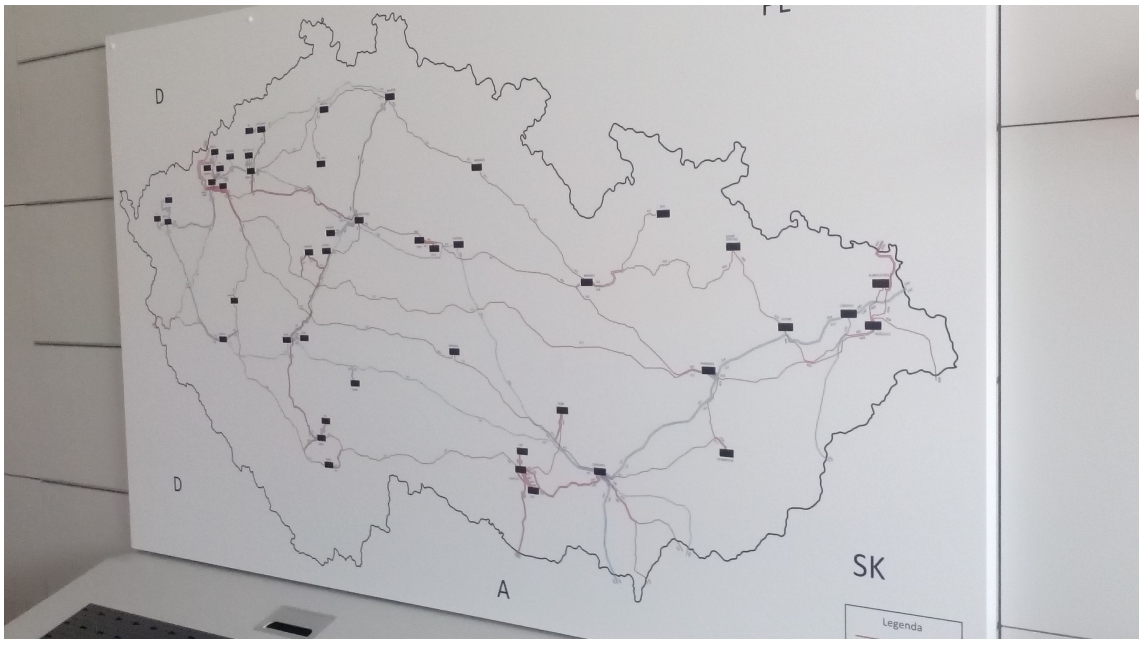
Standard IEC 60870 se svými funkcionalitami blíží spíše staršímu standardu DNP3, zatímco standard IEC 61850 má potenciál být využit jako integrované řešení správy informací téměř ve všech odvětvích užitkových aplikací (energetika, rozvodné sítě, rozvod plynu či vody), které uživateli poskytuje konzistentní a okamžitou znalost systému. Oproti IEC 60870 staví na datovém modelování, konfiguračních službách a pokročilých komunikačních modelech. Dále také poskytuje komplexní jazyk konfigurace systému, který je klíčovou součástí tohoto standardu. [8, 16, 21]

2 Polygon přenosové soustavy ČR

Pojem polygon představuje obecné označení soustavy simulující konkrétní prostředí a jeho chování. Takovýto polygon je následně využíván pro zaškolování nových zaměstnanců či testování nových zařízení bez nutnosti narušení stability reálné rozvodné sítě.

Na ústavu telekomunikací byl realizován polygon PS ČR (viz obr. 2.1) pro výukové, simulační a testovací účely. Polygon simuluje reálný datový provoz mezi jednotlivými stanicemi a dohledovým střediskem. Data přenášená v těchto zprávách obsahují informace o aktuálně generovaných velikostech napětí, proudu, teplotě či stavy jednotlivých ochranných zařízení.

Polygon je složen ze 47 zařízení Raspberry Pi a čtyř rozbočovačů od firmy MikroTik. Každé zařízení Raspberry Pi představuje hraniční komunikační bránu jedné elektrárny, či rozvodny. Jedná se tedy o SAS[1] jednotku komunikující s řídícím SCADA systémem reprezentovaným open-source softwarem OpenMUC[2]. Výčet všech použitých elektráren a rozvoden spadajících do PS ČR je obsažen v příloze D. [22]



Obr. 2.1: Polygon energetické přenosové soustavy.

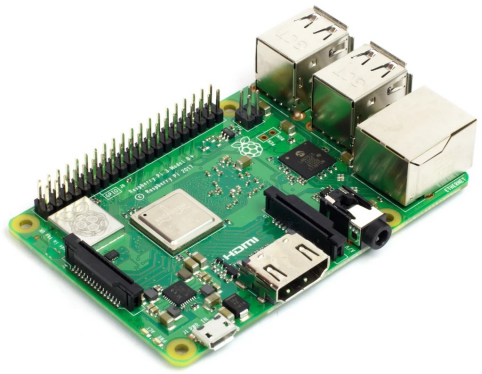
Raspberry Pi

Raspberry Pi označuje malý jednodeskový počítač s deskou plošných spojů viz obr. 2.2. K provozu je používán primárně operační systém Raspbian. Tento jed-

[1] Substation Automation System

[2] Java framework pro práci se SCADA systémy, dostupný na https://www.openmuc.org.

nodeskový počítač byl vyvinut nadací Raspberry Pi Foundation s cílem podpořit výuku informatiky. Cena tohoto zařízení se aktuálně pohybuje kolem 1 000 Kč. Nejnovějším modelem z řady Raspberry Pi je model Raspberry Pi 4 model B. [23, 24]



Obr. 2.2: Raspberry Pi 3 Model B+.

Pro realizaci polygonu energetické PS bylo zvoleno zařízení Rapsberry Pi 3 model B+. Tabulka 2.1 zobrazuje výčet základních parametrů tohoto modelu. [24]

Tab. 2.1: Parametry zařízení Raspberry Pi 3 B+.

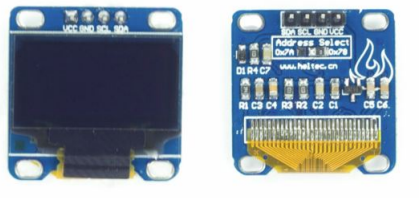
Model procesoru	Broadcom BCM2837
Počet jader	4
Frekvence	1400 MHz
Velikost operační paměti	1000 MB
GPU	Broadcom VideoCore IV @ 400 MHz / 300 MHz
Počet USB portů	4
HDMI	Ano
DSI	Ano
Wi-Fi	Ano
Ethernet	Ano
Bluetooth	Ano
Úložiště	microSD slot
Adresní prostor	64 bitů
Architektura	ARMv8
Jádro	Cortex-A53

Kromě základního síťového portu obsahuje také každé zařízení Raspberry Pi USB[3] adaptér, který vytváří druhý síťový port, aby bylo možné oddělit komunikaci datovou a servisní. Za účelem vizuální zpětné vazby generovaných dat je ke každému zařízení Raspberry Pi připojen zobrazovací displej IIC I2C OLED.

[3]Universal Serial Bus

IIC I2C OLED displej

Pro realizaci polygonu energetické PS byl zvolen displej IIC I2C OLED display 0,96"128x64 viz obr. 2.3.



Obr. 2.3: Informační displej IIC I2C OLED.

Toto zařízení používá zobrazovací technologii OLED[4]. Oproti klasickému LCD[5] displeji disponuje vyšším kontrastem zobrazení při stejném výkonu. Dále také tato technologie dovoluje tenčí provedení celého zařízení. Tabulka 2.2 zobrazuje základní parametry tohoto displeje. [25]

Tab. 2.2: Parametry displeje IIC I2C OLED.

Sběrnice	IIC I2C
Úhlopříčka	0,96"
Rozlišení displeje	128 x 64 px
Příkon	40 mW
Napájení	3,3–5 V DC
Rozměry	27 x 27 x 4,1 mm
Řadič	SSD1306

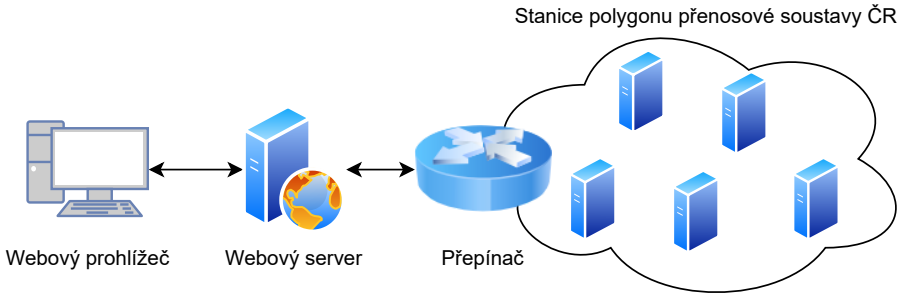
2.1 Správa polygonu

Pro řízení polygonu PS byla vytvořena webová aplikace (viz kapitola 2.3), která pomocí webového serveru komunikuje se stanicemi emulujícími rozvodny a elektrárny. Základní schéma ovládání polygonu je zobrazeno na obr. 2.4. Úplné zapojení polygonu přenosové soustavy bude zobrazeno a popsáno v kapitole 3.

Správa tohoto polygonu je vytvořen obdobným způsobem jako samotné dálkové řízení, a to na modelu klient–server. Spojení mezi webovým serverem a stanicemi polygonu je realizováno pomocí SSH[6]. Detailnější popis komunikace viz kapitola 3.1.

[4]Organic Light Emitting Diode
[5]Liquid Crystal Display
[6]Secure Shell

Polygon je složen ze dvou navzájem oddělených sítí. Dosáhneme tak efektu, kdy můžeme komunikovat, popřípadě měnit určité parametry jednotlivých stanic, bez přímého zásahu do datové komunikace. Kupříkladu při simulaci útoku nepřijde cvičená osoba do kontaktu s jiným provozem než s datovou komunikací protokolu IEC 60870-5-104. Obdobně je tomu v případě DDoS[7] útoku s tím rozdílem, že datová síť může být zahlcena, ovšem síť servisní nebude ovlivněna a nedojde k odepření přístupu.



Obr. 2.4: Schéma zapojení ovládacího a kontrolního rozhraní.

2.2 Emulace stanic

Jak již bylo naznačeno v kapitole 2, polygon přenosové soustavy je tvořen 47 zařízeními Raspberry Pi. Každé zařízení emuluje elektrárnu/rozvodnu pomocí programu simulující komunikaci reálných stanic energetické soustavy.

Celý kód je součástí knihovny *lib60870-2.2.0*[8], která obsahuje všechny základní funkce pro práci s komunikačním protokolem IEC 60870-5-104, včetně funkcí pro navazování TCP spojení. Všechny funkce jsou popsány v příloze H, a to v chronologickém pořadí jejich výskytu v kódu. [26, 27]

Stanice přijímají příkazy/dotazy od nadřazené stanice a odesílají na ně odpovědi. Dále pak zastávají funkci simulátorů dat, které data posílají na klientskou stanici k dalšímu zpracování. V případě klidového stavu, kdy tyto stanice nepodléhají žádným nežádoucím vlivům, simulují data dle tabulky 2.3.

Tab. 2.3: Simulovaná data stanicí polygonu.

Typ dat	Počet	Rozsah IOA	Význam dat
36	12	1000–1011	Data představující vstupní hodnoty transformátoru.
36	12	2000–2011	Data představující vstupní hodnoty transformátoru.
36	5	3000–3004	Data teplot transformátoru a frekvence.
4	5	4000–4004	Dvoubitové informace — stavy ochranných prvků.
2	5	5000–5005	Jednobitové informace — události.

[7]Distributed Denial of Service – Útok na odepření přístupu k síťovým službám.
[8]Dostupná na stránkách – `https://www.mz-automation.de/`

Pro lepší orientaci je v tabulce 2.4 detailní rozpis jednotlivých dat a jejich informačních objektů. Tyto data jsou simulovány pomocí implementované funkce v rozsahu stanoveném konfiguračním souborem odpovídajícím standardním rozsahům reálných stanic (viz kapitola 2.4.1), kromě hodnot HT[9] a LT[10], které jsou konstantní. Hodnoty činného a jalového výkonu jsou oproti ostatním hodnotám dopočítávány.

Tab. 2.4: Simulovaná data stanicí polygonu včetně jejich IOA.

Vstup		Výstup	
U_a	1000	U_a	2000
U_b	1004	U_b	2004
U_c	1008	U_c	2008
I_a	1001	I_a	2001
I_b	1005	I_b	2005
I_c	1009	I_c	2009
P_a	1002	P_a	2002
P_b	1006	P_b	2006
P_c	1010	P_c	2010
Q_a	1003	Q_a	2003
Q_b	1007	Q_b	2007
Q_c	1011	Q_c	2011
Teplota			
HT	3002	LT	3001
Okolní teplota	3003	Teplota trafa	3000
Frekvence		3004	
Ochranné prvky			
Hlavní jistič		4000	
Odpojovač		4001	
Události			
Změna hlavního jističe		5000	
Změna odpojovače		5001	
Změna ochranného relé		5002	
Spuštění alarmu		5003	
Chyba přepínacího příkazu		5004	
Poplach			
Přepětí		4002	
Podpětí		4003	
Zkrat		4004	

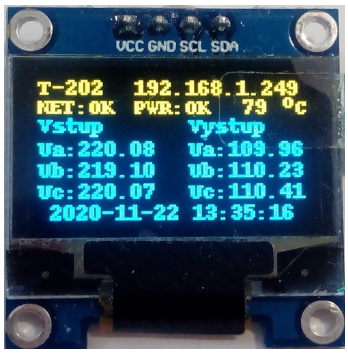
[9]High Temperature – Maximální povolená hodnota teploty okolí.
[10]Low Temperature – Minimální povolená hodnota teploty okolí.

Informační displej ovšem efektivně nezobrazí velké množství dat, a tak byla zvolena pouze nejdůležitější data (teplota, vstupní a výstupní napětí jednoho transformátoru), viz tabulka 2.5.

Tab. 2.5: Zobrazovaná data na informačním displeji.

Teplota trafa		3000	
Vstup		Výstup	
U_a	1000	U_a	2000
U_b	1004	U_b	2004
U_c	1008	U_c	2008

Na obrázku 2.5 můžeme vidět reálnou ukázku zobrazení informačním displejem. V rámci rozvodné stanice může existovat více než jedna instance simulující transformátor, proto je tento displej naprogramován k periodickému přepínání mezi daty jednotlivých instancí. Kromě již zmíněných dat se zde nachází informace o IP adrese zařízení, jejím aktuálním zobrazovaném trafu, stavu sítě (NET), stavu generování hodnot odpovídající klidovému stavu (PWR) a aktuálním času.



Obr. 2.5: Základní zobrazení dat displejem IIC I2C OLED.

V případě, kdy je vyvolána určitá událost buď lokálně, či vzdáleně, jsou posílány kromě periodických dat i data spontánní. Přesněji jsou odesílána data objektů, kterých se daná změna stavu týká (např. při odpojení hlavního jističe je odeslána spontánní zpráva o stavu a změně jističe, tedy objekty 4000 a 5000, viz kapitole 3.2).

Pro účely zpětného testování a analýzy dat je zde přítomen i logovací systém. Jedná se o záznam obecných informací spojených s vytvořením stanice, či její spojení *EventLog.txt* a o dva textové soubory pro jednotlivou vytvořenou instanci. Tyto logovací soubory jsou rozděleny na soubor s daty přijatými a odeslanými, dále pak číslem portu, na kterém tato komunikace probíhá. Struktura názvu logovacích souborů je vytvořena následně:

Log[TX/RX][číslo portu].txt,

tedy logovací soubor odeslaných dat komunikujících na portu 2404 bude vypadat následovně: *LogTX2404.txt*.

Jedním z hlavních konfiguračních souborů je *ServerStatus.txt*, který je při spuštění vygenerován na rozdíl od ostatních konfiguračních souborů. Slouží pro lokální ovládání chování jednotlivých instancí stanice. Při inicializaci tohoto souboru se do tohoto souboru vygenerují aktuální čísla používaných portů a k nim odpovídající stavy. V základním nastavení jsou všechny stavy nastaveny na hodnotu 1. Chování jednotlivých instancí stanice je pak odvozeno z následující tabulky 2.6.

Tab. 2.6: Možné stavy chování instancí stanice.

Stav	Význam	Popis
0	Podpětí	Zaslání spontánní zprávy o podpětí, změně hlavního jističe, stavu hlavního jističe a spuštění alarmu.
1	Normální stav	Normální běh programu, zasílání periodických dat.
2	Přepětí	Zaslání spontánní zprávy o přepětí, změně hlavního jističe, stavu hlavního jističe a spuštění alarmu.
3	Zkrat	Zaslání spontánní zprávy o zkratu, změně odpojovače, stavu odpojovače a spuštění alarmu.
4	Vypnutí hlavního jističe	Zaslání spontánní zprávy změně hlavního jističe a stavu hlavního jističe.
5	Vypnutí odpojovače	Zaslání spontánní zprávy změně odpojovače a stavu odpojovače.

Spuštění stanice polygonu

Pro spuštění jedné stanice je vytvořen speciální spouštěcí skript *LauncherS.py* napsaný v jazyce python. Spouštěcí skript je složen ze čtyř fází. V první fázi vytváří pomocné matice pro následný zápis na displej, dále pak inicializuje soubor *ServerStatus.txt* a následně spouští instance stanice. Nakonec je poslán příkaz k samotnému zobrazení dat na displeji. Poté již v nekonečné smyčce kontroluje, zda běží všechny vytvořené instance stanice a v případě, kdy nějaká instance neběží, ji opět spustí. Tento skript používá jeden spouštěcí parametr, a to počet instancí:

python LauncherS.py [počet instancí],

tedy pro spuštění stanice ve třech instancích zadáme příkaz *python LauncherS.py 3*. V případě, kdy chceme spustit pouze jednu instanci můžeme zadat následující příkaz:

./cs104_server [IP] [port],

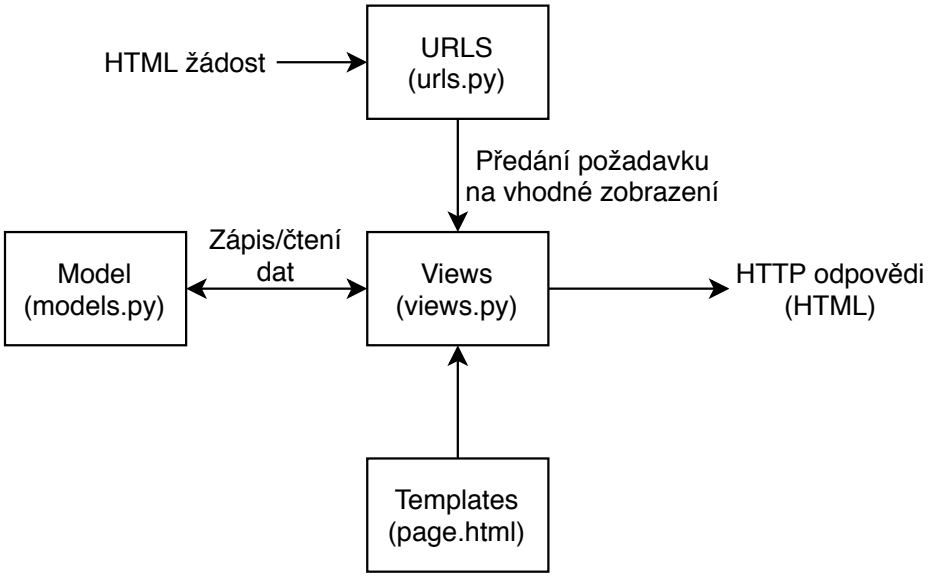
tento skript přijímá dva parametry, a to IP adresu daného zařízení a komunikační port. Tedy pro spuštění serveru na IP adrese 10.0.2.3 a portu 2405 zadáme *./cs104_server 10.0.2.3 2405*. Pro zapnutí zobrazovacího displeje provedeme příkaz:

python TXmatrix.py [počet instancí],

ovšem musí zde být i odpovídající počet pomocných souborů *TXmatrix[port].txt*, ze kterých tento displej získává potřebná data. Tedy pro spuštění displeje ve čtyřech instancích zadáme příkaz *python TXmatrix.py 4*.

2.3 Ovládací rozhraní

Za účelem managementu polygonu přenosové soustavy ČR vznikla aplikace běžící na webovém serveru. Základem aplikace je open-source webový framework Django[11]. Charakteristickým rysem je architektura „Model–view–controller“. Jde o softwarovou architekturu, která rozděluje datový model aplikace, uživatelské rozhraní a řídicí logiku do tří nezávislých komponent tak, že modifikace některé z nich má jen minimální vliv na ostatní. Schéma „Model–view–controller“ je zobrazeno na obr. 2.6.

