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

MODELOVÁNÍ A HODNOCENÍ KYBERNETICKÉ BEZPEČNOSTI ELEKTROENERGETICKÝCH SYSTÉMŮ
MODELING AND EVALUATION OF CYBERSECURITY IN ELECTRICAL POWER SYSTEMS

DISERTAČNÍ PRÁCE
DOCTORAL THESIS

AUTOR PRÁCE — **Ing. Petr Blažek**
AUTHOR

VEDOUCÍ PRÁCE — **doc. Václav Zeman, Ph.D.**
ADVISOR

BRNO 2025

ABSTRAKT

Disertační práce se zabývá kybernetickou bezpečností chytrých sítí, se zaměřením na datovou komunikaci a zajištění bezpečnosti přenosové a distribuční soustavy. V kontextu narůstající digitalizace a vzájemného propojení operačních technologií se práce soustředí na návrh realistické sandbox architektury pro výzkum, testování a vzdělávání v oblasti kybernetické bezpečnosti elektroenergetických systémů. Hlavním výstupem je modulární a škálovatelné testovacího prostředí, které kombinuje fyzické, emulované a virtualizované komponenty, umožňující simulaci provozu elektrických stanic, modelování útoků a ověřování mitigačních opatření bez rizika pro reálnou infrastrukturu. Východiskem pro návrh byla systematická analýza komunikační architektury chytrých sítí s využitím standardů IEC 61850 a IEC 60870, doplněná o modelování přenosových charakteristik zpráv prostřednictvím teorie front (M/M/1, M/D/1, MMPP). Součástí řešení je vícevrstvá bezpečnostní analýza využívající metody STRIDE a MITRE ATT&CK, která identifikuje zranitelnosti protokolů a zařízení. Výsledky byly následně porovnány s požadavky standardů IEC 62351, IEC 62443, NIST 800-82 a doporučeními ENISA. Výsledné prostředí umožňuje efektivní a technicky věrné testování zátěžových scénářů, školení odborného personálu a generování reprezentativních dat pro další výzkum. Práce tak přispívá ke zvýšení odolnosti elektroenergetických systémů vůči kybernetickým hrozbám a podporuje rozvoj aplikované bezpečnosti v oblasti elektroenergetické kritické infrastruktury.

KLÍČOVÁ SLOVA

chytré sítě, distribuční soustava, IEC 60870-5-104, IEC 61850, IEC 62351, IEC 62443, kritická infrastruktura, kybernetická bezpečnost, MITRE ATT&CK, NIST 800-82, přenosová soustava, STRIDE

ABSTRACT

This dissertation addresses the issue of cybersecurity in smart grids, with a focus on data communication and the protection of the transmission and distribution infrastructure. In response to the increasing digitalization and integration of operational technologies, the work aims to design a realistic sandbox architecture for research, testing, and training in the field of cybersecurity for power systems. The main outcome is a modular and scalable test environment that combines physical, emulated, and virtualized components, enabling simulation of substation operations, modeling of cyberattacks, and validation of mitigation measures without endangering real infrastructure. The design is based on a systematic analysis of the communication architecture in smart grids using IEC 61850 and IEC 60870 standards, extended with traffic modeling through queueing theory (M/M/1, M/D/1, MMPP). The solution includes a multi-layered security analysis based on STRIDE and MITRE ATT&CK, identifying vulnerabilities in protocols and devices. The results were compared against the requirements of standards such as IEC 62351, IEC 62443, NIST 800-82, and ENISA recommendations. The resulting platform supports effective and technically faithful testing of high-load scenarios, hands-on training of technical staff, and the generation of representative datasets for further research. The dissertation contributes to strengthening the resilience of electrical power systems against cyber threats and supports the development of applied security in the domain of critical infrastructure.

KEYWORDS

critical infrastructure, cybersecurity, distribution system, IEC60870-5-104, IEC61850, IEC62351, IEC62443, MITRE ATT&CK, NIST 800-82, smart grid, STRIDE, transmission system

BLAŽEK, Petr. *Modelování a hodnocení kybernetické bezpečnosti elektroenergetických systémů*. Disertační práce. Brno: Vysoké učení technické v Brně, Fakulta elektrotechniky a komunikačních technologií, Ústav telekomunikací, 2025. Vedoucí práce: doc. Václav Zeman, Ph.D.