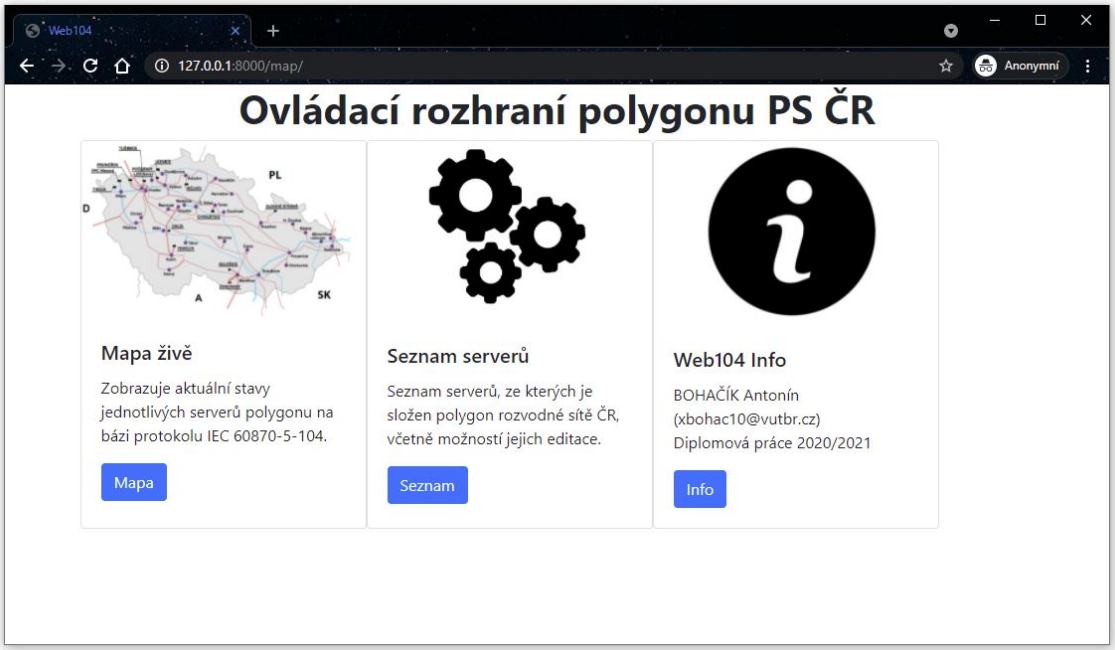


Obr. 2.6: Schéma model–view–controller.

Webová aplikace byla vybrána především kvůli možnosti ovládání nezávislém na daném hardwaru (cross-platform). Jedinou podmínkou je nainstalovaný webový prohlížeč a spuštěný webový server (viz kapitola 2.3.2). Polygon je tedy možné ovládat

[11]Stránky Django – `https://www.djangoproject.com/`

jak z osobního počítače s operačním systémem Linux či Windows, tak i z mobilního zařízení s operačním systémem Android či iOS. Webová aplikace byla implementována pomocí programovacího prostředí Visual Studio Code[12]. Ukázka webového rozhraní je zobrazena na obr. 2.7.



Obr. 2.7: Webové ovládací rozhraní PS ČR.

2.3.1 Struktura webové aplikace

Webová aplikace je tvořena čtyřmi webovými stránkami, a to úvodní stránkou, stránkou zobrazující stavy jednotlivých stanic polygonu v reálném čase „Mapa živě“. Dále je přítomna webová stránka „Seznam serverů“ obsahující tabulkou veškerých serverových stanic včetně nezbytných funkcí k samotnému ovládání a nakonec i stránku s informacemi o webu „Web104 info“.

Úvodní stránka

Stránka obsahuje karty (resp. odkazy) ostatních stránek vytvořené webové aplikace. Byla navržena s ohledem na budoucí vývoj a snadné přidávání dalších modulů, popřípadě celých aplikací. Ukázka úvodní stránky již byla zobrazena na obr. 2.7. Ukázka kódu pro vytvoření jedné karty je zobrazena ve výpisu 2.1.

[12]Stránky VSCode – `https://code.visualstudio.com/`

Výpis 2.1: Soubor *homepage.hmtl* pro vytvoření karty.

```
#DEFINOVÁNÍ KARTY
<div class="card" style="width: 18rem;">
#VLOŽENÍ NÁHLEDOVÉHO OBRÁZKU DO KARTY
 <img class="card-img-top" src="{%static "/media/mapa.png"%}"
 alt="Live Map">
#TĚLO KARTY
 <div class="card-body">
  <h5 class="card-title">Mapa živě</h5>
  <p class="card-text">Zobrazuje... ...IEC 60870-5-104.</p>
#VYTVOŘENÍ TLAČÍTKA S ODKAZEM NA DANOU STRÁNKU
  <a href="{%url "url_map"%}" class="btn btn-primary">
  Mapa</a>
 </div>
</div>
```

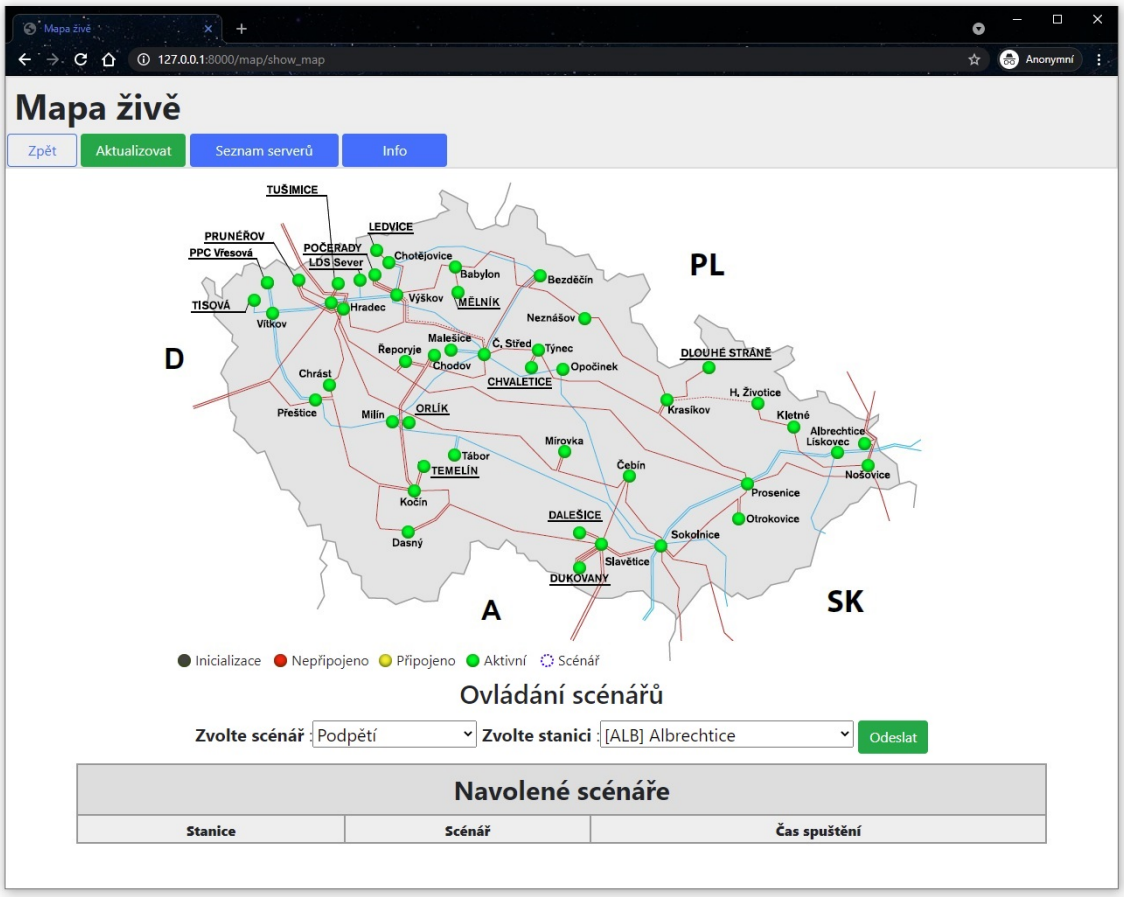
Mapa živě

Při návrhu a samotné implementaci webové aplikace bylo nezbytné vytvořit rozhraní, které je přizpůsobeno k průběžnému monitorování stavů jednotlivých serverů pro možnost ovládání polygonu PS v reálném čase. Rovněž bylo zapotřebí implementovat funkce spojené s rychlým spouštěním (resp. ukončením) scénářů kritických stavů stanic či útoků na ně. Ukázka stránky „Mapa živě“ je zobrazena na obr. 2.8.

Vykreslení webové stránky zajišťuje funkce definovaná v souboru *view.py*. Jedná se o klíčový soubor webové aplikace určující způsob zpracování přijatých požadavků, případně určuje jaké webové stránky se mají zobrazit (resp. vykreslit). Ukázka kódu pro vykreslení webové stránky „Mapa živě“ je zobrazena ve výpisu 2.2.

Výpis 2.2: Funkce souboru *views.py* pro práci s daty.

```
#DEFINOVÁNÍ FUNKCE
def map_page_view(request):
#IDENTIFIKACE TYPU METODY
  if request.method == "GET":
#PŘEDÁNÍ HODNOT A VYKRESLENÍ STRÁNKY
    form = TakeCommandForm2()
    scenare = Scenare()
    user_simulated_scenarios = ScenariosDB.objects.all()
    context = {"form":form,
        "scenar": scenare,
        "User": user_simulated_scenarios}
    return render(request, "map.html", context)
```



Obr. 2.8: Webová stránka „Mapa živě“.

Hlavní úlohou webové stránky je zobrazování stavů serverů polygonu PS v reálném čase. Stanice jsou reprezentovány body (přesněji html prvky) a mohou nabývat 4 základních stavů:

- Inicializace – Dočasný stav, kdy webový server zjišťuje stav stanice PS.
- Nepřipojeno – Stanice je vypnuta, nebo ji nelze kontaktovat.
- Připojeno – Stanice je zapnuta, komunikuje s webovým serverem, ovšem neprobíhá emulace datového provozu.
- Aktivní – Stanice je zapnuta, komunikuje s webovým serverem a probíhá emulace datového provozu.

Všechny výše zmíněné stavy (kromě stavu „Inicializace“) mohou být v kombinaci se stavem „Scénář“. Stanice vykonávající navolený scénář je od ostatních odlišena speciálním ohraničením.

Pro zajištění zobrazení stavů serverů v reálném čase byl do webové aplikace vytvořen a následně implementován asynchronní JavaScript. Ten zajišťuje pravidelnou aktualizaci html prvků (bodů) bez nutnosti aktualizace dané webové stránky. Ukázka vytvořeného JavaScriptu je zobrazena ve výpisu 2.3

Výpis 2.3: Vytvořený JavaScript pro aktualizaci stavů stanic.

```
#VOLÁNÍ AKTUALIZACE STAVŮ
window.onload = ExtractSSHData()
var intervalID = window.setInterval(ExtractSSHData, 15000)

#DEFINOVÁNÍ FUNKCE PRO AKTUALIZACI STAVŮ
function ExtractSSHData(){
  $.ajax({
#EXTRAKCE PŘIJATÝCH DAT
    type: "GET", url: "{%url "ssh_objects"%}",
    success: function(data){
#FUNKCE ROZLIŠUJÍCÍ STAVY JEDNOTLIVÝCH STANIC
    for (const [key, val] of Object.entries(data)) {
      if (val == 1) {
#AKTUALIZACE BODU REPREZENTUJÍCÍ STANICI
        document.getElementById(key).style.backgroundColor
        ="#FFEA17";
        document.getElementById(key).style.border = "0px";}
      ...
      DALŠÍ PODMÍNKY
      ...
    }},
  });
};
```

Jak již bylo zmíněno, webová stránka „Mapa živě“ obsahuje ovládací prvky pro práci s vytvořenými scénáři (kapitola 2.4). Konkrétně se jedná o sekci „Ovládání scénářů“, kde je možné zvolit typ scénáře a stanici, pro kterou se má zvolený scénář aplikovat. Funkce zajišťující spouštění scénářů kritických stavů je zobrazena ve výpisu 2.4.

V případě, že je scénář úspěšně spuštěn, je zapsán do databáze scénářů. Každý zápis do databáze obsahuje název scénáře, stanici a časové razítko. Struktura prvků databáze je zobrazena ve výpisu 2.5.

Po zapsání scénáře do databáze je rovněž zobrazen v sekci „Navolené scénáře“. Ukázka dvou navolených scénářů je zobrazena na obr. 2.9. V případě, že je daný scénář ukončen (resp. je na zvolené stanici spuštěn scénář standardního provozu), je z databáze odebrán.

Výpis 2.4: Funkce souboru *scenarios.py* pro spouštění scénáře.

```
#DEFINOVÁNÍ FUNKCE PRO SPOUŠTĚNÍ KRITICKÝCH SCÉNÁŘŮ
def scenario0_3(IP:str, scenar:int):
#VYTVOŘENÍ SPOJENÍ
    stanice = ssh(IP)
#NALEZENÍ STANICE V DATABÁZI
    db_query = Servers.objects.get(IP=IP)
#EDITACE KONFIGURAČNÍHO SOUBORU STANICE
    stanice.getfile("/home/pi/"+str(db_query.my_dir)
    +"/ServerStatus.txt",DOWNLOAD_FILE)
    for i in range(db_query.traffo_amount):
        stanice.openfile(i,scenar)
    stanice.uploadfile("/home/pi/"+str(db_query.my_dir)
    +"/ServerStatus.txt",DOWNLOAD_FILE)
#UKONČENÍ SPOJENÍ
    stanice.client.close()
    return 0
```

Výpis 2.5: Definice modelu souboru *models.py*.

```
#VYTVOŘENÍ MODELU
class ScenariosDB(models.Model):
#DEFINOVÁNÍ ATRIBUTŮ PRVKU
  scenario = models.CharField(max_length=50)
  station = models.CharField(max_length=100)
  time_stump = models.DateTimeField(auto_now=True)

#FUNKCE VRACEJÍCÍ PRVEK DATABÁZE V PODOBĚ ŘETĚZCE
  def __str__(self):
    return "Scenario: " +self.scenario +" Stanice:
    "+self.station+" TS: "+str(self.time_stump)
```

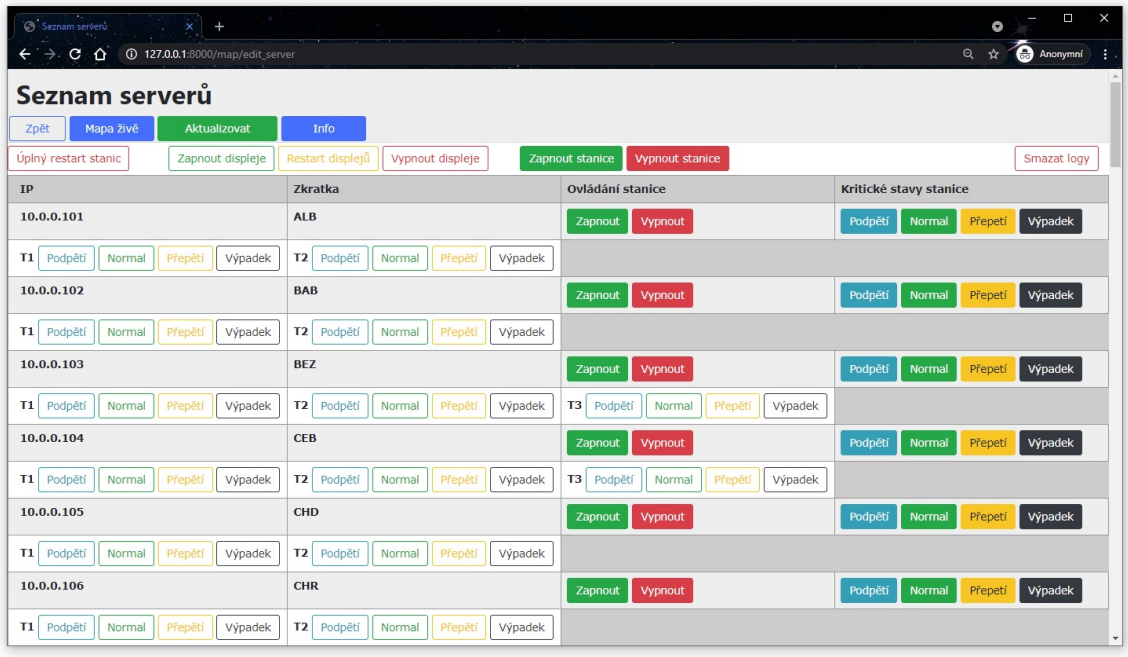
Navolené scénáře

Stanice	Scénář	Čas spuštění
[CEB] Čebín	Podpětí	May 9, 2021, 8:04 p.m.
[KRA] Krasíkov	Vyřazení kontroly	May 9, 2021, 8:06 p.m.

Obr. 2.9: Záznam spuštěných scénářů webové stránky „Mapa živě“.

Seznam serverů

Webová stránka slouží ke kompletní správě polygonu PS. Kromě záhlaví, které je přítomno u všech webových stránek a slouží k navigaci v rámci webové aplikace, obsahuje seznam všech serverů polygonu. Stanice jsou vykresleny z databáze serverů obdobně jako v případě spuštěných scénářů (viz „Mapa živě“). Záznam je tvořen IP adresou, zkratkou stanice a počtem simulovaných transformátorů. Ukázka webové stránky „Seznam serverů“ je zobrazen na obr. 2.10.



Obr. 2.10: Webová stránka „Seznam serverů“.

Všechny příkazy lze spustit pomocí ovládacích tlačítek a byly zde vytvořeny funkce jak pro správu individuálních stanic, tak funkce globální pro hromadnou správu stanic polygonu. Kód zajišťující spouštění scénářů je obdobný výpisu 2.4. Do kategorie globální správy spadá:

- Úplný restart stanic – Příkaz k restartu všech stanic polygonu.
- Zapnutí/Restart/Vypnutí displejů – Příkazy k ovládání informačních displejů IIC I2C OLED.
- Zapnutí/Vypnutí stanic – Příkazy ke spuštění/zastavení emulace datové komunikace protokolu IEC 60870-5-104 stanicemi polygonu.
- Smazat logy – Příkaz ke smazání zaznamenaných údajů na stanicích polygonu.

Do kategorie individuálních ovládacích funkcí patří:

- Zapnutí/Vypnutí – Příkazy ke spuštění/zastavení emulace datové komunikace dané stanice.

- Podpětí/Přepětí/Výpadek (stanice) – Příkazy ke spuštění simulace kritických stavů stanice.
- Podpětí/Přepětí/Výpadek (transformátor) – Příkazy ke spuštění simulace kritických stavů konkrétního transformátoru stanice.

Web104 info

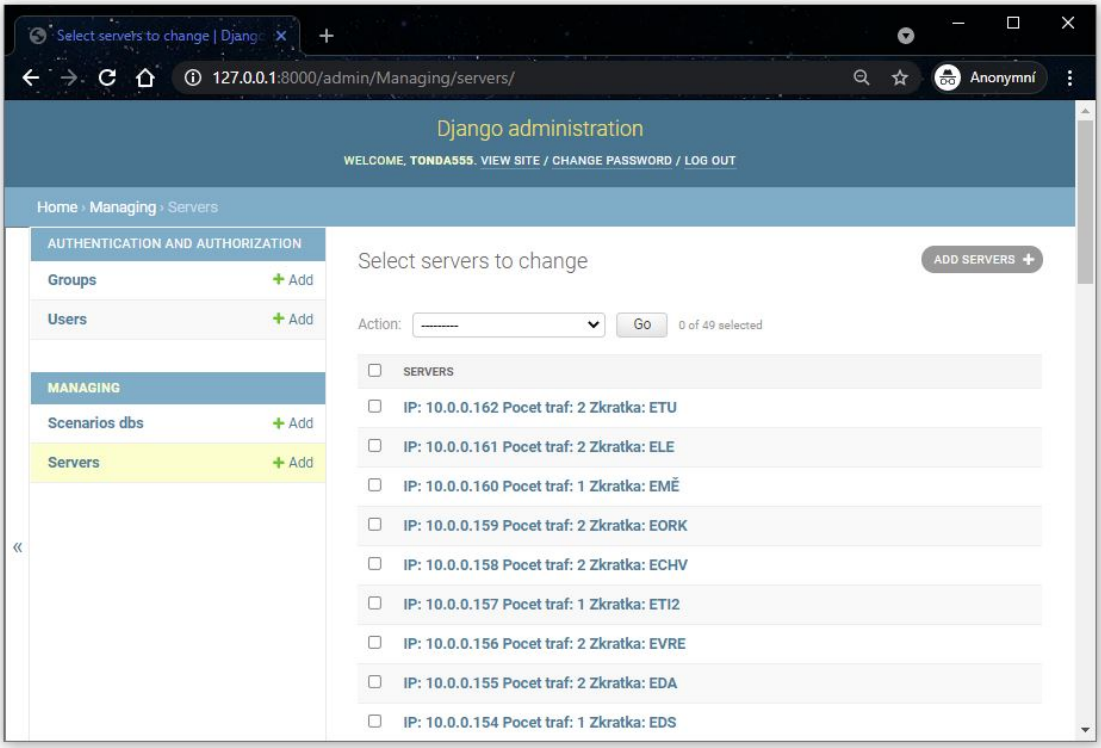
Poslední vytvořenou webovou stránkou je „Web104 info“, viz obr. 2.11. Stránka obsahuje základní informace o webové aplikaci včetně kontaktních údajů či odkazů na zdrojové soubory.

Obr. 2.11: Webová stránka „Web104 info“.

Django admin site

Jedná se o administrátorskou webovou stránku (resp. celou oblast webu) Django aplikace. Je generovaná automaticky a pomocí definovaných modelů (viz výpis 2.5) vytvoří rozhraní pro správu databází, kterou lze využít k tvorbě, aktualizaci a mazání záznamů databází.

Na rozdíl od databáze scénářů, nelze přistupovat k záznamům databáze serverů jiným způsobem než pomocí administrátorské webové stránky. Hlavním důvodem je zabránit neoprávněné editaci záznamů a tím narušit správné fungování celé webové aplikace. Ukázka administrátorské webové stránky je zobrazena na obr. 2.12.



Obr. 2.12: Webová stránka „Django administration“.

Přístup k administrátorské webové stránce je omezen pro administrátory a oprávněné uživatele. Účet „superuživatele“, který má plný přístup k webové aplikaci a všechna potřebná oprávnění k vytváření oprávněných uživatelů, lze vytvořit pomocí souboru *manage.py*.

2.3.2 Spuštění webového serveru

Spuštění webového serveru probíhá pomocí příkazové řádky. Přistoupíme do složky projektu a zadáme příkaz:

python manage.py runserver [IP]:[port],

v případě korektního spuštění webového serveru, dostáváme konzolový výpis obdobný výpisu 2.6. Následně stačí zapnout webový prohlížeč s příslušnou IP adresou a portem. V rámci realizace webového serveru polygonu PS byla zvolena IP adresa 10.0.0.9 a port 8888.

Výpis 2.6: Konzolový výpis při spuštění serveru.

```
Watching for file changes with StatReloader
Performing system checks...

System check identified no issues (0 silenced).
May 08, 2021 - 17:38:37
Django version 3.1.2, using settings 'Web104.settings'
Starting development server at http://10.0.0.9:8888/
Quit the server with CTRL-BREAK.
```

2.4 Scénáře chování

Stanice přenosové sítě ČR mají definovaná pravidla provozu, kde nejvýznamnějším z nich je „Kodex přenosové soustavy“ (dále jen kodex). Cílem kodexu je stanovit technické, konstrukční a provozní požadavky pro připojení a užívání PS a stanovit podmínky pro poskytování Podpůrných služeb (PpS) a Poskytování systémových a přenosových služeb (PřS). Výsledkem je zajištění funkčnosti PS v případě standardních i nestandardních situací. [28]

Pod pojmem „scénář chování“ si můžeme představit nadefinovanou sekvenci provozních kroků určitého systému (v našem případě PS ČR). Takto nadefinované chování může následně sloužit k testování, zkouškám nových zařízení, či generování síťového provozu běžného pro daný typ sítě.

Pro vytvořený polygon energetické PS byly v rámci této práce vytvořeny níže zmíněné scénáře. Ty byly vytvořeny tak, aby reprezentovaly nejčastější stavy, ve kterých se mohou reálné stanice PS (popřípadě samotný polygon) nacházet. Mezi realizované scénáře chování patří:

- scénář standardního provozu,
- podpětí transformátoru,
- přepětí transformátoru,
- výpadek transformátoru,
- útoku vyřazení lokální kontroly stanice,
- útok na elektrárny.

Jedná se o komplexní scénáře, které jsou definované od samotných transformátorů v rámci jedné rozvodny/elektrárny až po celou infrastrukturu PS. Navrženy a implementovány byly tak, aby je v případě potřeby bylo možné spustit např. jen pro jeden transformátor dané rozvodny/elektrárny. Výjimku tvoří scénáře útoku, které jsou aplikovány na stanici, či skupinu stanic polygonu.

2.4.1 Scénář standardního provozu

Dle kodexu vytvořeného ČEPSem musí všechny stanice PS splňovat stanovené rozsahy napětí, frekvence atd. (viz níže) po dobu 99 % času provozu (ovšem existují i výjimky). Představuje tak nejběžnější stav stanice PS, ve kterém se nachází a pro který byla navržena a uzpůsobena. Jedná se tedy o stav, kdy nepodléhá žádným nepříznivým vnějším či vnitřním vlivům, které by měly dopad na správné fungování. Kodex mimo jiné také upřesňuje rozsahy simulovaných hodnot pro zařízení spadající do PS, konkrétně velikosti vstupních a výstupních napětí, hodnoty jalových a zdánlivých výkonů a frekvencí. Scénář představuje standardní chování transformátoru (či celé stanice) v době, kdy simulované hodnoty spadají do rozsahů stanoveným kodexem PS. [28]

Regulace napětí

Při standardním provozu musí 99 % všech měřených hodnot efektivního napětí (pro libovolné týdenní období) spadat do rozsahu stanovených tab. 2.7. Hodnoty vychází ze souboru změřených hodnot v intervalech měření 10 minut. Zároveň kodex definuje, že pro napěťovou úroveň $110\,kV$ nesmí být žádná z průměrných efektivních hodnot napájecích napětí mimo rozsah $110\,kV$ $\pm 15\,\%$. [28]

Tab. 2.7: Napěťové rozsahy sítě.

Napájecí úroveň	Stanovená hodnota napětí	Napěťový rozsah
$110\,kV$	$110\,kV$ $\pm 10\,\%$	99–121 kV
$220\,kV$	$220\,kV$ +11,8 / -10 %	198–246 kV
$400\,kV$	$400\,kV$ +5 / -10 %	360–420 kV

Regulace frekvence

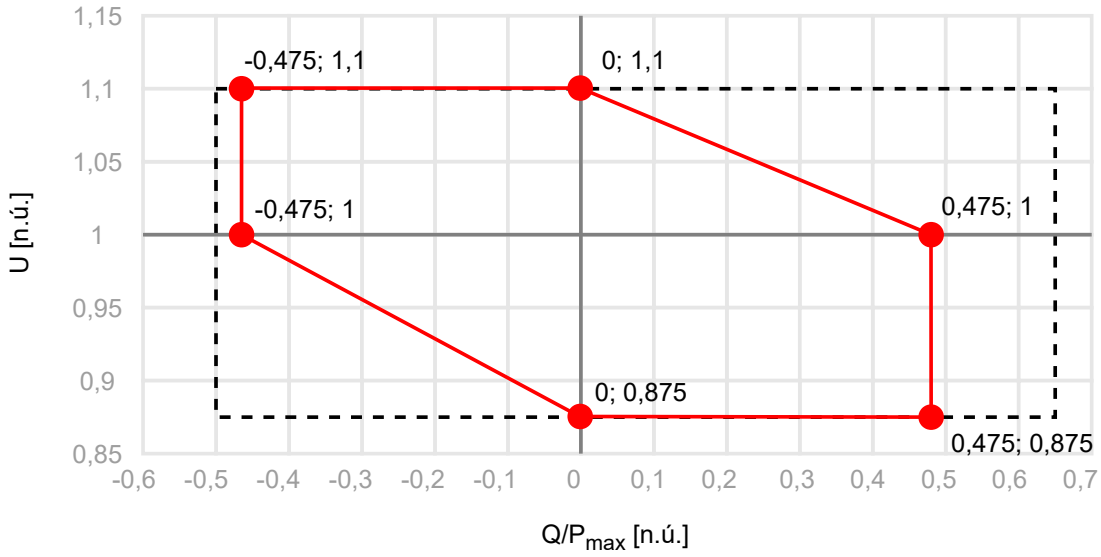
Obdobně jako v případě regulace napětí stanoveného kodexem, podléhá soustava také frekvenční regulaci. Jmenovitý kmitočet napájecího napětí je $50\,Hz$. Za normálního provozu musí střední hodnota kmitočtu odpovídat hodnotám stanovených tabulkou 2.8, ze souboru dat měřených v intervalech 10 s. [28]

Tab. 2.8: Frekvenční rozsahy sítě.

Doba provozu	Stanovená hodnota frekvence	Frekvenční rozsah
99,5 %	$50\,Hz$ $\pm 10\,\%$	49,5–50,5 Hz
100 %	$50\,Hz$ +4 % / -6 %	47–52 Hz

Jalový, činný a zdánlivý výkon zařízení PS

Každé zařízení PS musí být schopno dodávat dodatečný jalový výkon, který kompenzuje nabíjecí výkon vedení nebo kabelu vysokého napětí mezi vysokonapěťovými svorkami blokového transformátoru nového zařízení, respektive VM[13] nebo svorkami jeho nového VM. V případě dodávky maximálního činného výkonu do soustavy, musí být VM schopen pracovat v mezích stanovených diagramem na obr. 2.13. Uvedený diagram je stanoven pro jmenovitou hodnotu frekvence 50 Hz a je vztažen k referenční napěťové úrovni (n.ú.) 400, 220 nebo 110 kV. [28]



Obr. 2.13: Diagram dodávky jalového výkonu při maximálním činném výkonu.

Regulační systém činného výkonu nového VM musí být schopen upravovat zadanou hodnotu činného výkonu (v souladu s pokyny ČEPS) neboli musí obsahovat terminál elektrárny pro dálkové řízení. Doba, během níž musí být zadaná hodnota činného výkonu dosažena, je stanovena na 5 minut pro synchronní VM a 1 minuta pro nesynchronní VM. Přípustná odchylka skutečného činného výkonu od požadované hodnoty je ±5 %. [28]

PS se propojují synchronně, tj. jsou připojeny přímo vedením, nebo asynchronně přes soustavu stejnosměrných spojek. Synchronně propojené soustavy mají shodný kmitočet střídavého napětí, neboť je kmitočet systémová veličina, která je dána rovnováhou činného výkonu mezi výrobou a spotřebou v celé propojené soustavě. Asynchronní soustavy mají kmitočet navzájem odlišný a jsou na hodnotách svých kmitočtů nezávislé. Jmenovitá hodnota kmitočtu může být u asynchronních soustav stejná, ovšem okamžitý kmitočet je vždy alespoň nepatrně rozdílný. [2]

[13] Výrobní Modul

Teplotní rozsahy

Norma IEC 60076-7 stanovuje maximální dovolené teploty pro různé části transformátorů. Limitní hodnoty pro normální cyklické a nouzové zatěžování jsou uvedeny v tabulce 2.9. V případě, kdy teploty oleje překročí 140 °C, může docházet ke snížení dielektrické pevnosti transformátoru, kvůli vzniku plynových bublinek. [29, 30]

Tab. 2.9: Teplotní limity výkonových transformátorů přenosové soustavy.

Komponenty transformátoru	Normální zatěžování	Dlouhodobé nouzové zatěžování	Krátkodobé nouzové zatěžování
Vinutí a metalické části bez kontaktu s olejem	120 °C	140 °C	160 °C
Metalické části, které jsou v kontaktu s olejem	140 °C	160 °C	180 °C
Olej horní části transformátoru	105 °C	115 °C	115 °C

Realizace scénáře standardního provozu

Jak již bylo řečeno, jedná se o standardní chování transformátoru, kde jsou simulovány periodické zprávy velikostí měřených fyzikálních veličin, které jsou následně posílány do dispečerního střediska pomocí protokolu IEC 60870-5-104. Výše zmíněné informace z kodexu byly použity jako podklady při vytváření scénářů chování.

Transformátor při scénáři standardního provozu simuluje data vstupních a výstupních napětí (U_{ab}, U_{bc}, U_{ca}) v rozsahu 360–420 kV pro napěťovou úroveň 400 kV, 198–246 kV pro úroveň 220 kV a 99–121 kV pro úroveň 110 kV dle tabulky 2.7. Dále simuluje velikost vstupních a výstupních proudů (I_a, I_b, I_c) pohybující se ve stovkách až tisících ampérech podle typu rozvodny/elektrárny. Velikosti hodnot činného výkonu (P_a, P_b, P_c) jsou dopočítávány pomocí vzorce:

$$P = U \cdot I \cdot cos(\varphi) \quad [W]. \tag{2.1}$$

Velikosti hodnot jalového výkonu (Q_a, Q_b, Q_c) jsou dopočítávány pomocí vzorce:

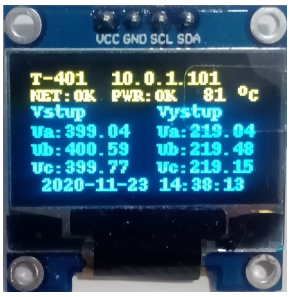
$$Q = U \cdot I \cdot sin(\varphi) \quad [var], \tag{2.2}$$

kde hodnota φ představuje fázový posun a je nastavena na hodnotu 0,525 rad (přibližně 30°, představující efektivitu 85 %).

Dále jsou simulovány hodnoty frekvence v rozsahu 49,5–50,5 Hz pro jmenovitou frekvenci 50 Hz. Tento rozsah odpovídá rozsahu provozu stanice po libovolnou dobu bez omezení viz tab. 2.8. Maximální a minimální teploty transformátoru jsou

konstantní a určují teplotní pásmo, ve kterém se může teplota transformátoru pohybovat. Pro tento polygon byl zvolen rozsah 100 až 140 °C. Simulovány jsou také hodnoty teploty transformátoru v rozsahu 120 ±20 °C (viz tab. 2.9) a hodnoty okolní teploty 20 ±5 °C reprezentující vnější podmínky.

V neposlední řadě jsou simulovány také zprávy o stavech událostí či zda je spuštěn poplach kritického stavu (v tomto scénáři vždy negativní), viz kapitola 2.4.2. Ukázka zobrazení standardního provozu informačním displejem je zobrazena na obr. č. 2.14.



Obr. 2.14: Zobrazení standardního provozu.

Programové řešení umožňuje modifikaci těchto rozsahů a hodnot pomocí konfiguračního souboru *MainConfig_server.txt* i v průběhu simulace. Všechny výše zmíněné hodnoty jsou generovány s periodou 0,5 s. Periodické zprávy posílané dispečernímu středisku jsou odesílány s periodou 5 s. Ke spuštění tohoto scénáře dochází automaticky po spuštění programu simulujícího transformátor stanice PS.

2.4.2 Kritické stavy

Provoz zdrojů průběžně sleduje Dispečink ČEPS pomocí databázových aplikací. Kontinuálně jsou sledovány všechny bloky PE, PPE, JE, VE a PVE[14], které jsou přímo vyvedené do PS a dále bloky PE a PPE vyvedené do sítí s napěťovou úrovní 110 kV a méně, pokud poskytují, nebo jsou schopné poskytovat PpS. [28]

Průběžně se sledují také výpadky prvků PS (vedení, přípojnic v rozvodnách a transformátorů) s důrazem na příčiny výpadků a na příslušná omezení výroby nebo dodávky, která vznikla v důsledku těchto výpadků. Je sledována a evidována příčina, velikost odpadlého výkonu, příslušná doba omezení, dále pak velikost nedodané nebo nevyrobené energie. Zvláštní pozornost je pak věnována plánovaným odstávkám a neplánovaným výpadkům mezistátních vedení 400 a 220 kV. [28]

Potíže v PS bývají jednou z příčin výpadků dodávky elektrické energie. Jedním z důvodů může být např. poškození důležitých venkovních vedení působením nepříznivých přírodních podmínek (námraza, silný vítr atd.), ale i celkovým přetížením

[14]PE - parní elektrárny, PPE - paroplanové elektrárny, JE - jaderná elektrárna, VE - vodní elektrárna, PVE - přečerpávací vodní elektrárny

soustavy. Zařízení PS jsou vybavena bezpečnostními prvky, které zajistí odpojení vybraných odběratelů v případě, že by hrozilo zničení nebo rozpad sítě vlivem jejího přetížení. Mohlo by dojít k tzv. kaskádovému šíření poruchy. Jedná se o stav, kdy po selhání přetíženého vedení vzroste přetížení zbytku sítě. Postupně jsou odpojovány další prvky sítě, až do kompletního rozpadu PS. [31]

ČEPS jako hlavní provozovatel rozvodné sítě ČR má vypracovanou celou řadu postupů a návodů, jak postupovat v krizových situacích, při různých poruchách, či výpadcích. Hlavním pravidlem provozu PS je tzv. kritérium N-1. To udává, že provoz, údržba, či modernizace soustavy dokáže udržet stabilitu soustavy i v případě výpadku jednoho prvku soustavy. V případě jaderných elektráren je aplikováno pravidlo N-2. Jedná se o pravidlo udržet normální parametry chodu i po výpadku dvou prvků soustavy. [28, 32, 33]

Z důvodů výskytu těchto plánovaných a neplánovaných událostí vznikly v rámci této práce scénáře kritických stavů. Scénáře představují chování stanice (v našem případě transformátoru stanice), která podléhá neočekávané události, která ovlivňuje její schopnost správného fungování. Jedná se o stavy plánovaného (např. údržba, oprava), či neplánovaného (např. technické poruchy, přebytek, nedostatek činného výkonu) odchýlení od běžných provozních rozsahů stanovených kodexem.

Všechny kritické scénáře je možné spustit pomocí příslušných tlačítek vytvořené webové aplikace (viz obr. 2.10). Tato tlačítka jsou naprogramována k patřičné editaci souboru *ServerStatus.txt* viz kapitola 2.2. Druhou možností spuštění scénáře kritického stavu je přímou editací tohoto souboru na daném zařízení dle tabulky 2.6.

Podpětí transformátoru

Rozvodné sítě mají zásadní nedostatek v podobě omezené schopnosti skladování energie. Znamená to, že objem vyrobené energie musí co nejvíce odpovídat množství spotřebovanému. V případě, kdy se tato rovnováha naruší, vzniká v síti přepětí (při nadměrné produkci), nebo podpětí (při nadměrné spotřebě). Při nedostatečné kompenzaci těchto odchylek dispečerním střediskem může dojít k výpadku sítě, či její části. S těmito nežádoucími stavy se v dnešní době příliš často nesetkáváme, protože v národních sítích jsou výkyvy ve spotřebě a dodávce zpravidla úspěšně tlumeny např. pomocí přečerpávacích elektráren.

Scénář představuje situaci, kdy daný transformátor nemá dostatek napájecí energie. Dochází k postupnému úbytku transformovaného napětí až do doby, kdy zareagují ochranné prvky, které transformátor (popřípadě celou stanici) odpojí, aby nedošlo k dalšímu poškození zařízení. V takovém případě jsou posílány kromě periodických dat i data spontánní. Přesněji data objektů, kterých se daná změna stavu týká, a to konkrétně hodnota „Hlavního jističe“ a stavu poplachu pro „Podpětí“,

dále pak i události „Změna hlavního jističe“ a „Spuštění alarmu“, která dohledové stanici indikuje změnu stavu hlavního jističe a zároveň i spuštění poplachu neobvyklé události. Tyto spontánní zprávy jsou odeslány bez ohledu na periodu odesílaných zpráv (viz kapitola 2.4.1) a to v době výskytu události každé 2 s až do doby, kdy je stanice vzdáleně či lokálně vypnuta, či znovu zapnuta.

V rámci tohoto scénáře dochází k úbytku transformované energie, který lze definovat v konfiguračním souboru *MainConfig_server.txt*. Je možno definovat míru úbytku energie, popřípadě rozmezí pro sepnutí ochranných prvků zařízení. Jak již bylo řečeno v úvodu této kapitoly, tento scénář lze spustit jak lokálně pomocí editace *ServerStatus.txt* (viz tabulka 2.6) nebo pomocí vytvořené webové aplikace. Samotná ukázka a testování tohoto scénáře je rozebráno v kapitole 3.2.2.

Přepětí transformátoru

Obdobě jako v předchozím případě, kde je narušena rovnováha produkce a spotřeby energie z důvodů nedostatku energie, může dojít k opačnému případu, kdy je energie naopak přebytek. Tento stav může být způsoben např. přebytkem nespotřebované energie odběratelů, či zapojením nového zařízení generujícího elektrickou energii.

Tento scénář tedy představuje situaci, kdy má daný transformátor přebytek napájecí energie oproti standardnímu provozu. Dochází k postupnému zesilování transformovaného napětí až do doby, kdy zareagují ochranné prvky, které transformátor odpojí od sítě, aby nedošlo k dalšímu poškození zařízení, či připojených rozvodných sítí. Při tomto stavu jsou opět posílány kromě periodických dat i data spontánní. Stejně jako v předchozím případě v době výskytu události a následně každé 2 s až do doby, kdy je na tuto událost zareagováno (vzdáleně či lokálně). V případě přepětí je posílána hodnota „Hlavního jističe“ a stav poplachu pro „Přepětí“, dále pak i události „Změna hlavního jističe“ a „Spuštění alarmu“.

V rámci tohoto scénáře dochází k nárůstu transformované energie, který lze definovat v konfiguračním souboru *MainConfig_server.txt*. Je možno definovat míru nárůstu energie, rozmezí pro sepnutí ochranných prvků zařízení, či dobu prodlevy odeslání spontánních zpráv. Stejně jako v předchozím případě lze tento scénář spustit jak lokálně pomocí editace *ServerStatus.txt* (viz tabulka 2.6) nebo pomocí vytvořené webové aplikace. Ukázka a testování tohoto scénáře je rozebráno v kapitole 3.2.3.

Výpadek transformátoru

Posledním kritickým scénářem je samotný výpadek (porucha) transformátoru. Jedná se o situaci, kdy daný transformátor okamžitě přestává plnit svoji primární funkci,

popřípadě kdy je přerušena dodávka energie. Jak již bylo řečeno v úvodu kapitoly 2.4.2, mezi nejčastější důvody patří výpadek způsobený přírodními vlivy, technickou závadou či lidským faktorem, popřípadě útokem na zařízení (viz kapitola 2.4.3).

V rámci tohoto scénáře dochází k okamžitému vypnutí transformace energie, respektive dochází k simulování nulových hodnot transformačních veličin (napětí, proud, výkon a frekvence). Stejně jako v předchozích případech jsou v době výskytu této neočekávané události odesílána i spontánní data s hodnotami „Hlavního jističe“ a stav poplachu pro „Zkrat“, dále pak události „Změna hlavního jističe“, „Spuštění alarmu“ a také „Změna ochranného relé“, které středisku oznamují, že došlo k okamžitému odpojení transformátoru.

Stejně jako v předchozích scénářích lze měnit doby prodlev odeslání spontánních zpráv pomocí konfiguračního souboru *MainConfig_server.txt*. Spustit scénář je možno lokálně pomocí editace *ServerStatus.txt* (viz tabulka 2.6) nebo pomocí vytvořené webové aplikace. Samotná ukázka a testování tohoto scénáře je rozebráno v kapitole 3.2.4.