Prohlášení autora o původnosti díla

Jméno a příjmení autora:	Ing. Petr Blažek
VUT ID autora:	140217
Typ práce:	Disertační práce
Akademický rok:	2024/25
Téma závěrečné práce:	Modelování a hodnocení kybernetické bezpečnosti elektroenergetických systémů

Prohlašuji, že svou závěrečnou práci jsem vypracoval samostatně pod vedením vedoucího závěrečné práce a s použitím odborné literatury a dalších informačních zdrojů, které jsou všechny citovány v práci a uvedeny v seznamu literatury na konci práce. Při vypracovávání práce byl použit nástroj GPT-4, a to za účelem zlepšení čitelnosti textu. Po použití tohoto nástroje jsem obsah zkontroloval a upravil a za obsah práce přebírám plnou odpovědnost. Uvedený nástroj je použit v souladu s pravidly VUT v Brně platnými v době psaní této práce dostupnými na adrese https://www.vut.cz/uredni-deska/ai/vzdelavani.

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

Brno ....

podpis autora*

*Autor podepisuje pouze v tištěné verzi.

PODĚKOVÁNÍ

Rád bych poděkoval vedoucímu své disertační práce doc. Václavu Zemanovi, Ph.D., za odborné vedení, cenné konzultace, trpělivost a podnětné návrhy, které významně přispěly k výsledné podobě této práce. Poděkování patří také mé rodině, která mě po celou dobu studia podporovala. Jejich trpělivost, povzbuzení a porozumění byly pro mě stálým zdrojem motivace a pomohly mi soustředit se na dosažení vytyčených cílů.

Zvláštní poděkování patří také doc. Radkovi Fujdiakovi, Ph.D. a mým kolegům, kteří mě během práce doprovázeli, sdíleli své zkušenosti, poskytovali cenné rady a ochotně pomáhali při řešení dílčích problémů. Jejich podpora byla nejen praktickým přínosem, ale také zdrojem inspirace a dobré spolupráce.

Na závěr děkuji všem, kteří se jakýmkoli způsobem podíleli na vzniku této práce, ať už prostřednictvím odborných konzultací, podpory nebo povzbuzení.

Obsah

Seznam obrázků

Seznam tabulek

Úvod

Energetický sektor prochází zásadní transformací směrem k digitalizovaným chytrým sítím, které zahrnují interoperabilní zařízení a síťovou komunikaci spolu s pokročilými řídicími systémy. Tradičně izolované průmyslové řídicí systémy (ICS) a deterministicky řízené v elektroenergetice se vyvinuly v komplexní kyber-fyzické systémy (CPS). Provozní bezpečnost v nich závisí na integritě a spolehlivosti datové komunikace v reálném čase. Mezi klíčové komponenty patří inteligentní elektronická zařízení (IED) a vzdálené terminálové jednotky (RTU), které jsou propojeny komunikační infrastrukturou využívající standardizované protokoly, například IEC 60870-5-104 nebo IEC 61850. Větší propojení digitálních sítí s fyzickými prvky, spolu s narůstající mírou automatizace, zvyšuje pravděpodobnost vzniku nových zranitelností a sofistikovanějších útoků. Kybernetické útoky na energetickou infrastrukturu mohou způsobit ztrátu kontroly, fyzické škody nebo rozsáhlé výpadky. Moderní energetické systémy se staly aktivním cílem pro útočníky, jak dokazují reálné incidenty jako malware Stuxnet (2010) [160] nebo kybernetický útok na ukrajinskou rozvodnou síť (2015/2016) [179], a narušení digitální ochrany tak může mít přímé fyzické dopady na společnost. Tyto případy činí kybernetickou bezpečnost elektroenergetiky vysoce aktuálním tématem a zdůrazňují potřebu efektivního zabezpečení kritických infrastruktur.

Zajištění kybernetické bezpečnosti chytrých sítí přináší řadu specifických výzev. Energetická infrastruktura je ze své podstaty provozována nepřetržitě a jakékoliv zásahy do jejího chodu může mít negativní dopad, což výrazně omezuje možnosti testování bezpečnostních opatření nebo simulace incidentů přímo v reálném provozu. Taková omezení komplikují nejen vývoj a ověřování nových bezpečnostních mechanismů, ale i efektivní školení personálu v oblasti reakcí na bezpečnostní události.