2.4.3 Scénáře útoku

Energetický sektor je ve většině vyspělých zemí součástí kritické infrastruktury a kritické informační infrastruktury. Představuje tedy soustavu velkého významu pro fungování daného státu, které by mělo odolávat kybernetickým hrozbám. Ovšem tento energetický sektor v jeho implementaci není primárně zaměřen na bezpečnost, ale na funkčnost. To představuje velké množství zranitelností, které může potencionální útočník zneužít. V praxi může mít takový zásah značný dopad na provoz soustavy a schopnost výroby energetické energie pro samotné odběratele. [34]

Z tohoto důvodu byly v rámci polygonu realizovány a implementovány scénáře útoků na stanice polygonu či na infrastrukturu a integritu rozvodné sítě, aby existovala možnost zkoumat útoky v bezpečném (simulovaném) prostředí. Další výhodnou je možnost vytváření opatření proti dalším útokům, hledání zranitelností soustavy či zjišťování kritických bodů infrastruktury.
Mezi nejznámější realizované útoky cílené na energetický sektor jsou např. Shamoon, Dragonfly, Industroyer, Trisis/Triton, Grey Energy, Stuxnet a BlackEnergy. Poslední dva zmíněné útoky sloužily jako předloha pro vytvořené scénáře útoků. [35]

Útok vyřazení lokální kontroly stanice

Scénář útoku vyřazení lokální kontroly stanice byl realizován na základě analýzy malwaru „Stuxnet“ objeveného roku 2010 běloruskou bezpečnostní společností VirtusBlokAda a je považován za nejsofistikovanější malware, který měl za cíl íránský nukleární program. Jednalo se o úspěšný útok zpomalující proces obohacování uranu

a výroby nukleárních zbraní. Jedná se o první malware cílený přímo na průmysl, jehož součástí byl i programovatelný rootkit, který představuje techniku používanou při falzifikaci informací o škodlivém kódu s cílem skrýt jeho přítomnost. [35]

Tento scénář cílí na změnu odesílaných dat bez vědomí dispečerní kontroly. Skládá se z čtyř základních částí:

1. získání přístupu do stanice,
2. zachytávání simulovaných hodnot,
3. vytvoření zobrazovací smyčky,
4. vzdálené přetěžování sítě.

Při tomto scénáři útočník získá přístup do lokální ovládací a kontrolní sítě. Následně sesbírá dostatečný vzorek dat pro zacyklení veškerých zobrazovacích prostředků (v našem případě nejen informačního displeje, ale i zobrazení ve SCADA softwaru openMUC). Poté začne útočník vzdáleně přetěžovat síť PS. Dispečerní středisko bude od stanice dostávat nereálné údaje o sledovaných hodnotách, které nebudou odpovídat hodnotám skutečným.

Za účelem simulace útoku je do infrastruktury připojeno další zařízení představující útočníka. Ten pomocí zjištěného přihlašovacího jména a hesla, získaného např. jako při útoku Stuxnet pomocí sociálního inženýrství, získá přístup do stanice polygonu. Jelikož je celá rozvodna reprezentována programově, není možné reprezentovat útok s reálnými kroky. Útočník spustí skript, který zapříčiní zobrazování zacyklených dat podobných reálně snímaným datům stanice. Následně útočník upraví konfigurační soubory stanice k přetěžování PS.

Během tohoto scénáře jsou posílána periodická data dispečerní stanici stejně jako v případě standardního provozu. Dispečerní středisko bude zaznamenávat neobvyklý přebytek energie v celé PS, ovšem data přijatá od této stanice nebudou vykazovat známky výkyvů od stanovených rozsahů.

Vzhledem k faktu, že útočník má nad stanicí plnou kontrolu, může kromě zmíněného dlouhodobého přetěžování soustavy také přímo odpojit stanici, přeposílat reálná data, či odstranit bezpečnostní prvky stanice. Stejně jako v případě scénářů kritických stavů stanice, lze i tento scénář spouštět z vytvořené webové aplikace. Ukázka a samotný průběh tohoto scénáře je rozebrán v kapitole 3.2.5.

Útok na elektrárny

Obdobně jako předchozí scénář byl tento inspirován malwarem „BlackEnergy“ z roku 2015 cílený na ukrajinský energetický sektor. Při tomto útoku napadli útočníci tři regionální distribuční společnosti, což mělo za následek výpadek, který zasáhl přes 200 tisíc zákazníků. Kromě samotných distribučních společností byl útok zaznamenán i u ostatních kritických infrastruktur, ovšem bez provozního dopadu. [35]

V případě tohoto scénáře se jedná o útok na infrastrukturu rozvodné sítě běžným způsobem. Útočník, či více útočníků pomocí hrubé síly způsobí poškození kritické části elektrárny (např. chladicího okruhu, či ovládacího rozhraní stanice), která by vedla k okamžitému odstavení celé elektrárny. Dojde tedy k razantnímu poklesu generované elektrické energie, což povede k bezpečnostnímu odpojení zbylých stanic.

Scénář útoku na elektrárny cílí na vyřazení klíčových elektráren pro zastavení primární funkce PS. Je složen pouze ze dvou základních částí:

1. získání přístupu do stanice,
2. odstavení elektrárny.

Pro účel simulace útoku bude do infrastruktury připojeno zařízení představující útočníka. Stejně jako v předchozím případě získá útočník přístup do stanice polygonu (sociální inženýrství či brute-force). Přes toto zařízení bude pomocí ovládacího rozhraní vyslán konkrétní elektrárně příkaz, který zapříčiní přerušení programu simulující stanici. Ovšem v rámci dodržení autentičnosti útoku dochází po odstavení stanice k rozeslání povelu pro spuštění scénáře „Podpětí“ okolním návazným rozvodnám, který reprezentuje pokles napěťových úrovní až do doby jejich odstavení, či reakce dispečinku na událost.

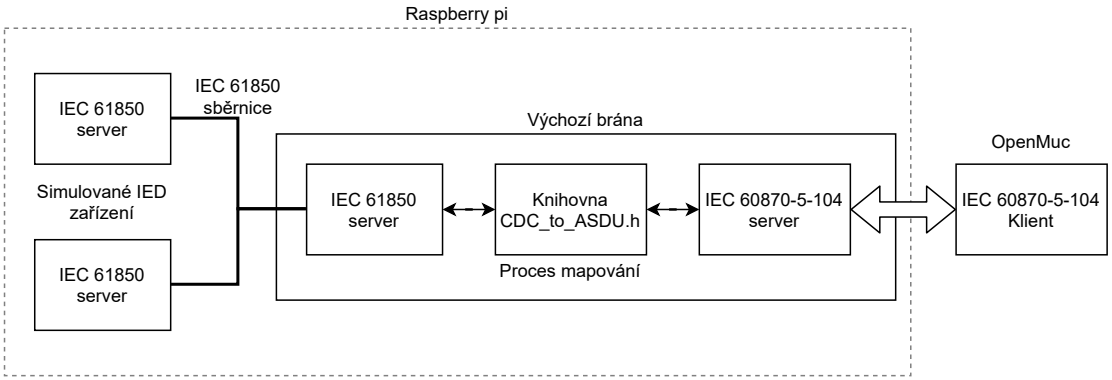
V průběhu útoku elektrárna nesimuluje žádná data, neboť došlo ke kritickému poškození s okamžitým vypnutím. Dispečerní středisko může okamžitě vyhodnotit, že došlo ke kritické chybě v infrastruktuře, či útoku, ovšem tento stav mohou pouze kompenzovat zvýšením výroby energie jiných zdrojů (k dodržení kritéria N-1) a nahlásit příslušným bezpečnostním a servisním orgánům. Ovšem v případě odstavení většího počtu elektráren současně by mohlo dojít k přetížení zbylých výrobních zařízení, které by mohlo vést k již zmíněnému kaskádovému šíření poruchy.

Dopad útoku může mít nedozírné následky. Při ochromení celé rozvodné sítě bude schopnost veřejných a bezpečnostních orgánů značně omezena. Většina mobilní komunikace nebude provozuschopná stejně jako výrobní fabriky firem. Ušlé zisky těchto firem a náklady na opravu poškozených elektráren se mohou vyšplhat do řádu miliard korun. Průběh tohoto scénáře je zobrazen a popsán v kapitole 3.2.6.

2.5 Mapovací modul IEC 61850-80-1

Jak již bylo vysvětleno v kapitole 1.3.2, norma IEC 61850-80-1 rozšiřuje původní standard IEC 61850 a poskytuje pokyny pro výměnu informací z datového modelu CDC na IEC 60870-5-101/104. V rámci implementace technické normy do vytvořeného polygonu PS byla vytvořena knihovna *CDC_to_ASDU.h* obsažená v příloze A. Knihovna zajišťuje převod zprávy z datového typu CDC na korektní typ

ASDU zprávy protokolu IEC 60870-5-104. Schéma pro komunikaci mezi standardy IEC 61850 a IEC 60870 je znázorněno na obr. 2.15.



Obr. 2.15: Komunikační schéma mapovacího modulu.

Pro převod dat byly využity simulátory IED zařízení generující datový provoz standardu IEC 61850. Generovaná data jsou pomocí sběrnice přenesena do serverové stanice IEC 61850 představující výchozí bránu (popř. proxy server). Následně dochází k procesu mapování pomocí knihovny *CDC_to_ASDU.h*. Vytvořená zpráva je předána serverové stanici IEC 60870-5-104. Tento proces probíhá v rámci jedné výchozí brány, obdobně jako v případě koncepčního schématu na obr. 1.5. Následně je zpráva odeslána pomocí protokolu IEC 60870-5-104 (přes TCP/IP) klienstké stanici IEC 60870-5-104, v tomto případě realizované softwarem OpenMUC.

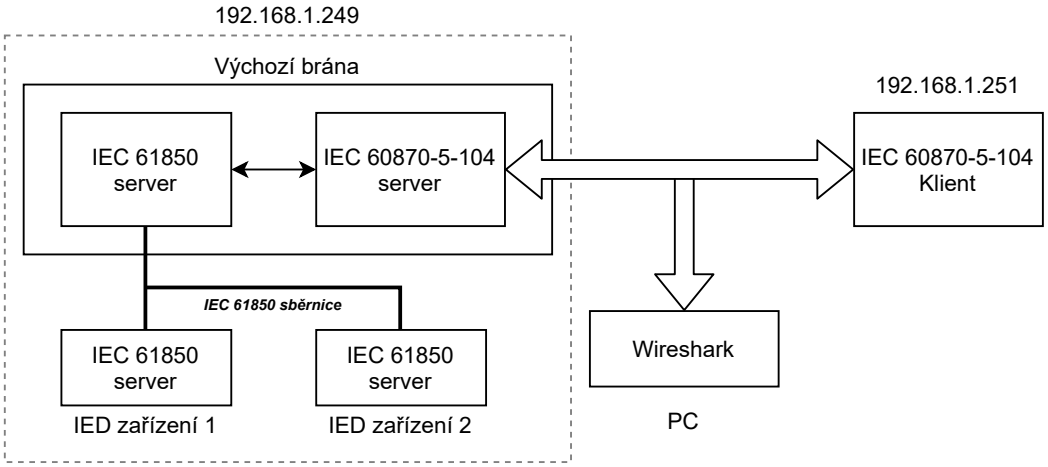
Knihovna CDC_to_ASDU

Vytvořená knihovna *CDC_to_ASDU.h* je složena z několika částí, kde každá slouží ke specifickému účelu. První část obsahuje pomocné definice a konstanty, které jsou následně využívány k procesu mapování. Vzhledem k faktu, že standard IEC 61850 je založený na jmenném nikoli numerickém systému, bylo potřebné definovat seznam typů CDC a přiřadit jim numerickou hodnotu stejně jako v případě standardu IEC 60870-5-104. Další část obsahuje kompletní mapovací tabulky vycházející z technické normy IEC 61850-80-1. [20]

Následně jsou v knihovně obsaženy funkce sloužící k vytvoření konkrétních typů ASDU zpráv a jednotlivých typů informačních objektů, viz příloha E. V poslední části jsou definovány přepínače, které na základě mapovací tabulky volají příslušné funkce pro vytvoření zpráv včetně všech ostatních náležitostí. Mezi tyto náležitosti patří např. číslo informačního objektů (IOA), měřená (respektive předávaná) hodnota, adresa původce zprávy (OA), adresa kanálu (CA), nebo pokud je obsaženo, tak i časové razítko.

Testování modulu

Schéma využité při testování mapovacího modulu je zobrazeno na obr. 2.16. Vzhledem k charakteru modulu a simulovaných IED zařízení byla komunikace zachytávána mezi výchozí bránou stanice polygonu a dohledovým střediskem OpenMUC. Komunikace zachycená programem Wireshark odpovídá komunikaci rozebrané v kapitole 3.1. Simulované IED zařízením generovaly testovací hodnoty typu SPS[15], DPS[16], či MV[17]. Všechna simulovaná data byla úspěšně převedena (dle tabulky G.1) a doručena dohledovému středisku pomocí protokolu IEC 60870-5-104. Záznam komunikace je zobrazen v příloze B na obr. B.6.

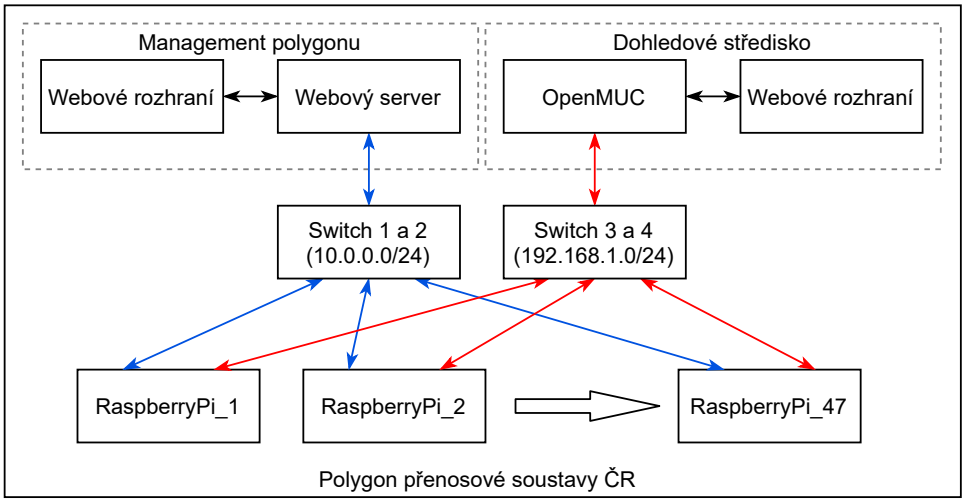


Obr. 2.16: Testovací schéma mapovacího modulu.

[15]Single point status – Stav jednobodové informace.
[16]Double point status – Stav dvoubodové informace.
[17]Measured value – Měřená hodnota.

3 Testování a rozbor komunikace

Jak již bylo řečeno v kapitole 2.1, zapojení se skládá ze dvou sítí a to servisní a datové, viz schéma 3.1. Servisní síť *10.0.0.0/24* je vytvořena pro správu a management jednotlivých serverových stanic. Datová síť *192.168.1.0/24* je naopak využita pro přenos simulujících dat protokolu IEC 60870-5-104 a je zatížena mnohonásobně více než síť servisní.



Obr. 3.1: Schéma zapojení polygonu přenosové soustavy ČR.

Ve schématu se nachází 47 zařízení Raspberry Pi reprezentující serverové stanice rozvoden a elektráren. Tyto stanice jsou připojeny do čtyř rozbočovačů značky MikroTik. Rozbočovač 1 a 2 slouží k propojení jednotlivých stanic s webovým serverem, na kterém běží ovládací a kontrolní rozhraní. Naopak rozbočovač 3 a 4 propojuje stanice s dohledovým střediskem využívající softwarový framework OpenMUC. Ten slouží ke zjednodušení implementace jednotlivých monitorovacích a řídicích aplikací.

3.1 Rozbor komunikace

Tato část rozebírá základní komunikační prvky jak z datové, tak i servisní části polygonu. Mezi tyto prvky patří například navázání spojení mezi klientem a serverem, synchronizace času či ukončení spojení, dále pak i komunikace mezi webovým serverem a serverovou stanicí. Všechny komunikační prvky budou demonstrovány na jednom vzorku klient-server, neboť komunikace je pro všechny ostatní stanice polygonu či prvky managementu velice obdobná. Všechny záznamy komunikace zachycené pomocí programu Wireshark[1] nalezneme v příloze B.

[1]Stránky Wireshark – `https://www.wireshark.org/`

Navázání spojení

Při procesu navazování spojení mezi klientem a serverem (v tomto případě stanicí polygonu) dochází k vytvoření TCP spojení na definovaném portu. Tento port lze nastavit pomocí konfiguračního souboru *MainConfig_server*. Následně je odeslána APCI zpráva *StartDT_act*, která zjišťuje, zda je daný server připraven ke vzájemné komunikaci. V případě, že je server připraven, odpoví zprávou *StartDT_con*. V opačném případě server nereaguje. Obě zprávy mají velikost 60 B. Ukázka APCI zprávy *StartDT_act* je zobrazena na obr. č. B.1 a zprávy *StartDT_con* na obr. B.2.

Synchronizace času

Synchronizace času je důležitým prvkem při komunikaci v energetickém i jiném podobném odvětví. V případě události a zpětné analýzy jevu udávají důležitá data převážně prostřednictvím časových razítek. Tato razítka jsou připojována ke generovaným datům, aby prokázala čas jejich vytvoření. Díky nim je možné analyzovat události v přesném časovém sledu.

Celková velikost této zprávy je 76 B, z čehož samotné časové razítko zabírá 7 B. Zpráva synchronizace času je zobrazena na obr. B.3. V dolní části si můžeme povšimnout samotného časového razítka ve formátu CP56Time2a.

Ukončení spojení

K ukončení spojení mezi klientem a serverem polygonu dojde, když jedna ze stran ukončí TCP spoj, viz obr. B.4, nebo při vyslání zprávy *StopDT*. V případě, kdy server nemá navázané spojení a nemá komu dané zprávy posílat, je ukládá do odesílací fronty. Po opětovném připojení klientské stanice jsou zprávy odeslány, takže nedochází k zahazování zpráv, kromě případu naplnění odesílací fronty.

Komunikace webového serveru a stanice polygonu

Spojení mezi webovým serverem a stanicemi emulujícími elektrárny/rozvodny přes servisní síť je realizováno převážně pomocí SSH. Jedná se o protokol pro zabezpečené komunikační spojení v sítích, které používají TCP/IP. Ukázka navázání spojení mezi webovým serverem a stanicí polygonu je zobrazena na obr. B.5.

3.2 Rozbor scénářů

Tato část je věnována rozboru simulovaných hodnot a zpráv poslaných serverem během jednotlivých scénářů včetně vizuálního znázornění průběhu. Zachycenou komunikaci a ukázky logovacích souborů nalezneme v příloze C.

3.2.1 Rozbor scénáře standardního provozu

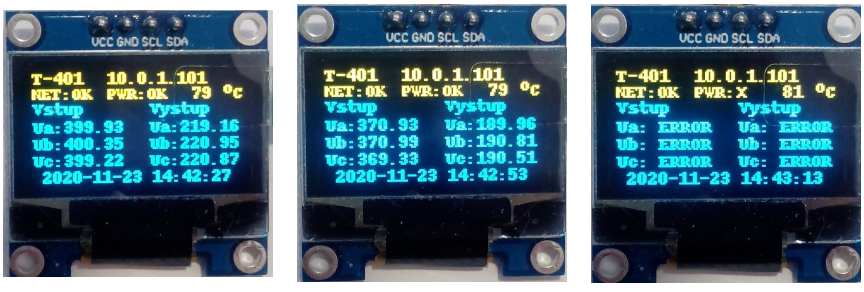
Jak již bylo řečeno v kapitole 2.4.1, scénář odpovídá standardnímu chování elektráren a rozvoden. Jedná se o nejběžnější stav, ve kterém se tyto stanice nachází. Na obr. C.1 jsou zobrazena periodická data vstupních hodnot (IOA=1000–1011), obdobně jsou posílána i data hodnot výstupních (IOA=2000–2011). Velikost těchto zpráv je 246 B a nesou data 12 objektů.

Obrázek C.2 ukazuje periodickou zprávu obhajující hodnoty teplot a frekvence (IOA=3000–3003). Tato zpráva je se svými 141 B podstatně menší, ovšem nese v sobě data pouze čtyř objektů. A nakonec obr. C.3 zobrazuje zprávu nesoucí hodnoty stavů ochranných prvků a poplachů (IOA=4000–4004). Jedná se o jednoduší typ zprávy, neboť obsahuje například zkrácené časové razítko, a tak dosahuje velikosti 101 B. Obdobná data jsou přenášena i pro zprávu týkající se událostí (IOA=5000–5004). Všechny tato data server odesílá klientské (dohledové) stanici a přímo odpovídají tabulce 2.4. Pro lepší přehlednost obr. C.4 obsahuje výpis logovacího souboru přijatých dat klientskou stanicí.

Při sečtení velikostí všech periodických zpráv dostáváme 835 B generovaných serverem pro každý cyklus. Perioda jednoho cyklu je nastavena na 5 sekund, ovšem změnou nastavení v konfiguračním souboru *MainConfig_server.txt* lze tuto periodu modifikovat. Zobrazení dat na informačním displeji již bylo ukázáno na obr. 2.14.

3.2.2 Rozbor scénáře podpětí

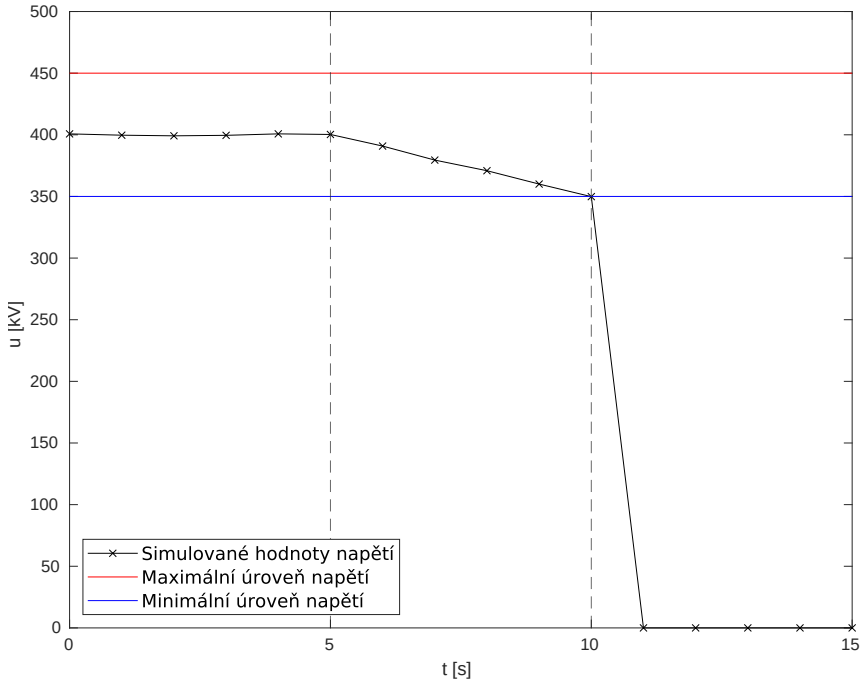
V kapitole 2.4.2 byl popsán tento scénář, který odpovídá postupnému poklesu energie. Na obr. 3.2 můžeme vidět průběh scénáře podpětí prostřednictvím informačního displeje. Nejprve vidíme počáteční klidový stav (3.2a). Poté je spuštěna simulace podpětí s projevením poklesu napěťové úrovně (3.2b). A nakonec vidíme stav po reakci ochranných prvků (3.2c).



(a) (b) (c)

Obr. 3.2: Průběh scénáře podpětí.

Znázornění simulovaných hodnot můžeme vidět na obr. 3.3. Černá křivka znázorňuje simulované hodnoty napětí, červená hladina určuje maximální a modrá minimální povolenou úroveň napětí. V čase 5 sekund byl spuštěn scénář podpětí. Následně můžeme zaznamenat pokles napěťové úrovně až do doby, kdy překročí nejmenší povolenou úroveň tj. v čase 10 sekund. V ten moment zareagují ochranné prvky, které transformátor odpojí. Program je přizpůsoben ke změně sklonu křivky či minimální úrovně k sepnutí ochranných prvků.

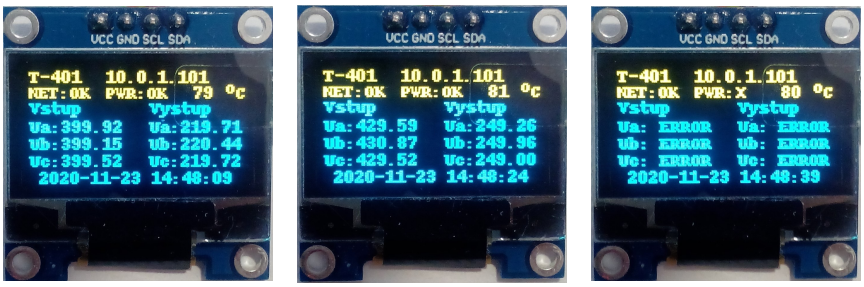


Obr. 3.3: Simulované hodnoty během scénáře podpětí.

Jak již bylo zmíněno, při sepnutí ochranných prvků jsou vysílána spontánní data. Jedná se o zprávu typu 4 (M_DP_TA_1) dle přílohy E, která obsahuje dvoubitové hodnoty stavů. Zde došlo ke změně ochranného prvku hlavního jističe (IOA=4000) a stavu poplachové hodnoty (IOA=4003), která udává poplach pro stav „Podpětí“. Další zpráva typu 2 (M_SP_TA_1) obsahuje jednobitové hodnoty. V tomto případě došlo ke změně hlavního jističe (IOA=5000) a spuštění alarmu (IOA=5003), viz obr. C.5. Velikost zpráv spontánních a periodických je stejná (101 B).

3.2.3 Rozbor scénáře přepětí

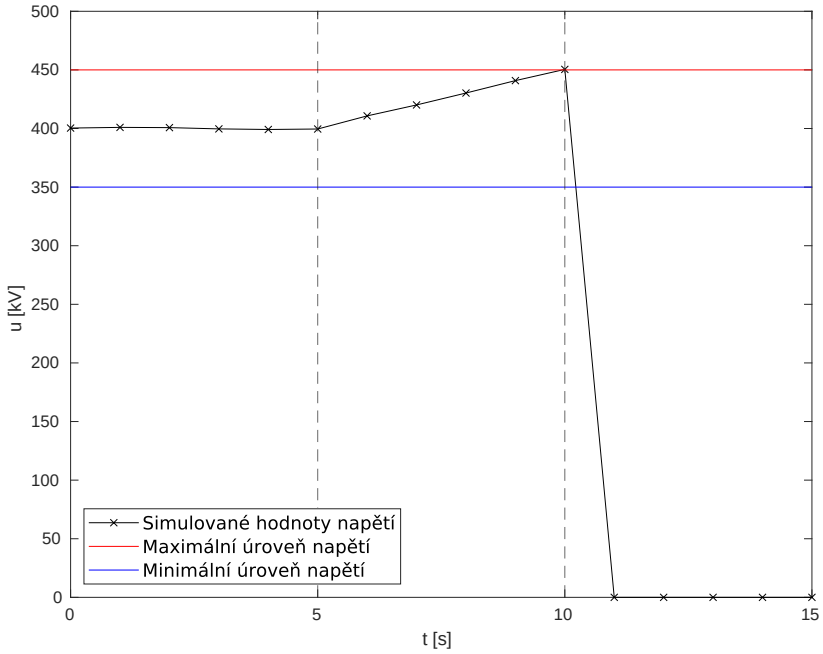
Jak již bylo řečeno v kapitole 2.4.2, tento scénář odpovídá postupnému přírůstku energie. Na obrázku 3.4 je možné vidět průběh tohoto scénáře prostřednictvím informačního displeje. Obdobně jako u předchozího scénáře můžeme vidět počáteční stav (3.4a). Následně je spuštěna simulace přepětí, která způsobuje postupný nárůst napěťové úrovně (3.4b). A nakonec vidíme stav po reakci ochranných prvků (3.4c).



(a) (b) (c)

Obr. 3.4: Průběh scénáře přepětí.

Obrázek 3.5 znázorňuje simulované hodnoty serverem během scénáře přepětí. V čase 5 sekund byl spuštěn scénář přepětí. Následně můžeme zaznamenat nárůst napěťové úrovně až do doby, kdy překročí maximální povolenou úroveň (v čase 10 sekund), a reakci ochranných prvků.

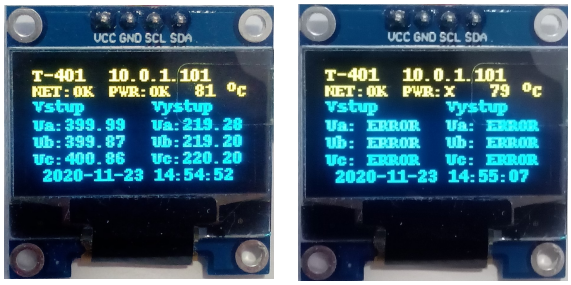


Obr. 3.5: Simulované hodnoty během scénáře přepětí.

Při sepnutí ochranných prvků jsou vysílána spontánní data. Jedná se o zprávu typu 4 a 2 dle přílohy E. V tomto případě došlo ke změně ochranného prvku hlavního jističe (IOA=4000) a stavu poplachové hodnoty (IOA=4002), která udává poplach pro stav „Přepětí“. Dále došlo ke změně hlavního jističe (IOA=5000) a spuštění alarmu (IOA=5003), viz obr. C.5.

3.2.4 Rozbor scénáře výpadku

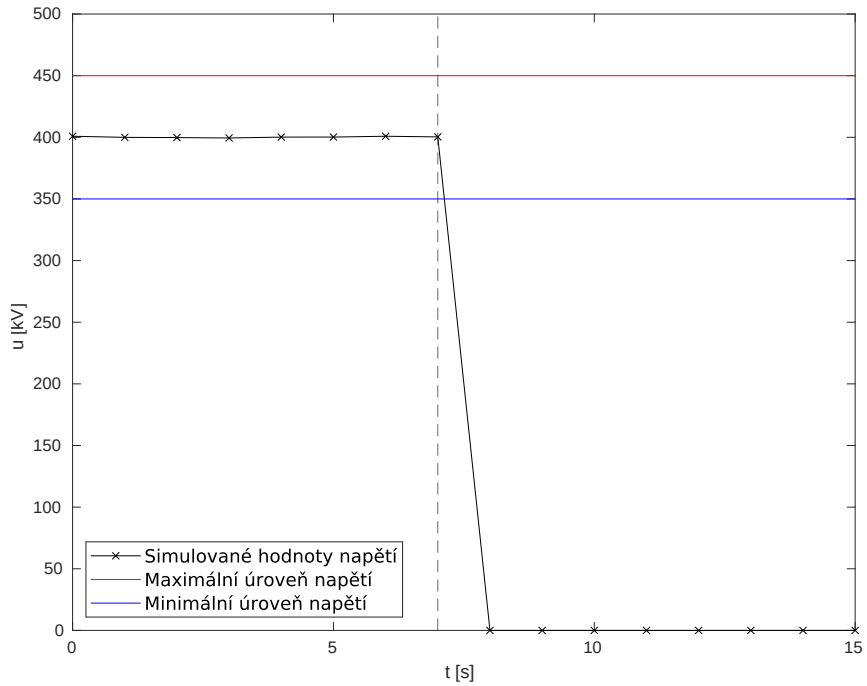
Scénář výpadku odpovídá okamžitému ukončení funkce stanice. Obr. 3.6 zobrazuje průběh tohoto scénáře prostřednictvím informačního displeje. Obdobně jako u předchozích scénářů vidíme počáteční klidový stav (3.6a). Následně je vyvolán výpadek na zařízení s okamžitou reakcí ochranných prvků (3.6b).



(a) (b)

Obr. 3.6: Průběh scénáře výpadku.

Obrázek 3.7 znázorňuje generované hodnoty a celý průběh výpadku. V čase 7 sekund byla spuštěna simulace výpadku. Dochází k okamžitému bezpečnostnímu vypnutí stanice. Stejně jako v ostatních případech stanice i nadále komunikuje s klientskou (dohledovou) stanicí.



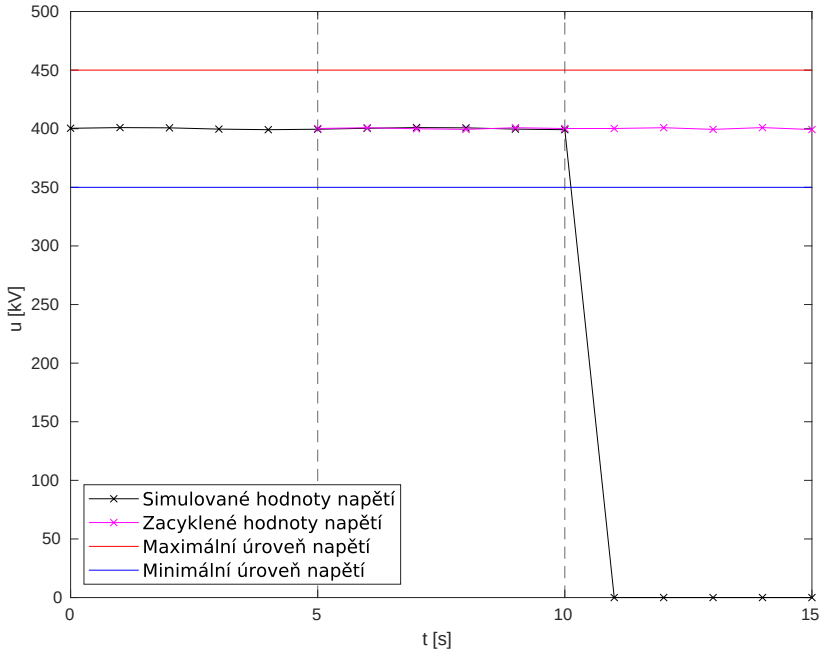
Obr. 3.7: Simulované hodnoty během scénáře výpadku.

Při bezpečnostním vypnutí jsou také vysílána spontánní data. Jedná se opět o zprávy typu 4 a 2 dle přílohy E. V tomto případě dochází ke změně ochranného prvku hlavního jističe (IOA=4000) a stavu poplachové hodnoty (IOA=4004), která udává poplach pro stav „Zkrat“. Dále dochází ke změně hodnoty hlavního jističe (IOA=5000), změně ochranného relé (IOA=5002) a spuštění alarmu (IOA=5003), viz obr. C.7.

3.2.5 Rozbor útoku vyřazení lokální kontroly stanice

Tento scénář byl popsán v kapitole 2.4.3. Jedná se o útok, který naruší lokální kontrolu a ovládání stanice. Průběh tohoto scénáře prostřednictvím informačního displeje se nijak neliší od scénáře standardního chování, viz obr. 2.14.

Pro lepší přehlednost obr. 3.8 znázorňuje simulované hodnoty během tohoto útoku. Obdobně jako v předchozích scénářích, černá křivka představuje skutečně simulovaná data serverem. Útočník v čase 5 sekund spustí simulaci zacyklených dat, které jsou zobrazeny na informačním displeji a odesílány dispečernímu středisku. Tato data jsou v grafu reprezentována fialovou křivkou. Nakonec v čase 10 sekund útočník odpojí stanici od rozvodné sítě.



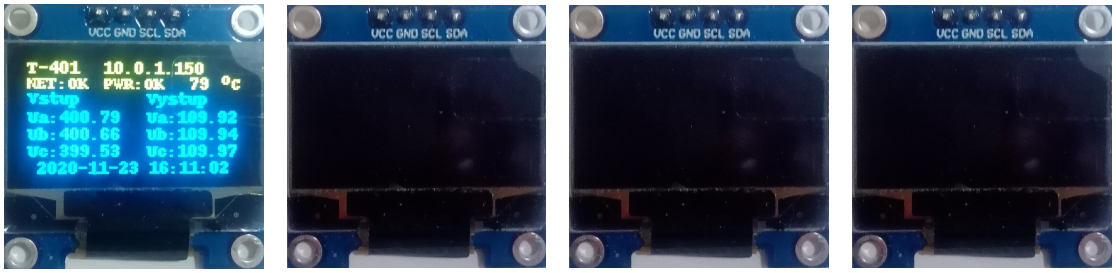
Obr. 3.8: Simulované hodnoty během útoku vyřazení lokální kontroly.

Při lokálním vypnutí stanice útočníkem jsou také vysílána spontánní data. Opět se jedná o zprávy typu 4 a 2 dle přílohy E. V tomto případě dochází ke změně ochranného prvku odpojovače (IOA=4001) a k události změně odpojovače (IOA=5001), viz obr. C.8.

3.2.6 Rozbor scénáře útoku na elektrárny

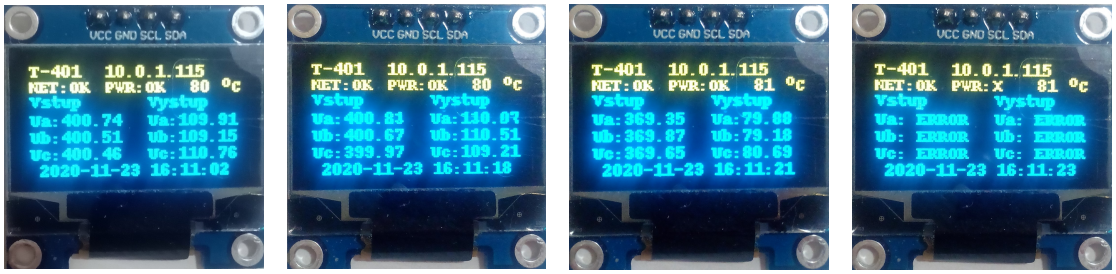
Posledním scénářem chování polygonu je útok na elektrárny. Jedná se o jediný scénář, který nelze reprezentovat pomocí jednoho transformátoru stanice. V rámci tohoto scénáře bylo zaznamenáno chování dvou stanic. Jedna představuje elektrárnu, která je cílem útoku, druhá představuje rozvodnu na ní závislou.

Při tomto scénáři dochází v důsledku útoku ke kritickému poškození elektrárny. Obrázky 3.9 a 3.10 zobrazují průběhy tohoto scénáře pro elektrárnu a rozvodnu prostřednictvím informačních displejů. Nejprve lze vidět stav před zahájením útoku (3.9a a 3.10a). Poté dochází ke zmíněnému poškození elektrárny (3.9b) s následným poklesem napěťové úrovně závislé rozvodny (3.10c). A nakonec vidíme stav, ve kterém ani jedna ze zmíněných stanic není provozuschopná (3.9d a 3.10d).



(a) (b) (c) (d)

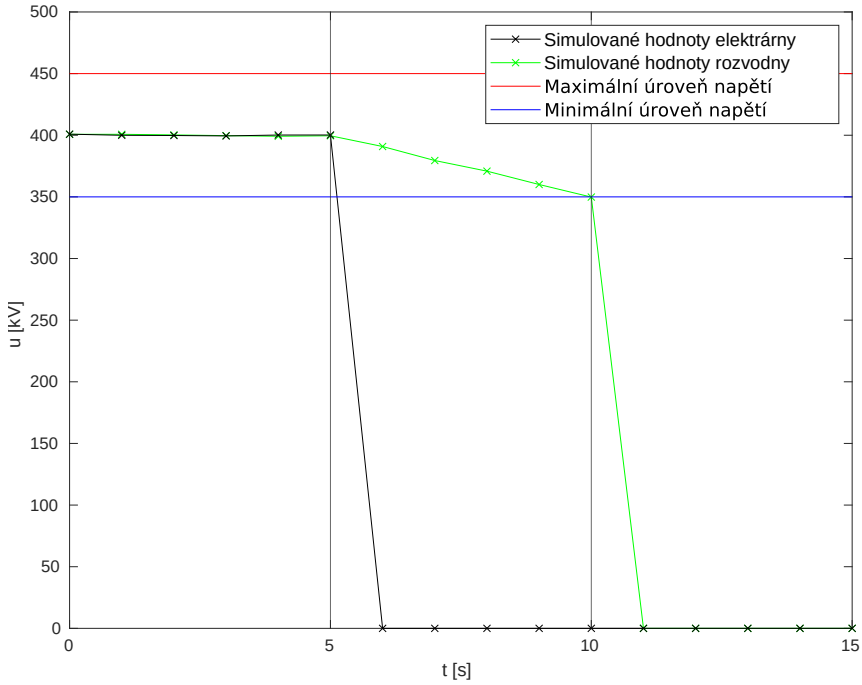
Obr. 3.9: Průběh scénáře útoku na elektrárnu – displej elektrárny.



(a) (b) (c) (d)

Obr. 3.10: Průběh scénáře útoku na elektrárnu – displej rozvodny.

Obrázek 3.11 znázorňuje simulované hodnoty elektrárnou (černá křivka) a rozvodny (zelená křivka) během tohoto scénáře. V čase 5 sekund došlo k poškození elektrárny. Následně můžeme zaznamenat pokles napěťové úrovně rozvodny až do doby, kdy překročí minimální povolenou úroveň (v čase 10 sekund) s reakcí ochranných prvků, které stanici odpojí od sítě.



Obr. 3.11: Simulované hodnoty elektrárnou a rozvodnou během scénáře útoku.

Závěr

Náplní diplomové práce bylo obeznámit se s principem energetické soustavy ČR, včetně prostudování standardů IEC 60870 a IEC 61850. Této problematice je věnována první část teorie, která popisuje již zmíněné standardy, uvádí důvody jejich vzniku a krátce shrnuje jejich historii. Dále jsou popsány normy, ze kterých tyto standardy vychází, a architektury protokolů vzhledem k modelu ISO/OSI. Také jsou zde popsány vlastnosti a především způsoby, kterými se jednotlivé protokoly utváří, a jejich možnosti komunikace.

V rámci praktické části práce bylo vytvořeno programové řešení reprezentující jednotlivé stanice polygonu. Toto řešení bylo detailně rozebráno včetně popisu jeho spuštění. Dále byla vytvořena a detailně popsána webová aplikace pro správu stanic. Rovněž byla ukázána implementace tohoto ovládacího rozhraní, včetně rozboru jednotlivých funkcí a způsobu ovládání. Poté byl do polygonu přenosové soustavy implementován a následně i otestován standard IEC 61850-80-1, který zajišťuje převod dat mezi protokoly standardu IEC 61850 a protokolem IEC 60870-5-104. Také byly definovány scénáře chování stanic. Mezi tyto scénáře patří standardní provoz, který reprezentuje klasické chování stanice, scénáře kritických stavů (podpětí, přepětí, výpadek) a nakonec i scénáře útoků na infrastrukturu polygonu.

Následně byly zobrazeny a popsány zprávy pro navazování a ukončování spojení mezi dohledovou (klientskou) a serverovou stanicí. Rovněž byla ukázána zpráva pro synchronizaci času včetně časového razítka, které je pro dispečerní řízení klíčové. Dále došlo k rozboru komunikace mezi webovou aplikací (respektive webovým serverem) a stanicemi polygonu přenosové soustavy.

Poslední část práce byla věnována samotnému testování implementovaných scénářů. Jednotlivé scénáře byly v důležitých bodech simulace zaznamenány prostřednictvím informačního displeje a zároveň i graficky znázorněny pomocí grafu simulovaných hodnot. Následně byly zobrazeny a rozebrány zprávy simulované stanicí během těchto scénářů.