Další nedostatkem je samotná architektura používané komunikační infrastruktury. Mnohé průmyslové protokoly, jako například IEC 61850 nebo IEC 60870, nebyly navrženy s ohledem na bezpečnost a v původních verzích postrádají integrované mechanismy autentizace či šifrování. Rozšíření typu IEC 62351 sice tyto nedostatky částečně řeší, jejich implementace však není standardizována napříč odvětvím, což ponechává prostor pro útoky.

Současně dochází k propojování dosud oddělených infrastruktur informačních (IT) a provozních technologií (OT). Zatímco energetické systémy jsou čím dál více integrovány s podnikovými, chybí personál se znalostmi napříč těmito oblastmi. Specialisté jsou zpravidla vzděláni buď v oblasti IT bezpečnosti, nebo OT, nikoliv však v obou zároveň, což ztěžuje ochranu hybridních průmyslových prostředí.

Jedním z nejvýraznějších omezení současného výzkumu je nedostupnost realistických datových sad. Reálná provozní data jsou často klasifikována jako citlivá, kde obsahují detailní informace o topologiích, konfiguracích a stavech zařízení, a jejich sdílení podléhá přísné regulaci v rámci ochrany kritické infrastruktury. Tím vzniká zásadní překážka pro vývoj pokročilých metod pro eliminaci bezpečnostních incidentů.

V tomto kontextu se jako klíčové řešení jeví vytvoření realistického testovacího prostředí, který napodobuje chování reálné energetické sítě a současně umožňuje simulaci scénářů. Takové prostředí má sloužit nejen pro experimentální testování, ale také pro praktický trénink odborného personálu a generování syntetických dat bez nutnosti práce s reálnými provozními údaji.

Tato potřeba se promítá do struktury této disertační práce, která je rozdělena do šesti kapitol, logicky navazujících od úvodní analýzy problematiky přes formulaci cílů a návrh řešení až po jeho implementaci a ověření v praxi.

Kapitola 1 uvádí čtenáře do problematiky digitalizace elektroenergetiky, představuje koncept Smart Grid a analyzuje klíčové výzvy spojené s bezpečností provozních technologií. Součástí ka-

pitoly je GAP analýza a formulace výzkumných otázek zaměřených na zajištění kybernetické bezpečnosti v digitálních rozvodnách.

Kapitola 2 vymezuje cíle disertační práce, které reagují na identifikované problémy v oblasti školení, testování a sběru dat v prostředí Smart Grid. Podrobně rozpracovává čtyři klíčové cíle: (1) formální analýzu technologického prostředí, (2) rizikovou analýzu a identifikaci mezer ve standardech, (3) návrh a realizaci sandbox architektury a (4) návrh scénářů pro školení a generování realistických datasetů.

Kapitola 3 se věnuje návrhu architektury digitální rozvodny a referenčního modelu datové komunikace v prostředí Smart Grid. Detailně popisuje vrstvy architektury, komunikující prvky (IED, RTU, SCADA, HMI) a specifikuje protokoly IEC 61850 a IEC 60870-5-104. Následně aplikuje teorii front k modelování datových toků (M/M/1, M/D/1, MMPP) včetně variant s redundancí.

Kapitola 4 se zaměřuje na bezpečnostní rozbor protokolů a komponent chytré rozvodny. Aplikuje metodiku STRIDE-LM a MITRE ATT&CK for ICS, mapuje zranitelnosti na jednotlivé vrstvy architektury a analyzuje pokrytí hrozeb v rámci standardů IEC 62443, IEC 62351 a NIST 800-82. Výsledkem je bezpečnostní rámec pro navrženou infrastrukturu.

Kapitola 5 popisuje návrh struktury testovacího prostředí (testbedu), které emuluje komunikační model chytré rozvodny. Využívá DFD modely pro návrh jednotlivých vrstev, segmentuje síť dle funkcí a validuje přenosovou kapacitu. Kapitola srovnává dostupná výzkumná prostředí a zdůvodňuje volbu vlastní architektury.