Výsledky diplomové práce byly prezentovány na konferenci „Student EEICT 2021“ a v budoucnu dojde k propojení tohoto polygonu přenosové soustavy s Kybernetickou arénou a Kyber-fyzickým dvojčetem městské infrastruktury vyvíjené na ústavu telekomunikací.

Literatura

[1] Přenosová a distribuční soustava - 1. část | E.ON Distribuce. *Provozujeme distribuční síť elektřiny a plynu | E.ON Distribuce* [online]. Copyright © 2020 E.ON Distribuce, a.s. Distributor elektřiny a plynu [cit. 18.10.2020]. Dostupné z URL: <https://www.eon-distribuce.cz/clanek/prenosova-distribucni-soustava-1-cast>

[2] Přenosová soustava elektrické energie. *Energetika.tzb* [online]. Copyright © 2013 [cit. 18.10.2020]. Dostupné z URL: <https://energetika.tzb-info.cz/elektroenergetika/13676-prenosova-soustava-elektricke-energie>

[3] Počet elektráren v Česku se za sto let zvýšil šestkrát | iUHLI.cz. *iUHLI.cz* [online]. Copyright © 2018 pHmedia Czech Republic, s.r.o. [cit. 18.10.2020]. Dostupné z URL: <https://iuhli.cz/pocet-elektraren-v-cesku-se-za-sto-let-zvysil-sestkrat/>

[4] MAKHIJA, J; SUBRAMANYAN, L.R. *Comparison of protocols used in remote monitoring: DNP 3.0, IEC 870-5-101 and Modbus.* Electronics Systems Group, IIT Bombay, India, Tech. Rep, Copyright © 2003.

[5] CLARKE, G; REYNDERS, D; WRIGHT, E. *Modern SCADA protocols: DNP3, 60870.5 and relatedsystems.* [online]. Copyright © 2004 [cit. 18.10.2020]. Dostupné z URL: <https://www.julesbartow.com/Pictures/RF/Practical_modern_SCADA_protocols_-_dnp3,_60870-5_and_Related_Systems.pdf>

[6] Co je to SCADA?. *PROMOTIC SCADA Visualization software* [online]. Copyright © MICROSYS, spol. s.r.o. [cit. 21.10.2020]. Dostupné z URL: <https://www.promotic.eu/cz/pmdoc/WhatIsPromotic/WhatIsScada.htm>

[7] Training Videos Drivers. *Brodersen RTU PLC Datalogger Simply just Nr. 1* [online]. Copyright © 2020 [cit. 21.10.2020]. Dostupné z: <http://brodersen.com/wordpress/wp-content/uploads/BS_RTU32_IEC60870Config.pdf>

[8] MATOUŠEK, P. *Description and analysis of IEC 104 Protocol.* [online]. Copyright © 2017 [cit. 21.10.2020]. Dostupné z URL: <http://www.fit.vutbr.cz/research/view_pub.php.cs?id=11570>

[9] Komunikační protokoly pro dálkové ovládání IEC/ISO 60870-5. *Automa* [online]. Copyright © 2010 [cit. 29.10.2020]. Dostupné z URL: <http://automa.cz/cz/casopis-clanky/komunikacni-protokoly-pro-dalkove-ovladani-iec/iso-60870-5-2010_02_40552_5799/>

[10] UZAIR, M., *Communication methods (Protocols, format and language) for the substation automation and control* [online], [cit. 29.10.2020]. Dostupné z URL: <https://www.eng.uwo.ca/people/tsidhu/Documents/project%20report%20Uzair.pdf>

[11] Systémy a zařízení pro dálkové ovládání – Část 5-104: Přenosové protokoly – Síťový přístup pro IEC 60870-5-101 používající normalizované transportní profily. *ČSN EN 60870-5-104 (334650).* Copyright © 2007 [cit. 29.10.2020].

[12] Understanding IEC-60870-5-104 Traffic Patterns in SCADA Networks. *IDA - Department of Computer and Information Science* [online]. Copyright © 2018 [cit. 1.11.2020]. Dostupné z: <https://www.ida.liu.se/labs/rtslab/publications/2018/CPSS_2018.pdf>

[13] Beckhoff Information System - English. *Beckhoff Information System - German* [online]. Copyright © 2020 [cit. 1.11.2020]. Dostupné z: <https://infosys.beckhoff.com/english.php?content=../content/1033/tcplclibiec870_5_104/html/tcplclibiec870_5_104_objref_overview.htm&id>

[14] IEC 104 - encrypted communication. *WinCC OA* [online]. Copyright © ETM professional control 2015 [cit. 1.11.2020]. Dostupné z URL: <https://www.winccoa.top/help316p006/Treiber_IEC/iec_104_security.htm>

[15] What is an SSL TLS X.509 Certificate? | Venafi. *Machine Identity Management Solutions | Venafi* [online]. Copyright © 2020 [cit. 1.11.2020]. Dostupné z URL: <https://www.venafi.com/blog/what-ssltls-x509-certificate>

[16] MATOUŠEK, P. *Description of IEC 61850 Communication.* [online]. Copyright © 2018 [cit. 1.11.2020]. Dostupné z URL: <https://www.fit.vut.cz/research/publication-file/11832/TR-61850.pdf>

[17] IEC 61850 Communication Networks and Systems In Substations. *GE Grid Solutions* [online]. Copyright © Ig [cit. 9.11.2020]. Dostupné z URL: <https://www.gegridsolutions.com/multilin/journals/issues/spring09/iec61850.pdf>

[18] IEC 61850 Stack Overview. *Triangle MicroWorks* [online]. Copyright © 2013 [cit. 9.11.2020]. Dostupné z URL: <https://www.trianglemicroworks.com/products/source-code-libraries/iec-61850-scl-pages>

[19] VLADYKA, P. *Soubor norem pro komunikaci v energetice s velkým potenciálem výhod.* [online]. Copyright ©US 2010 [cit. 9.11.2020]. Dostupné z URL: <http://automa.cz/Aton/FileRepository/pdf_articles/40771.pdf>

[20] IEC TS 61850-80-1:2016. *Communication networks and systems for power utility automation – Part 80-1: Guideline to exchanging information from a CDC-based data model using IEC 60870-5-101 or 60870-5-104.*

[21] SCHWARZ, K. *Comparation of IEC 60870-5-101/-103/-104, DNP3, and IEC60870-6-TASE.2 with IEC 61850.* [online]. Copyright © 2017 [cit. 2.12.2020]. Dostupné z URL: <http://upload.scc-online.de/files/2019-02-10_154953/Comparison_DNP_60870_61850_2012-07-21_p.pdf>

[22] MikroTik Routers and Wireless. *MikroTik Routers and Wireless* [online]. Copyright © 2020 [cit. 12.11.2020]. Dostupné z URL: <https://mikrotik.com/>

[23] Raspberry Pi Downloads - Software for the Raspberry Pi. *Teach, Learn, and Make with Raspberry Pi – Raspberry Pi* [online]. Copyright © 2020 [cit. 12.11.2020]. Dostupné z URL: <https://www.raspberrypi.org/downloads/>

[24] Raspberry Pi 3 Model B+ 64-bit 1GB RAM. *RPishop.cz* [online]. Copyright © Copyright 2020 rpishop.cz. [cit. 12.11.2020]. Dostupné z URL: <https://rpishop.cz/raspberry-pi-3b/896-raspberry-pi-3-model-b-plus-64-bit-1gb-ram-713179640259.html>

[25] IIC I2C OLED display 0,96"128x64 Bílý | arduino-shop.cz. *Arduino-shop.cz: VELKOOBCHOD, MALOOBCHOD S ARDUINEM* [online]. Copyright © Copyright ECLIPSERA s.r.o. [cit. 12.11.2020]. Dostupné z URL: <hhttps://arduino-shop.cz/arduino/1569-iic-i2c-oled-display-0-96-128x64-bily.html>

[26] Downloads | LibIEC61850 / LibIEC60870-5. *Open source librariesfor IEC 61850 and IEC 60870.* [online]. Copyright © 2020 [cit. 12.11.2020]. Dostupné z URL: <https://libiec61850.com/libiec61850/downloads/>

[27] Lib60870-C: source code library for the IEC 60870-5-101/104 protocols. *Mz-automation* [online]. Copyright © 2020 [cit. 12.11.2020]. Dostupné z: <https://support.mz-automation.de/doc/lib60870/latest/index.html>

[28] Česká energetická přenosová soustava: Kodex přenosové soustavy. *ČEPS* [online]. Copyright © 2016 [cit. 10.2.2021]. Dostupné z: <https://www.ceps.cz/cs/kodex-ps>

[29] HARMAN, Dominik. *Účinnost chladících systémů transformátorů přenosové soustavy* [online]. Copyright © 2016 [cit. 10.2.2021]. Dostupné z: <https://otik.zcu.cz/bitstream/11025/22930/1/dp_harman_dominik.pdf>

[30] IEC 60076-7:2018. *Power transformers: Part 7: Loading guide for oil-immersed power transformers.*

[31] Elektrická přenosová soustava. *Wikipedie* [online]. Copyright © 2018 [cit. 10.2.2021]. Dostupné z: <https://cs.wikipedia.org/wiki/Elektrick%C3%A1_p%C5%99enosov%C3%A1_soustava>

[32] Havarijní plán k řešení stavů nouze v energetice. *KRÁLOVOPOLSKÁ, a.s.* [online]. Copyright © 2016 [cit. 02.12.2020]. Dostupné z: <https://www.kralovopolska.cz/data/energetika/nove/Havarijni_plan_Rozvod_elektricke_energie.pdf>

[33] ŠÍR, K. *Ochrana české přenosové soustavy před teroristickým útokem.* [online]. Copyright © 2015 [cit. 10.2.2021]. Dostupné z URL: <https://is.muni.cz/th/qxqr5/Sir_Krystof_BC.pdf>

[34] TOMÁŠKOVÁ, K. *Rizika a dopady black-outu v ČR.* [online]. Brno, 2019 [cit. 10.2.2021]. Dostupné z URL: <https://www.vutbr.cz/www_base/zav_prace_soubor_verejne.php?file_id=192348> Bakalářská práce. Vysoké učení technické v Brně, Fakulta strojního inženýrství, Energetický ústav. Vedoucí práce Martin Lisý.

[35] JAKESCHOVÁ, K. *Kybernetické útoky a energetický sektor.* [online]. Brno, 2019 [cit. 10.2.2021]. Dostupné z URL: <https://is.muni.cz/th/lvlqc/Diplomova_prace_-_Jakeschova.pdf>

Seznam symbolů, veličin a zkratek

ACSI	Abstract Communications Service Interface
ASDU	Application-layer Service Data Unit
CA	Certification Authority
CASDU	Common Adress Of ASDU
CDA	Běžný datový atribut
CDC	Change Data Capture
COT	Cause Of Transmission
DA	Datový Atribut
DDOS	Distributed Denial Of Service
DNP3	Distributed Network Protocol 3
DO	Datový Objekt
DPS	Double Point Status
EPA	Enhanced Performance Architecture
FC	Funkční omezení
HT	High Temperature
HTTP	Hypertext Transfer Protocol
IED	Intelligent Electronic Devices
IP	Internet Protocol
JE	Jaderná Elektrárna
LCD	Liquid Crystal Display
LD	Logické zařízení
LN	Logický Uzel
LT	Low Temperature
MMS	Multimedia Messaging Service
MV	Measured Value
OA	Originator Adress
OLED	Organic Light Emitting Diode
PE	Parní Elektrárna
PD	Physical device
PLC	Power Line Communication
PE	Přenosová Soustava
PPE	Paroplynová Elektrárna
PVE	Přečerpávací Vodní Elektrárny
SAS	Substation Automation System
SCADA	Supervisory Control And Data Acquisition
SCSM	System Center Service Manager
SQ	Sequence Number

SSH	Secure Shel
SSL	Secure Sockets Layer
SPS	Single Point Status
TCP	Transmission Control Protocol
TLS	Transport Layout Security
USB	Universal Serial Bus
VE	Vodní Elektrárna
VM	Výrobní Modul
WAN	Wide Area Network

Seznam příloh

A Veškeré použité programy

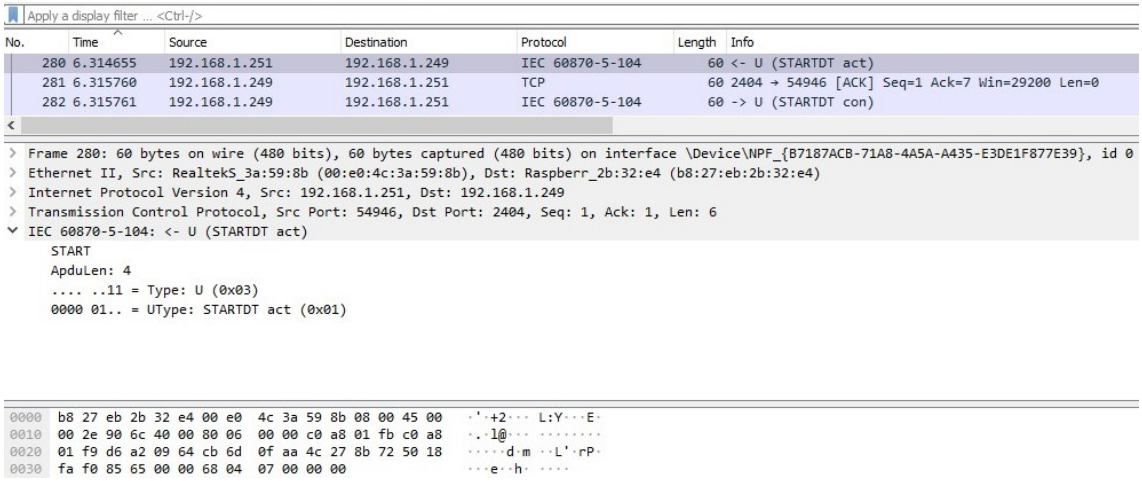
V příloze jsou s prací odevzdány i zdrojové soubory programu simulující stanice polygonu PS, zdrojové soubory webové aplikace a vytvořená knihovna *CDC_to_ASDU.h*.

Zdrojové soubory stanice polygonu PS:
<https://drive.google.com/drive/folders/1XoD3iQesTyqD_ZvIiq6ml5gtJVOFrDTJ>

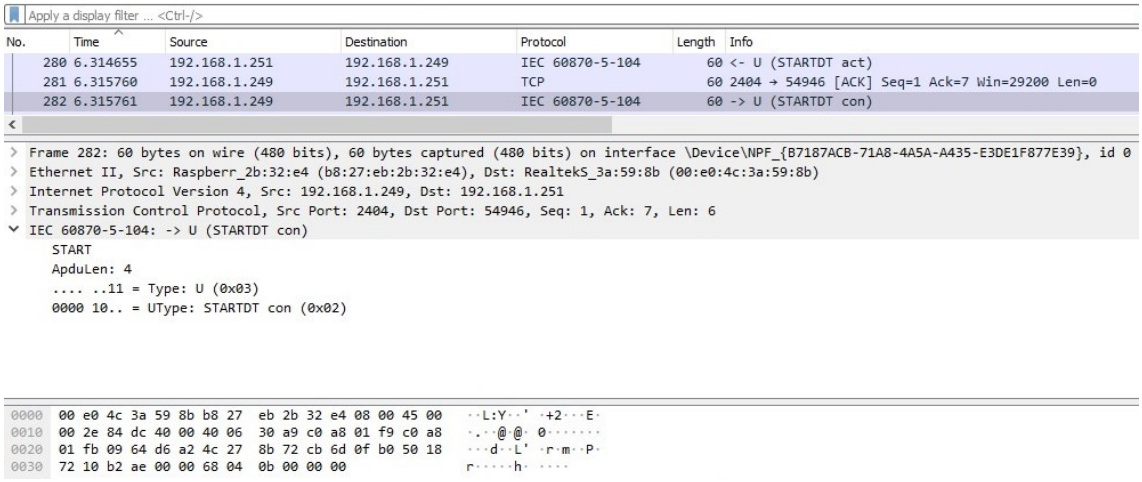
Zdrojové soubory webové aplikace:
<https://drive.google.com/drive/folders/1TI0vTS0_KSqbamjdsZxX7I_os9h7gTcu>

Knihovna *CDC_to_ASDU.h*:
<https://drive.google.com/file/d/1qJSJ8NYy8xrvA3NMzElAuCUjwARO59DE/>

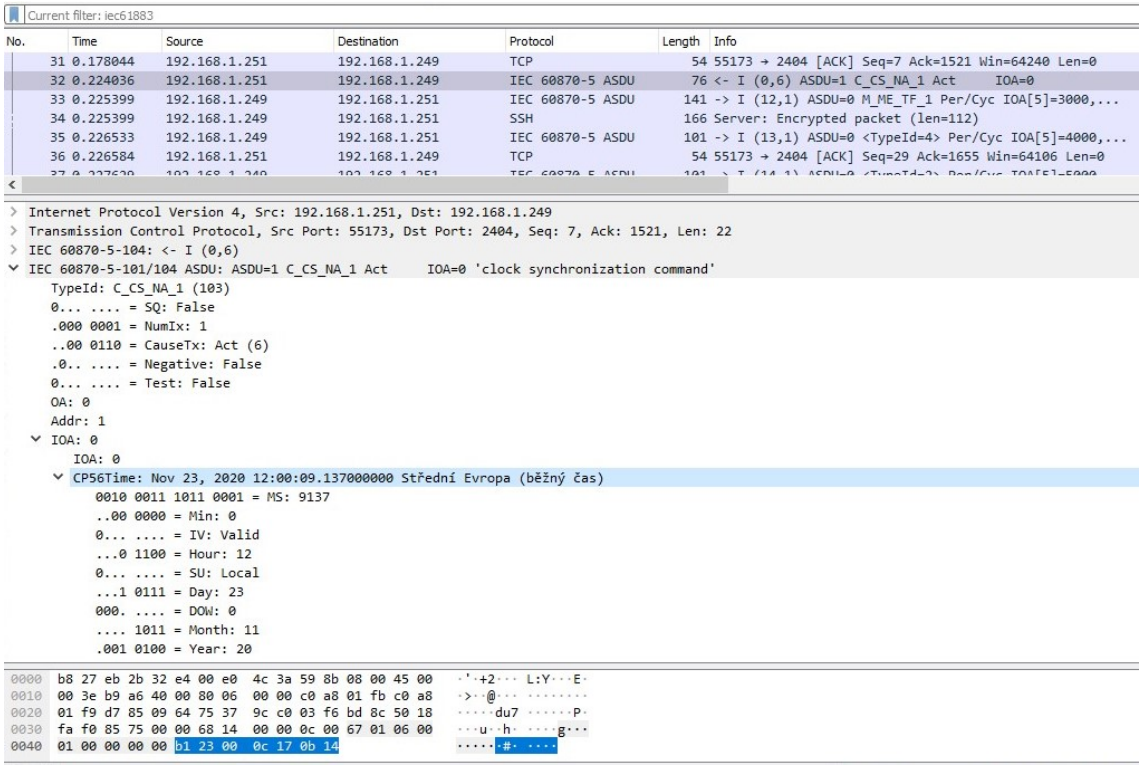
B Záznamy základní komunikace stanic polygonu



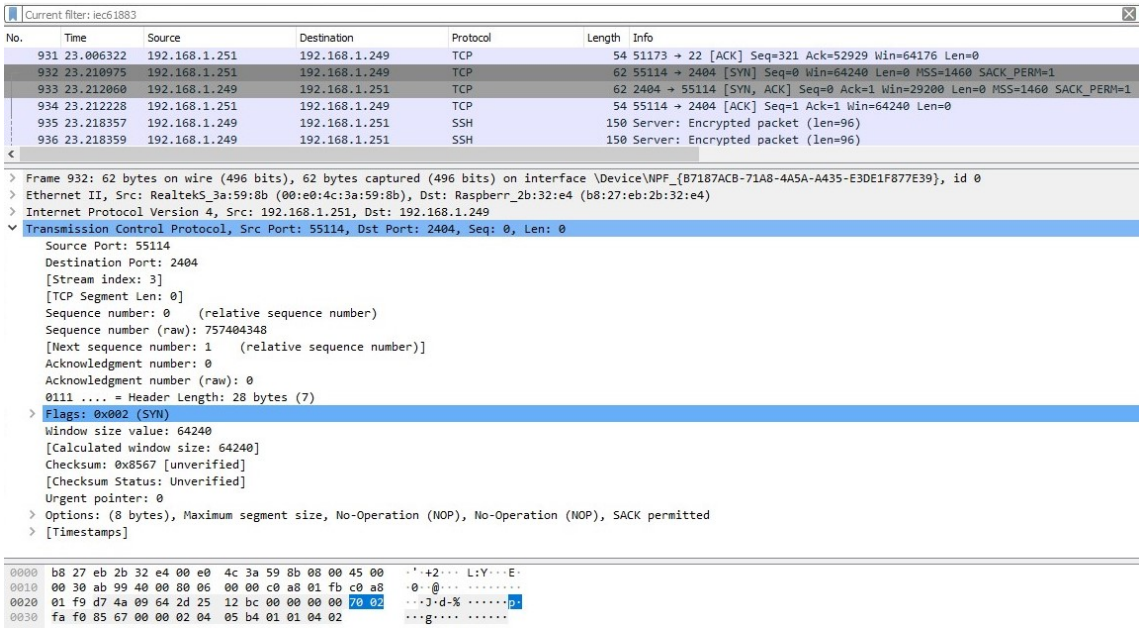
Obr. B.1: Zpráva StartDT_act.



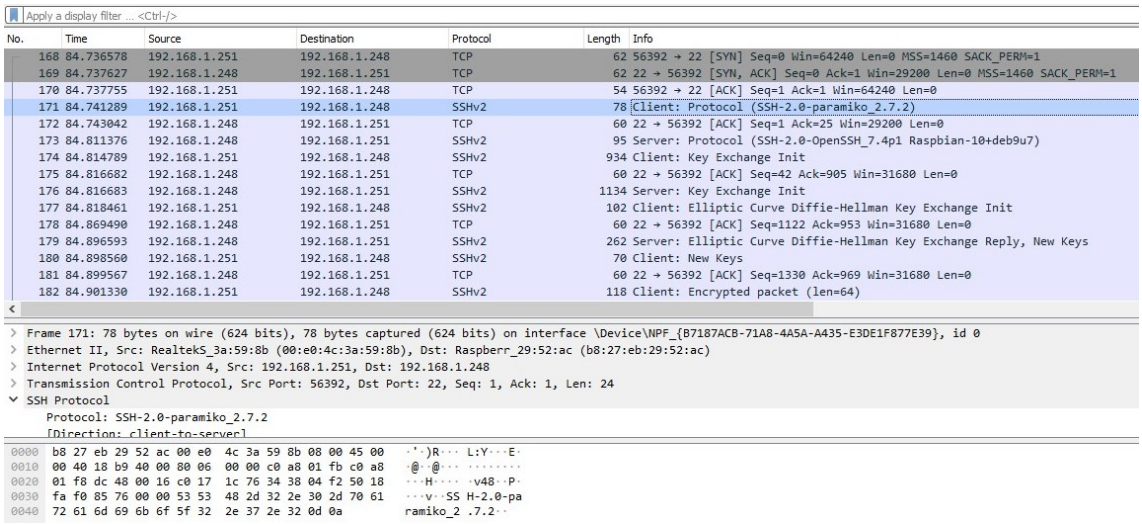
Obr. B.2: Zpráva StartDT_con



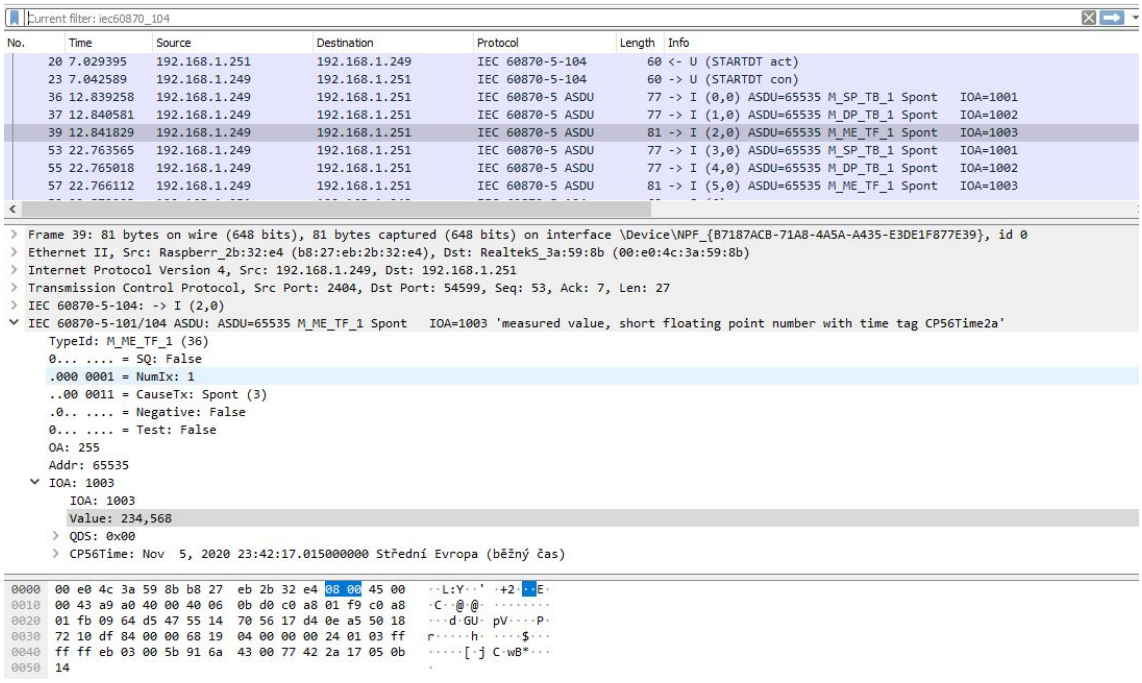
Obr. B.3: Zpráva synchronizace času.



Obr. B.4: Záznam ukončení TCP spojení mezi klientem a serverem.

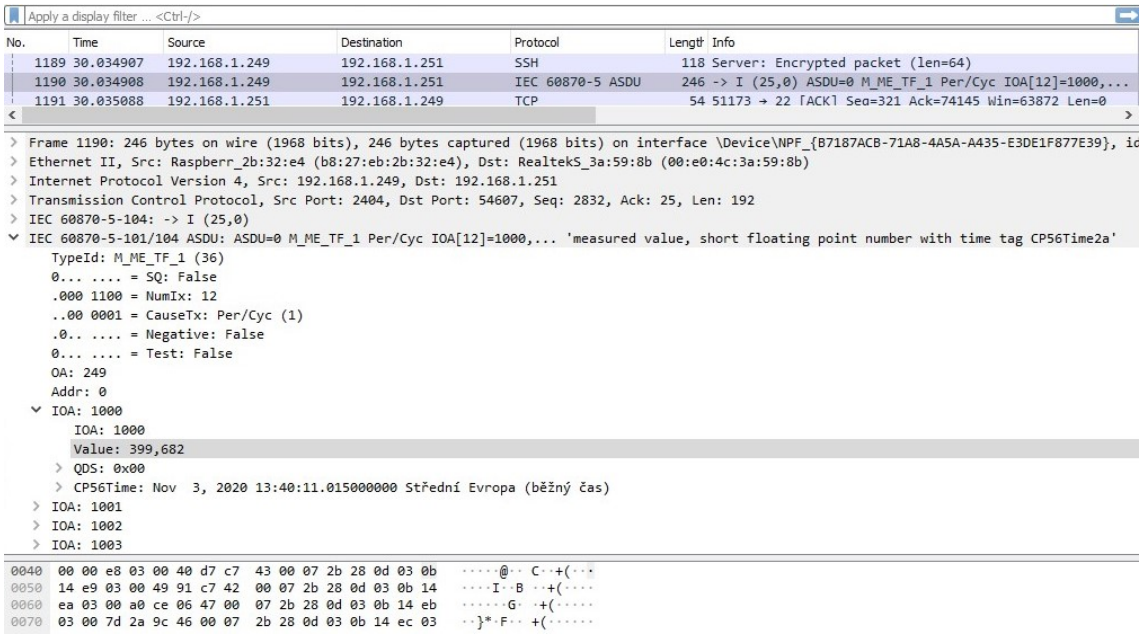


Obr. B.5: Záznam komunikace mezi webovým serverem a stanicí polygonu.

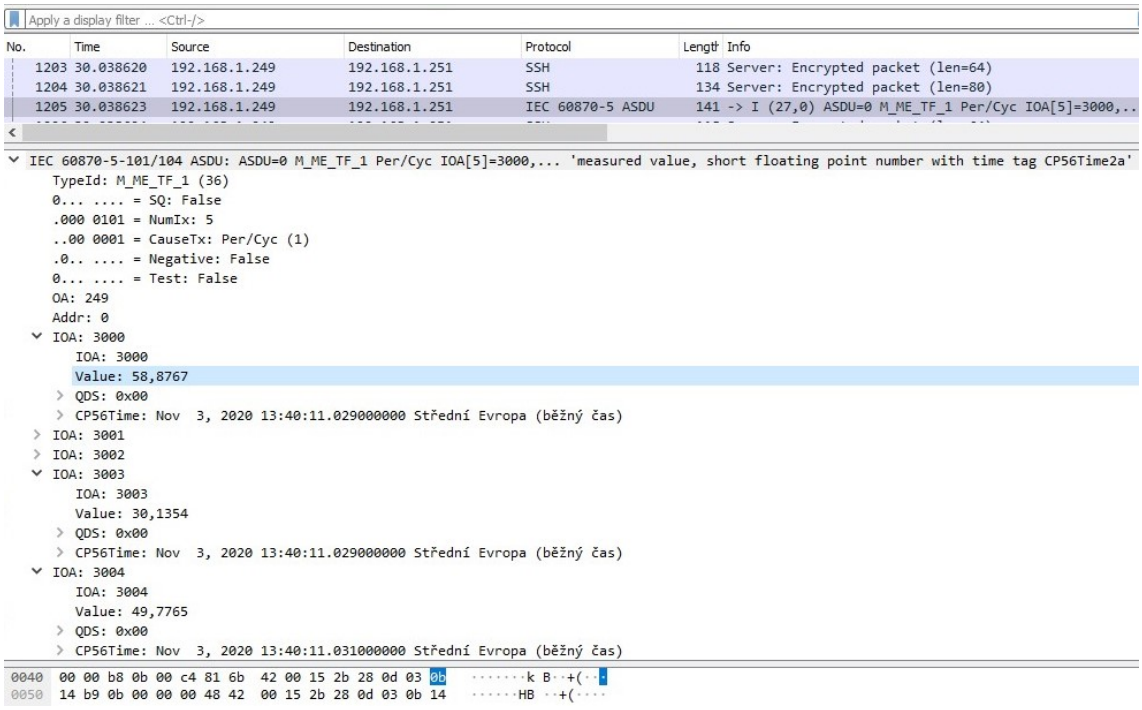


Obr. B.6: Záznam komunikace mapovacího modulu.

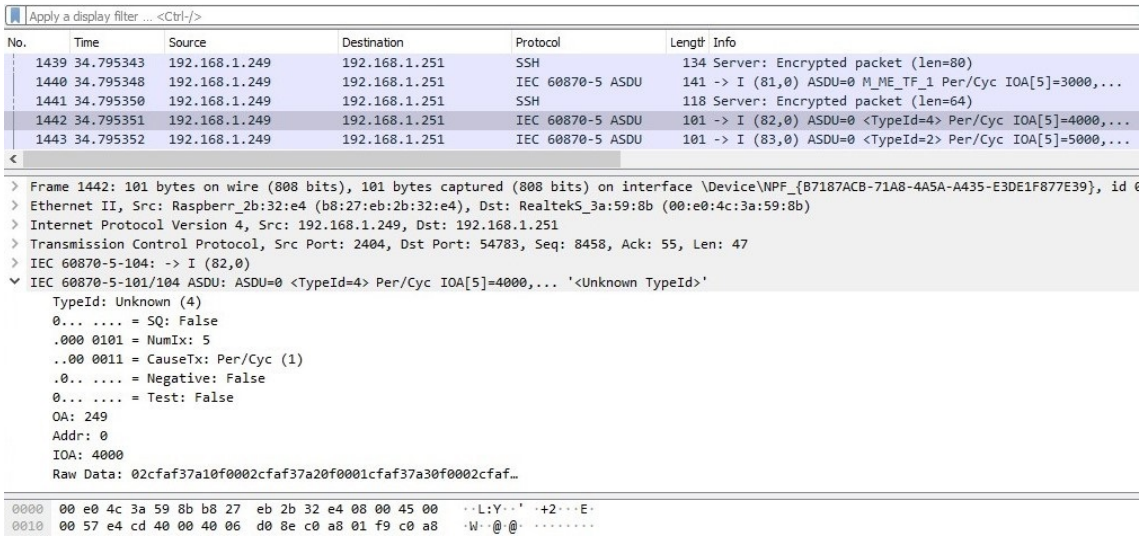
C Záznamy komunikace a logovací soubory během scénářů



Obr. C.1: Periodická zpráva vstupních veličin.



Obr. C.2: Periodická zpráva teplot a frekvence.



Obr. C.3: Periodická zpráva stavu ochranných prvků a poplachů.

```
2020-11-23 13:17:29 type(36) elements: 12
2020-11-23 13:17:29 IOA: 1000 value: 399.100342 with timestamp: 2020-11-03 15:01:48
2020-11-23 13:17:29 IOA: 1001 value: 99.766701 with timestamp: 2020-11-03 15:01:48
2020-11-23 13:17:29 IOA: 1002 value: 34454.539062 with timestamp: 2020-11-03 15:01:48
2020-11-23 13:17:29 IOA: 1003 value: 19956.759766 with timestamp: 2020-11-03 15:01:48
2020-11-23 13:17:29 IOA: 1004 value: 400.606659 with timestamp: 2020-11-03 15:01:48
2020-11-23 13:17:29 IOA: 1005 value: 99.698715 with timestamp: 2020-11-03 15:01:48
2020-11-23 13:17:29 IOA: 1006 value: 34561.011719 with timestamp: 2020-11-03 15:01:48
2020-11-23 13:17:29 IOA: 1007 value: 20018.429688 with timestamp: 2020-11-03 15:01:48
2020-11-23 13:17:29 IOA: 1008 value: 400.363831 with timestamp: 2020-11-03 15:01:48
2020-11-23 13:17:29 IOA: 1009 value: 99.904190 with timestamp: 2020-11-03 15:01:48
2020-11-23 13:17:29 IOA: 1010 value: 34611.250000 with timestamp: 2020-11-03 15:01:48
2020-11-23 13:17:29 IOA: 1011 value: 20047.527344 with timestamp: 2020-11-03 15:01:48
2020-11-23 13:17:29 type(36) elements: 12
2020-11-23 13:17:29 IOA: 2000 value: 219.625885 with timestamp: 2020-11-03 15:01:48
2020-11-23 13:17:29 IOA: 2001 value: 99.752480 with timestamp: 2020-11-03 15:01:48
2020-11-23 13:17:29 IOA: 2002 value: 18957.712891 with timestamp: 2020-11-03 15:01:48
2020-11-23 13:17:29 IOA: 2003 value: 10980.686523 with timestamp: 2020-11-03 15:01:48
2020-11-23 13:17:29 IOA: 2004 value: 219.595871 with timestamp: 2020-11-03 15:01:48
2020-11-23 13:17:29 IOA: 2005 value: 99.809372 with timestamp: 2020-11-03 15:01:48
2020-11-23 13:17:29 IOA: 2006 value: 18965.933594 with timestamp: 2020-11-03 15:01:48
2020-11-23 13:17:29 IOA: 2007 value: 10985.448242 with timestamp: 2020-11-03 15:01:48
2020-11-23 13:17:29 IOA: 2008 value: 219.378128 with timestamp: 2020-11-03 15:01:48
2020-11-23 13:17:29 IOA: 2009 value: 99.591110 with timestamp: 2020-11-03 15:01:48
2020-11-23 13:17:29 IOA: 2010 value: 18905.693359 with timestamp: 2020-11-03 15:01:48
2020-11-23 13:17:29 IOA: 2011 value: 10950.556641 with timestamp: 2020-11-03 15:01:48
2020-11-23 13:17:29 type(36) elements: 5
2020-11-23 13:17:29 IOA: 3000 value: 54.189873 with timestamp: 2020-11-03 15:01:48
2020-11-23 13:17:29 IOA: 3001 value: 50.000000 with timestamp: 2020-11-03 15:01:48
2020-11-23 13:17:29 IOA: 3002 value: 60.000000 with timestamp: 2020-11-03 15:01:48
2020-11-23 13:17:29 IOA: 3003 value: 29.202908 with timestamp: 2020-11-03 15:01:48
2020-11-23 13:17:29 IOA: 3004 value: 49.828636 with timestamp: 2020-11-03 15:01:48
2020-11-23 13:17:29 type(4) elements: 5
2020-11-23 13:17:29 IOA: 4000 value: 1.000000 with timestamp: 0001-48
2020-11-23 13:17:29 IOA: 4001 value: 2.000000 with timestamp: 0001-48
2020-11-23 13:17:29 IOA: 4002 value: 1.000000 with timestamp: 0001-48
2020-11-23 13:17:29 IOA: 4003 value: 1.000000 with timestamp: 0001-48
2020-11-23 13:17:29 IOA: 4004 value: 1.000000 with timestamp: 0001-48
2020-11-23 13:17:29 type(2) elements: 5
2020-11-23 13:17:29 IOA: 5000 value: 0.000000 with timestamp: 0001-48
2020-11-23 13:17:29 IOA: 5001 value: 0.000000 with timestamp: 0001-48
2020-11-23 13:17:29 IOA: 5002 value: 0.000000 with timestamp: 0001-48
2020-11-23 13:17:29 IOA: 5003 value: 0.000000 with timestamp: 0001-48
2020-11-23 13:17:29 IOA: 5004 value: 0.000000 with timestamp: 0001-48
```

Obr. C.4: Výpis logu pro standardní provoz.

```
2020-11-23 12:18:48 type(4) elements: 5
2020-11-23 12:18:48 IOA: 4000 value: 2.000000 with timestamp: 0003-07
2020-11-23 12:18:48 IOA: 4001 value: 2.000000 with timestamp: 0003-07
2020-11-23 12:18:48 IOA: 4002 value: 1.000000 with timestamp: 0003-07
2020-11-23 12:18:48 IOA: 4003 value: 2.000000 with timestamp: 0003-07
2020-11-23 12:18:48 IOA: 4004 value: 1.000000 with timestamp: 0003-07
2020-11-23 12:18:48 type(2) elements: 5
2020-11-23 12:18:48 IOA: 5000 value: 1.000000 with timestamp: 0003-07
2020-11-23 12:18:48 IOA: 5001 value: 0.000000 with timestamp: 0003-07
2020-11-23 12:18:48 IOA: 5002 value: 0.000000 with timestamp: 0003-07
2020-11-23 12:18:48 IOA: 5003 value: 1.000000 with timestamp: 0003-07
2020-11-23 12:18:48 IOA: 5004 value: 0.000000 with timestamp: 0003-07
```

Obr. C.5: Výpis logu pro scénář podpětí.

```
2020-11-23 12:22:50 type(4) elements: 5
2020-11-23 12:22:50 IOA: 4000 value: 2.000000 with timestamp: 0007-09
2020-11-23 12:22:50 IOA: 4001 value: 2.000000 with timestamp: 0007-09
2020-11-23 12:22:50 IOA: 4002 value: 2.000000 with timestamp: 0007-09
2020-11-23 12:22:50 IOA: 4003 value: 1.000000 with timestamp: 0007-09
2020-11-23 12:22:50 IOA: 4004 value: 1.000000 with timestamp: 0007-09
2020-11-23 12:22:50 type(2) elements: 5
2020-11-23 12:22:50 IOA: 5000 value: 1.000000 with timestamp: 0007-09
2020-11-23 12:22:50 IOA: 5001 value: 0.000000 with timestamp: 0007-09
2020-11-23 12:22:50 IOA: 5002 value: 0.000000 with timestamp: 0007-09
2020-11-23 12:22:50 IOA: 5003 value: 1.000000 with timestamp: 0007-09
2020-11-23 12:22:50 IOA: 5004 value: 0.000000 with timestamp: 0007-09
```

Obr. C.6: Výpis logu pro scénář přepětí.

```
2020-11-23 12:29:09 type(4) elements: 5
2020-11-23 12:29:09 IOA: 4000 value: 2.000000 with timestamp: 0013-28
2020-11-23 12:29:09 IOA: 4001 value: 2.000000 with timestamp: 0013-28
2020-11-23 12:29:09 IOA: 4002 value: 1.000000 with timestamp: 0013-28
2020-11-23 12:29:09 IOA: 4003 value: 1.000000 with timestamp: 0013-28
2020-11-23 12:29:09 IOA: 4004 value: 2.000000 with timestamp: 0013-28
2020-11-23 12:29:09 type(2) elements: 5
2020-11-23 12:29:09 IOA: 5000 value: 1.000000 with timestamp: 0013-28
2020-11-23 12:29:09 IOA: 5001 value: 0.000000 with timestamp: 0013-28
2020-11-23 12:29:09 IOA: 5002 value: 1.000000 with timestamp: 0013-28
2020-11-23 12:29:09 IOA: 5003 value: 1.000000 with timestamp: 0013-28
2020-11-23 12:29:09 IOA: 5004 value: 0.000000 with timestamp: 0013-28
```

Obr. C.7: Výpis logu pro scénář výpadku.

```
2020-11-23 13:42:24 type(4) elements: 5
2020-11-23 13:42:24 IOA: 4000 value: 1.000000 with timestamp: 0042-24
2020-11-23 13:42:24 IOA: 4001 value: 1.000000 with timestamp: 0042-24
2020-11-23 13:42:24 IOA: 4002 value: 1.000000 with timestamp: 0042-24
2020-11-23 13:42:24 IOA: 4003 value: 1.000000 with timestamp: 0042-24
2020-11-23 13:42:24 IOA: 4004 value: 1.000000 with timestamp: 0042-24
2020-11-23 13:42:24 type(2) elements: 5
2020-11-23 13:42:24 IOA: 5000 value: 0.000000 with timestamp: 0042-24
2020-11-23 13:42:24 IOA: 5001 value: 1.000000 with timestamp: 0042-24
2020-11-23 13:42:24 IOA: 5002 value: 0.000000 with timestamp: 0042-24
2020-11-23 13:42:24 IOA: 5003 value: 0.000000 with timestamp: 0042-24
2020-11-23 13:42:24 IOA: 5004 value: 0.000000 with timestamp: 0042-24
```

Obr. C.8: Výpis logu pro scénář vyřazení lokální kontroly.

D Seznam elektráren a rozvoden

Tab. D.1: Stanice polygonu energetické přenosové soustavy.