Kapitola 6 se věnuje implementaci a validaci navrženého testbedu. Popisuje hardwarovou a softwarovou realizaci elektrické stanice podle IEC 61850 a IEC 60870-5-104, komunikaci se SCADA a HMI systémy a začlenění komponent do prostředí BUTENET. V závěru kapitoly je demonstrována aplikace testovacího prostředí pro emulace provozu trafostanice, generování trénovacích dat pro neuronové sítě, testování BPL komunikace a využití pro ověření zabezpečení RTU jednotek.

1 Úvod do problematiky a výzkumná motivace

V oblasti elektroenergetiky dochází v posledních letech k zásadní proměně, která je způsobena přechodem od tradičních fyzicky izolovaných systému k digitálně řízeným systémům. Tento vývoj je důsledkem kombinace několika faktorů [82], mezi které patří rostoucí požadavky na efektivitu provozu, potřeba začlenění obnovitelných zdrojů, požadavek na flexibilní řízení a snaha o zajištění provozní spolehlivosti. Reakcí na tyto potřeby je zavádění konceptu chytrých sítí (Smart Grid), který integruje prvky digitalizace, pokročilé řízení, síťovou komunikaci a interoperabilní zařízení.

Na rozdíl od původních přenosových a distribučních soustav, které byly fyzicky izolované a deterministicky řízené, moderní energetická infrastruktura využívá data ze senzorů, ochranných zařízení a prvků k realizaci rozhodovacích procesů v reálném čase [174]. Komponenty jako IED nebo RTU zajišťují sběr a přenos dat v rámci sítí, které jsou propojené přes protokoly jako IEC 61850 nebo IEC 60870-5-104.

Moderní Smart Grid systémy představují prostředí, ve kterém provozní bezpečnost přímo závisí na správnosti přenášených dat, synchronizaci mezi subsystémy a schopnosti reagovat na anomálie nebo incidenty. Takové propojení fyzických a digitálních prvků se označuje jako kyber-fyzický systém, kde komunikace přímo ovlivňují fyzické operace a zpětně přijímají informace o jejich výsledku. Propojení jednotlivých prvků mezi sebou i s nadřazenými systémy přináší požadavek na jednotný rámec řízení komunikace, monitorování a zabezpečení. V praxi to znamená, že většina kritických operací, které dříve probíhaly lokálně a odděleně, je dnes navázána na sdílené digitální prostředky a síťovou infrastrukturu.

Zranitelnosti se mohou vyskytovat na všech úrovních od fyzických zařízení až po nadřazené dohledové systémy. Napadení řídicích protokolů, kompromitace komunikačních rozhraní nebo manipulace s parametrickými nastaveními zařízení může vést ke ztrátě kontroly nad provozem, ke škodám na infrastruktuře nebo k dlouhodobým výpadkům. Reálné incidenty typu Stuxnet [160] nebo Industroyer [179] ukazují, že energetická infrastruktura je aktivním cílem útočníků, a že bezpečnostní incidenty mohou mít přímý dopad na bezpečnost dodávky elektrické energie. Dále také dokazují, že selhání v oblasti digitální ochrany může mít okamžitý dopad na fyzickou infrastrukturu i samotnou společnosti.

Energetická infrastruktura je specifická tím, že se jedná o systém, jehož provoz je nepřetržitý a citlivý na jakékoliv zásahy. Testování bezpečnostních opatření, provozních změn nebo replikaci bezpečnostních incidentů v reálném prostředí není běžně možné bez odstávky, která může znamenat lokální nebo regionální výpadek dodávky elektrické energie. To vytváří významnou překážku pro experimentální validaci bezpečnostních mechanismů a pro vývoj metodik určených k detekci a mitigaci kybernetických hrozeb.

Vzhledem k výše uvedeným skutečnostem je nezbytné se zaměřit na otázky, jak navrhovat architektury energetických systémů s důrazem na odolnost vůči kybernetickým útokům, jak modelovat provozní i komunikační vrstvy tak, aby bylo možné ověřovat účinnost navržených bezpečnostních opatření, a především jak vytvořit prostředí, které umožní bezpečné, opakovatelné a technicky relevantní testování útoků, obranných scénářů a odpovídajících standardů. Právě z těchto důvodů se tato práce vědomě neorientuje na modelování fyzikálních jevů spojených s tokem energie, ale soustředí se na komunikaci, řízení a kybernetickou bezpečnost jako klíčové části Smart Grid.