Název	**Typ zařízení**	**Označení**	**Počet transf.**	**IP**	
				Servisní síť	**Datová síť**
Albrechtice	Rozvodna	ALB	2	10.0.0.101	192.168.1.101
Babylon	Rozvodna	BAB	2	10.0.0.102	192.168.1.102
Bezděčín	Rozvodna	BEZ	3	10.0.0.103	192.168.1.103
Čebín	Rozvodna	CEB	3	10.0.0.104	192.168.1.104
Čechy střed	Rozvodna	CST	4	10.0.0.108	192.168.1.108
Dalešovice	Elektrárna	EDA	2	10.0.0.155	192.168.1.155
Dásný	Rozvodna	DAS	2	10.0.0.109	192.168.1.109
Dlouhé stráně	Elektrárna	EDS	1	10.0.0.154	192.168.1.154
Dukovany	Elektrárna	EDU	4	10.0.0.151	192.168.1.151
Horní životice	Rozvodna	HZI	2	10.0.0.113	192.168.1.113
Hradec východ	Rozvodna	HRA	1	10.0.0.110	192.168.1.110
Hradec západ	Rozvodna	HRD	1	10.0.0.111	192.168.1.111
Chodov	Rozvodna	CHD	2	10.0.0.105	192.168.1.105
Chotějovice	Rozvodna	CHT	2	10.0.0.107	192.168.1.107
Chrást	Rozvodna	CHR	2	10.0.0.106	192.168.1.106
Chvaletice	Elektrárna	ECHV	2	10.0.0.158	192.168.1.158
Kletné	Rozvodna	KLT	2	10.0.0.114	192.168.1.114
Kočín	Rozvodna	KOC	2	10.0.0.115	192.168.1.115
Krasíkov	Rozvodna	KRA	3	10.0.0.116	192.168.1.116
LDS sever	Rozvodna	LDS	2	10.0.0.118	192.168.1.118
Ledvice	Elektrárna	ELE	2	10.0.0.161	192.168.1.161
Lískovec	Rozvodna	LIS	3	10.0.0.117	192.168.1.117
Malešice	Rozvodna	MAL	2	10.0.0.119	192.168.1.119
Mělník	Elektrárna	EMĚ	1	10.0.0.160	192.168.1.160
Milín	Rozvodna	MIL	1	10.0.0.120	192.168.1.120
Mírovka	Rozvodna	HBM	2	10.0.0.112	192.168.1.112
Neznášov	Rozvodna	NEZ	2	10.0.0.121	192.168.1.121
Nošovice	Rozvodna	NOS	2	10.0.0.122	192.168.1.122
Opočínek	Rozvodna	OPO	2	10.0.0.123	192.168.1.123
Orlík	Elektrárna	EORK	1	10.0.0.159	192.168.1.159
Otrokovice	Rozvodna	OTR	3	10.0.0.124	192.168.1.124
Počerady	Elektrárna	EPOC	3	10.0.0.153	192.168.1.153
Prosenice	Rozvodna	PRN	3	10.0.0.126	192.168.1.126

Název	Typ zařízení	Označení	Počet transf.	IP	
				Servisní síť	Datová síť
Prunéřov	Elektrárna	EPRU	2	10.0.0.152	192.168.1.152
Přeštice	Rozvodna	PRE	2	10.0.0.125	192.168.1.125
Řeporyje	Rozvodna	REP	3	10.0.0.127	192.168.1.127
Slavěnice	Rozvodna	SLV	3	10.0.0.128	192.168.1.128
Sokolnice	Rozvodna	SOK	4	10.0.0.129	192.168.1.129
Tábor	Rozvodna	TAB	1	10.0.0.130	192.168.1.130
Temelín	Elektrárna	ETE	2	10.0.0.150	192.168.1.150
Tisova	Elektrárna	ETI2	1	10.0.0.157	192.168.1.157
Tušimice	Elektrárna	ETU	2	10.0.0.162	192.168.1.162
Týnec	Rozvodna	TYN	2	10.0.0.131	192.168.1.131
Vernéřov	Rozvodna	VER	1	10.0.0.132	192.168.1.132
Vítkov	Rozvodna	VIT	2	10.0.0.133	192.168.1.133
Vřesová	Elektrárna	EVRE	2	10.0.0.156	192.168.1.156
Výškov	Rozvodna	VYS	2	10.0.0.134	192.168.1.134

E Tabulka typově identifikačních čísel

Tab. E.1: Typově identifikační čísla IEC 60870-5

ID	Název	Zkratka
Zpracování informace ve směru monitorování		
1	Jednobodová informace	M_SP_NA_1
2	Jednobodová informace s časovou značkou	M_SP_TA_1
3	Dvoubodová informace	M_DP_NA_1
4	Dvoubodová informace s časovou značkou	M_DP_TA_1
5	Informace o poloze kroku	M_ST_NA_1
6	Informace o poloze kroku s časovou značkou	M_ST_TA_1
7	Bitový řetězec o 32 bitech	M_BO_NA_1
8	Bitový řetězec o 32 bitech s časovou značkou	M_BO_TA_1
9	Měřená hodnota, normalizovaná hodnota	M_ME_NA_1
10	Měřená hodnota, normalizovaná hodnota s časovou značkou	M_ME_TA_1
11	Měřená hodnota, škálovaná hodnota	M_ME_NB_1
12	Měřená hodnota, škálovaná hodnota s časovou značkou	M_ME_TB_1
13	Měřená hodnota, krátká hodnota s plovoucí desetinnou čárkou	M_ME_NC_1
14	Měřená hodnota, krátká hodnota s plovoucí desetinnou čárkou s časovou značkou	M_ME_TC_1
15	Integrované součty	M_IT_NA_1
16	Integrované součty s časovou značkou	M_IT_TA_1
17	Událost ochranného zařízení s časovou značkou	M_EP_TA_1
18	Zabalené počáteční události ochranného zařízení s časovou značkou	M_EP_TB_1
19	Informace o výstupním obvodu paketu ochranného zařízení s časovou značkou	M_EP_TC_1
20	Jednobodové informace o paketu s detekcí změny stavu	M_PS_NA_1
21	Měřená hodnota, normalizovaná hodnota bez deskriptoru kvality	M_ME_ND_1
Vyhodnocované telegramy s časovým razítkem CP56Time2a		
30	Jednobodová informace s časovou značkou CP56Time2a	M_SP_TB_1
31	Dvoubodová informace s časovou značkou CP56Time2a	M_DP_TB_1
32	Informace o poloze kroku s časovou značkou CP56Time2a	M_ST_TB_1
33	Bitový řetězec 32 bitů s časovou značkou CP56Time2a	M_BO_TB_1
34	Měřená hodnota, normalizovaná hodnota s časovou značkou CP56Time2a	M_ME_TD_1

ID	Název	Zkratka
35	Měřená hodnota, škálovaná hodnota s časovou značkou CP56Time2a	M_ME_TE_1
36	Měřená hodnota, krátká hodnota s plovoucí desetinnou čárkou s časovou značkou CP56Time2a	M_ME_TF_1
37	Integrované součty s časovou značkou CP56Time2a	M_IT_TB_1
38	Událost ochranného zařízení s časovou značkou CP56Time2a	M_EP_TD_1
39	Zabalené počáteční události ochranného zařízení s časovou značkou CP56time2a	M_EP_TE_1
40	Zabalené informace o výstupním obvodu ochranných zařízení s časovou značkou CP56Time2a	M_EP_TF_1
Zpracování informace ve směru řízení		
45	Jednoduchý příkaz	C_SC_NA_1
46	Dvojitý příkaz	C_DC_NA_1
47	Regulace krokového příkazu	C_RC_NA_1
48	Příkaz požadované hodnoty, normalizovaná hodnota	C_SE_NA_1
49	Příkaz požadované hodnoty, škálovaná hodnota	C_SE_NB_1
50	Příkaz požadované hodnoty, krátká hodnota s plovoucí desetinnou čárkou	C_SE_NC_1
51	Bitový řetězec 32 bitů	C_BO_NA_1
Ovládací telegramy s časovým razítkem CP56Time2a		
58	Jednoduchý příkaz s časovou značkou CP56Time2a	C_SC_TA_1
59	Dvojitý příkaz s časovou značkou CP56Time2a	C_DC_TA_1
60	Regulace krokového příkazu s časovou značkou CP56Time2a	C_RC_TA_1
61	Příkaz požadované hodnoty, normalizovaná hodnota s časovým štítkem CP56Time2a	C_SE_TA_1
62	Příkaz požadované hodnoty, měřítková hodnota s časovou značkou CP56Time2a	C_SE_TB_1
63	Příkaz požadované hodnoty, krátká hodnota s plovoucí desetinnou čárkou s časovou značkou CP56Time2a	C_SE_TC_1
64	Bitový řetězec 32 bitů s časovou značkou CP56Time2a	C_BO_TA_1
Systémové informace ve směru monitorování		
70	Konec inicializace	M_EI_NA_1
Systémové informace ve směru řízení		
100	Obecný dotazovací příkaz	C_IC_NA_1
101	Dotazový příkaz na čítač	C_CI_NA_1
102	Příkaz čtení	C_RD_NA_1
103	Příkaz synchronizace hodin	C_CS_NA_1
104	Testovací příkaz	C_TS_NB_1
105	Příkaz restartu procesu	C_RP_NC_1

ID	Název	Zkratka
106	Příkaz zpoždění akvizice	C_CD_NA_1
107	Testovací příkaz s časovou značkou CP56Time2a	C_TS_TA_1
	Parametr ve směru řízení	
110	Parametr měřené hodnoty, normalizovaná hodnota	P_ME_NA_1
111	Parametr měřené hodnoty, škálovaná hodnota	P_ME_NB_1
112	Parametr měřené hodnoty, krátká hodnota s plovoucí desetinnou čárkou	P_ME_NC_1
113	Aktivace parametrů	P_AC_NA_1
	Přenos souboru	
120	Soubor připraven	F_FR_NA_1
121	Sekce připravena	F_SR_NA_1
122	Adresář volání, vybraný soubor, soubor volání, volání sekce	F_SC_NA_1
123	Poslední sekce, poslední segment	F_LS_NA_1
124	Potvrzení souboru, potvrzení sekce	F_AF_NA_1
125	Segment	F_SG_NA_1
126	Adresář	F_DR_TA_1
127	Požadavek archivního souboru	F_SC_NB_1

F Tabulka hodnot COT

Tab. F.1: Možné příčiny přenosu zprávy IEC 60870-5.

Kód	**Příčina zprávy**	**Zkratka**
1	Periodická, cyklická	per/cyc
2	Dotazování na pozadí	back
3	Spontánní	spont
4	Inicializováno	int
5	Dotázán nebo dotazování	req
6	Aktivace	act
7	Potvrzení aktivace	actcon
8	Deaktivace	deact
9	Potvrzení deaktivace	deactcon
10	Ukončení aktivace	actterm
11	Zpětná vazba způsobená vzdáleným příkazem	retrem
12	Zpětná vazba způsobená místním příkazem	retloc
13	Přenos dat	file
14-19	Vyhrazeno pro další kompatibilní definice	–
20	Dotazování obecným dotazem	inrogen
21	Dotazování dotazovou skupinou 1	inro1
22	Dotazování dotazovou skupinou 2	inro2
23	Dotazování dotazovou skupinou 3	inro3
...		
34	Dotazování dotazovou skupinou 14	inro14
35	Dotazování dotazovou skupinou 15	inro15
36	Dotazování dotazovou skupinou 16	inro16
37	Dotazování obecným čítačem	reqcogen
38	Dotazování dotazovým čítačem skupiny 1	reqco1
39	Dotazování dotazovým čítačem skupiny 2	reqco2
40	Dotazování dotazovým čítačem skupiny 3	reqco3
41	Dotazování dotazovým čítačem skupiny 4	reqco4
...		
44	Neznámá identifikace typu	unknow_type
45	Neznámá příčina	unknown_type
46	Neznámá adresa ASDU	unknown_asdu_address
47	Neznámá adresa informačního objektu	unknown_object_address

G Mapování CDC na ASDU

Datové třídy typu VSS, ORG, TSG, CUG a VSG stanovené normou IEC 61850-7-3 nemůžou být přímo namapovány na ASDU protokolu IEC 60870-5-101/104. Obdobně je tomu i u přidaných datových tříd z normy IEC 61400-25-2, a to konkrétně třídy CURVE, DPL, CDS a SAV.

Tab. G.1: Mapování struktury CDC na typy ASDU pro monitorovací směr.

CDC		**Typ ASDU**	
Zkratka	**Název**	**Událost**	**Odpověď**
IEC 61850-7-3:2010			
SPS	Stav jednobodové informace	30	1
DPS	Stav dvoubodové informace	31	3
INS	Stav celého čísla	30, 33, 35	1, 7, 11
ACT	Informace o aktivaci ochrany	30, 39	1
ACD	Informace o aktivaci směrové ochrany	30, 40	1
SEC	Počet narušení bezpečnosti	37	37
BCR	Čtení binárního čítače	37	37
MV	Měřená hodnota	35, 36	11, 13
CMV	Komplexní měřená hodnota	35, 36	11, 13
WYE	Měřené hodnoty mezi fázemi a zemí v třífázovém systému	35, 36	11, 13
DEL	Fázově závislé naměřené hodnoty ve třífázovém systému	35, 36	11, 13
SEQ	Sekvence	35, 36	11, 13
HMV	Harmonická hodnota	35, 36	11, 13
HWYE	Harmonická hodnota pro WYE	35, 36	11, 13
HDEL	Harmonická hodnota pro DEL	35, 36	11, 13
ENS	Vyčíslený stav	30, 35	1, 11
HST	Histogram	33, 35	7, 11
IEC 61400-25-2			
STV	Stav hodnoty	30, 33, 35	1, 7, 11

Tab. G.2: Mapování struktury CDC na typy ASDU pro oba směry.

CDC		**Typ ASDU**			
Zkratka	**Název**	**Monitorovací směr**		**Řídící směr**	
		Událost	**Odpověď**	**Bez času**	**S časem**
IEC 61850-7-3:2010					
SPC	Ovládatelná jednobodová informace	30	1	45	58
DPC	Ovládatelná dvoubodová informace	31	3	46	59
INC	Stav ovládatelného celého čísla	35	11	49	62
BSC	Binárně kontrolovatelné informace o poloze kroku	32	5	47	60
ISC	Celé číslo řízené informace o poloze kroku	32	5	49	62
APC	Řiditelné informace o poloze analogové sady	36	13	50	63
ENC	Řízený vyčíslený stav	30, 35	1, 11	45, 49	58, 62
BAC	Binárně řízená analogová procesní hodnota	36	13	47	60
IEC 61400-25-2					
SPV	Požadovaná hodnota	36	13	50	63
ALM	Poplach	30, 33, 35	1, 7, 11	45	58
CMD	Příkaz	35	11	49	62
CTE	Počet událostí	30, 33, 35	1, 7, 11	45	58
TMS	Časování stavu	30, 33, 35	1, 7, 11	45	58

Tab. G.3: Mapování struktury CDC na typy ASDU pro řídící směr.

CDC		**Typ ASDU**	
Zkratka	**Název**	**Bez času**	**S časem**
IEC 61850-7-3:2010			
SPG	Nastavení jednobodé informace	45	58
ING	Nastavení stavu celého čísla	49	62
ASG	Analogové nastavení	50	63
ENG	Nastavení vyčísleného stavu	45, 49	58, 62
CSG	Nastavení tvaru křivky	50	63

H Popis kódu cs104_server

sharedMatrixPER_clr

Funkce slouží k mazání všech dat v pomocné matici.

nacteniMC

Funkce pomocí komunikačního portu dané instance serveru otevře specifický konfigurační soubor. Dále pomocí čtení ze souboru přečte tento konfigurační soubor a hodnoty přiřadí daným proměnným, se kterými je dále pracováno.

getStatus

Funkce slouží k přečtení pomocného konfiguračního souboru *ServerStatus.txt*, a tyto hodnoty uloží do pomocného listu (generating), ze které se vyhodnocuje stav dané instance serveru.

getRandomVal, getTemperature, getTemperature

Funkce mají podobnou funkci, a tou je vrátit náhodnou hodnotu pro vytvoření pseudonáhodné teploty či velikost simulované hodnoty.

clockSynchadler

Při obdržení zprávy nesoucí požadavek na časovou synchronizaci, ji tato funkce zpracuje a vypíše (v tomto případě není použito samotné nastavení).

interrogationHadler

Funkce slouží k rozpoznání příchozího dotazu na skupinu (v tomto případě není použito).

Logovací funkce

Funkce slouží čistě k zaznamenávání událostí, které se staly na daném zařízení. Struktura všech logů je takřka stejná. Pomocí zápisu do souboru a aktuálního času zapíše událost do konkrétního souboru. V případě zápisu přijatých/odeslaných hodnot zapíše i dané hodnoty a adresy informačních objektů, které je nesou.

asduHadler

Funkce porovnává obsah hlavičky přijatých zpráv a následně rozeznává o jaký typ zprávy se jedná. Dále je pak s každým typem zprávy postupováno obdobně, jen

specificky pro každý informační objekt dané zprávy. Tyto data jsou následně vypsány do konzole a do logovacích souborů (v tomto případě *LogRX[port].txt*). Pro zprávy typu double command (46) se zde nachází speciální blok kódu, který slouží pro práci s příchozími povely od klientské stanice (např. příkaz na vypnutí hlavního jističe).

connectionRequestHadler

Funkce zpracuje příchozí požadavek na spojení. Výsledek vypíše do konzole a do logovacího souboru (v tomto případě *EventLog.txt*).

connectionEventHadler

Funkce zpracuje příchozí ASDU zprávu connect, která přišla na zařízení a dále vypisuje výsledek při pokusu o navázání spojení.

CreateMONITOR_IN_ASDU, CreateMONITOR_OUT_ASDU

Funkce slouží k vytvoření ASDU zpráv, do které přidají všechny hodnoty (vygenerované a vypočítané), které mají spojitost se vstupními/výstupními daty. Postup přidávání informačních objektů je následující. Nejprve je přidána hodnota napětí (1000/2000), dále pak hodnota proudu (1001/2001). Poté dopočítaný výkon činný (1002/2002), a nakonec i výkon jalový (1003/2003). V tomto případě je použit konstantní úhel 30° (=0,525 rad). Tento postup je zopakován ještě 2x (začínaje 1004/2004 a konče 1011/2011), neboť jsou zde 3 fáze. Následně jsou tyto zprávy odeslány a zapsány do logovacího souboru. Všechny hodnoty jsou z konfiguračních souborů nahrány do matic monitor_in/monitor_out a z nich simulovány již konkrétní hodnoty do matice monitor_in_actual/monitor_out_actual.

CreateTEMPERATURE_ASDU, CreateMONITOR_FREQ_ASDU

Funkce slouží k vytvoření ASDU zprávy, do které přidají všechny hodnoty týkající se teploty a frekvence. Postup přidávání informačních objektů je následující. Nejprve je přidána hodnota teploty trafa, která je pseudonáhodná (3000), dále pak konstantní teploty minimální (3001) a maximální (3002) a nakonec teplota okolní (3003). Nakonec je k tomuto přidána i hodnota frekvence (3004). Tyto hodnoty jsou čerpány z proměnných temperature, temperatureRange, temperatureAmb a monitor_freq.

CreateMONITOR4_ASDU, CreateMONITOR2_ASDU

Funkce slouží k vytvoření ASDU zprávy, do které přidají všechny hodnoty týkající stavových hodnot instance serveru (události a stavy ochranných prvků).

CreateEvent4_ASDU, CreateEvent2_ASDU

Funkce slouží k vytvoření ASDU zprávy, do které ovšem nejsou přidány všechny hodnoty týkající se stavových proměnných, ale pouze hodnoty týkající se již konkrétních událostí dle tabulky 2.6.

Main

V první části dochází k načtení konfiguračního souboru (pomocí vstupních parametrů), výpisu načtených proměnných, a nakonec k samotnému vytvoření serveru. Pro správné fungování je potřeba zadat, mimo jiné, správnou adresu daného zařízení či komunikační port. Výsledek vytvoření instance serveru vypíše do konzole a zapíše do logovacího souboru (v tomto případě EventLog.txt).

Druhá část je již nekonečná smyčka, která každou vteřinu kontroluje, zda nedošlo ke změně stavu serveru (k nějaké události), pomocí konfiguračního souboru ServerStatus.txt či zprávy od klienta k vypnutí hlavního jističe/odpojovače. V případě, kdy nastane událost, se přejde do konkrétního bloku kódu (podle daného typu události). Např. v bloku podpětí dochází každou vteřinu ke snížení simulovaných hodnot, do doby nastavené v konfiguračním souboru. Poté je spuštěn ochranný jistič a simulování dat je zastaveno. V případě obnovení normálního stavu, program znovu načte výchozí hodnoty z konfiguračního souboru a pokračuje v simulaci hodnot. Obdobně je tomu pro ostatní události (přepětí, zkrat, odpojení hlavního jističe, odpojení odpojovače).

Dále je zde přítomen kód, zajišťující ochranu proti neočekávaným stavům v důsledku vzdáleného a lokálního ovládání. Také je zde kód pro odeslání spontánních dat v případě, že nastala událost 0, 2 či 3 (viz tabulka 2.6) a kód pro nastavení nulových hodnot pro simulování v případě odpojení hlavního jističe/odpojovače.

Následuje blok, který převádí simulované hodnoty napětí a proudu do pomocných matic (monitor_in_actual/monitor_out_actual). Taktéž vybraná data (v tomto případě napětí a teplotu) zapíše do pomocné matice (sharedMatrixPER), kterou následně zapíše do pomocného souboru *TXmatrix[port].txt*.

Poslední částí nekonečné smyčky je blok, který je aktivní v případě, kdy program dovrší přednastaveného času pro poslání periodických zpráv.