1.1 Vývoj Smart Grid

Tradiční elektrizační soustava byla po desetiletí charakterizována centrálním řízením, jednosměrným tokem energie, omezeným monitoringem a minimální mírou automatizace [83]. Řídicí rozhodnutí byla lokalizována do centrálních dispečinků a komunikace probíhala pomocí analogových nebo proprietárních technologií. Tyto soustavy byly navrženy tak, aby byly stabilní a predikovatelné, bez nutnosti dynamických zásahů do provozu v reálném čase. S nástupem nových komunikačních a řídicích technologií, které umožňují obousměrný tok dat i energie, decentralizovanou výrobu a širší využití měření v reálném čase, došlo k postupné transformaci směrem k tzv. chytrým sítím [83]. Tento vývoj probíhal ve více etapách, z nichž každá reflektuje zvýšený stupeň digitalizace, automatizace a propojenosti.

Smart Grid 1.0

Fáze Smart Grid 1.0 zahrnovala první kroky digitalizace, to je měření spotřeby pomocí inteligentních elektroměrů, přenos údajů pomocí SCADA systémů a základní automatizaci distribuční sítě [83]. Přestože šlo o významný pokrok oproti předchozím systémům, infrastruktura zůstávala do značné míry uzavřená, silně centralizovaná a technologicky nejednotná. Komunikační protokoly nebyly standardizované a bezpečnostní vrstvy byly většinou opomíjeny, což omezovalo rozšiřitelnost i možnosti ochrany před budoucími hrozbami.

Smart Grid 2.0

Následující vývojová fáze, označovaná jako Smart Grid 2.0 [81], je charakterizována přechodem k distribuovanému řízení a otevřené komunikační infrastruktuře. Dochází k výraznému rozšíření decentralizovaných výrobních zdrojů, zejména fotovoltaických a větrných elektráren, jejichž provoz vyžaduje dynamické řízení a vyvažování zátěže. V této fázi byla klíčová integrace standardizovaných protokolů, jako jsou IEC 61850 nebo IEC 60870-5-104, které umožňují interoperabilní komunikaci mezi zařízeními od různých výrobců. Smart Grid 2.0 přináší složitější architektury a provozní závislosti na datech. Subsystémy získávají určitou míru autonomie, kde například inteligentní rozvodny či mikrosítě jsou schopny reagovat na lokální provozní podmínky bez zásahu centrálního dispečinku, avšak s tím přichází i zvýšené nároky na zajištění integrity a dostupnosti komunikace.

Současný stav

Současný vývoj směřuje k propojení elektroenergetiky s digitálními technologiemi na úrovni kyberfyzických systémů [176]. Tato architektura propojuje výrobní, distribuční a spotřební části infrastruktury s nadřazenými informačními systémy, analytickými nástroji a prvky umělé inteligence. Dochází k nasazování inteligentních ochran s podporou vysokorychlostní výměny zpráv, zavádění digitálních dvojčat pro sledování a simulaci provozních stavů a využití edge computing[1] pro lokální rozhodování s minimální zpožděním. Důraz je kladen na návrh systémů podle principu security-by-design[2], kdy jsou bezpečnostní mechanismy integrovány přímo do architektury zařízení, nikoli dodatečně připojovány. Vedle technické úrovně roste i důležitost softwarového řízení, telemetrie, adaptivních modelů chování a provozní auditovatelnosti. Transformace směrem k CPS otevírá nové možnosti v oblasti řízení, predikce a optimalizace provozu, ale zároveň přináší zásadní výzvy v oblasti kybernetické bezpečnosti, spolehlivosti komunikace a testování odolnosti systémů vůči interním i externím hrozbám.

[1] Model distribuovaného výpočtu, který přenáší výpočet a datové úložiště blíže ke zdroji dat.

[2] Princip definující, že bezpečnost by měla být nedílnou součástí při návrhu produktu

1.2 Kybernetické hrozby v OT

Digitalizace elektroenergetické infrastruktury přináší zásadní změnu nejen v oblasti řízení, ale i v oblasti bezpečnosti. Integrace IT a OT technologií v chytrých sítích umožňuje pokročilé řízení přenosu, distribuce i spotřeby energie, ale zároveň zvyšuje zranitelnost vůči sofistikovaným kybernetickým hrozbám. Zatímco tradiční energetická infrastruktura byla z velké části izolovaná a fyzicky oddělená, současné systémy se stávají CPS, kde selhání softwaru nebo komunikační vrstvy může způsobit reálné dopady na dodávku energie, dostupnost zařízení a bezpečnost obsluhy.

Kybernetické útoky na energetickou infrastrukturu se již v minulosti prokázaly jako reálná a účinná hrozba, jak ukázaly incidenty jako Stuxnet, BlackEnergy nebo Industroyer. V rámci kritické infrastruktury představují zvláštní riziko zejména útoky zaměřené na řídicí systémy (např. RTU nebo IED) a jejich komunikační rozhraní, kde je možné narušit tok dat, manipulovat s řídicí logikou nebo vyřadit zařízení z provozu. Jednotlivé, známé a zdokumentované útoky jsou podrobně popsány v kapitole 4.2.

Podle zpráv ENISA Threat Landscape z let 2020–2024 [71, 72, 73, 74, 77] patří mezi nejčastější a nejzávažnější útoky právě ty, které kombinují více vrstev útoku a to od zneužití zranitelností softwaru (exploit) po šifrování dat (ransomware) či manipulaci s autentizací (spoofing). Tyto trendy potvrzuje i zaměření mnoha moderních útočníků na průmyslové řídicí systémy, kde ztráta integrity nebo dostupnosti může vést k domino efektům napříč energetickou soustavou. Jednotlivé zprávy jsou podrobněji popsané v kapitole 4.1.5.

1.3 GAP analýza

Navzdory pokročilé digitalizaci elektroenergetické infrastruktury a zavádění standardizovaných komunikačních protokolů přetrvává řada zásadních problémů, které omezují možnosti zabezpečení. Přestože technologické prostředky pro zajištění provozní bezpečnosti existují, v praxi narážejí na konkrétní omezení a to od nedostatečné implementace bezpečnostních vrstev až po absenci metodiky pro výzkum v kontrolovaném prostředí. V této souvislosti je vhodné využít GAP analýzu, která umožňuje systematicky porovnat současný stav zabezpečení s požadavky definovanými ve standardech a doporučených rámcích. Jejím cílem je identifikovat oblasti, kde existuje nesoulad mezi teoretickými možnostmi ochrany a jejich praktickou implementací, a odhalit tak konkrétní slabá místa. V následujících podkapitolách jsou proto podrobně rozpracovány hlavní nedostatky, které tento nesoulad způsobují, a které představují zásadní překážky pro dosažení vyšší úrovně kybernetické bezpečnosti.

Nedostatečné pokrytí komunikační bezpečnosti

Standardy jako IEC 61850 nebo IEC 60870-5-104 definují strukturu datové komunikace a interoperabilitu mezi jednotlivými zařízeními, ale v základním rozsahu neřeší bezpečnostní ochranu proti útokům [58]. Zranitelnosti v těchto protokolech umožňují např. spoofing (podvržení identity nebo falešná komunikace), replay (zachycení a opětovné přehrání dříve platné komunikace) nebo DoS (Denial of Service, zahlcení systému a znepřístupnění služby) útoky. Doplnění bezpečnostních mechanismů je realizováno externě, typicky prostřednictvím rozšíření jako IEC 62351, které však není plošně implementováno a jeho nasazení je často nekonzistentní a závislé na výrobci nebo provozovateli.

Absence realistických testovacích prostředí

Validace bezpečnostních opatření, testování reakčních mechanismů a vývoj obranných scénářů vyžadují prostředí, které umožní emulaci nebo simulaci energetické infrastruktury bez ohrožení provozu. V současnosti jsou běžně dostupné buď zjednodušené simulační nástroje, které neodrážejí reálné vlastnosti systému, nebo produkční prostředky, jejichž využití je vázáno na přísné provozní omezení a riziko výpadku [183].

Chybějící integrace mezi bezpečnostními standardy

Různé bezpečnostní rámce (IEC 62443, NIST 800-82, ISO/IEC 27019) existují paralelně, často bez jednotného propojení. Chybí mapování jednotlivých hrozeb na konkrétní kontrolní mechanismy a není zřejmé, kde dochází k překrytí nebo kde zůstávají mezery [78]. Tato situace komplikuje tvorbu bezpečnostních politik v prostředí s více dodavateli, technologiemi a provozními režimy.

Nízká připravenost personálu

Kybernetická bezpečnost vyžaduje znalosti z více domén – IT, OT, energetiky, komunikačních sítí. Personál rozvoden je často školen převážně v oblasti provozu zařízení, ale postrádá systematické školení v oblasti hrozeb a obranných mechanismů [80]. Znalosti o principech útoků, protokolech, metodách detekce nebo možnostech mitigace nejsou standardní součástí profesní přípravy.

Ochrana citlivých dat a legislativní nejasnosti

Z důvodu klasifikace elektroenergetiky jako kritické infrastruktury podléhá práce s daty řadě omezení [160]. Právní rámec (např. zákon o kybernetické bezpečnosti[3], zákon o ochraně utajovaných informací[4]) neumožňují volnou práci s reálnými daty v rámci výzkumu, což komplikuje sdílení datasetů, jejich publikaci nebo použití ve výukových scénářích. V důsledku toho je obtížné validovat analytické přístupy nebo vyhodnocovat účinnost obranných mechanismů na datech odrážejících skutečné podmínky provozu.

1.4 Definice problémů a výzkumných otázek

Na základě provedené GAP analýzy lze identifikovat několik klíčových problémů, které zásadně ovlivňují úroveň kybernetické bezpečnosti v prostředí chytrých sítí. Tyto problémy vycházejí nejen z technických nedostatků v oblasti komunikačních protokolů a dostupných testovacích prostředí, ale také z organizačních a legislativních překážek. Zvlášť závažná je nízká připravenost personálu na nové hrozby, absence bezpečného a přitom realistického prostředí pro testování bezpečnostních opatření a omezená dostupnost autentických dat, která brání rozvoji moderních detekčních a obranných mechanismů. Na tyto oblasti se proto zaměřuje následující formulace výzkumných problémů a otázek. Jejich cílem je systematicky popsat klíčové výzvy a poskytnout rámec pro návrh a implementaci řešení, které povedou k vyšší odolnosti energetické infrastruktury vůči kybernetickým hrozbám.

[3] Zákon č. 181/2014 Sb., o kybernetické bezpečnosti, účinný od 1. 1. 2015, ve znění 106/2017 Sb. atd.
[4] Zákon č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti.

Problém 1: Nedostatečná připravenost personálu v OT kybernetické bezpečnosti

S rozvojem Smart Grid dochází k prolínání OT s IT infrastrukturou. Současní technici dostatečně nespravují ani neprovozují bezpečnostní mechanismy, protože na ně nebyli školeni. Školení se zaměřují buď na IT, nebo na OT, nikoliv na integraci obou. Podle zprávy ENISA o kybernetické bezpečnosti z roku 2019 [79] představuje hlavní překážku rychlejší implementace bezpečnostních opatření v prostředí Průmyslu 4.0 kombinace nedostatečného povědomí o hrozbách, neexistence jednotných standardů, složitosti průmyslových prostředí a vysokých finančních nákladů. Dále uvádí, že většina odborníků má bezpečnostní znalosti pouze z oblasti IT nebo OT, zatímco Průmysl 4.0 vyžaduje znalosti v několika oblastech, např. bezpečnost sítí, vestavěné systémy, bezpečnost OT a IT a další.

Podobně na to pohlíží autoři v článku [186], která analyzuje dostupný obsah pro školení v oblasti kybernetické bezpečnosti energetických sítí. Toto přesně reflektuje, že stávající školení postrádají odpovídající rozsah témat a úrovní obtížnosti, které by pokryly současné potřeby operatorů. Článek identifikuje chybějící modulární strukturu kurzů, nízkou dostupnost pokročilých cvičení a absenci materiálů přizpůsobených průmyslovému personálu, což autoři považují za klíčové.

V dalším článku [175] autoři poukazují na to, že ICS/OT systémy jsou stále více propojeny s IT, školení často pokrývají jen IT přístupy a nástroje, aniž by řešily praktické bezpečnostní scénáře v hybridním prostředí ICS. Studie proto podporuje nutnost vzdělávání odborníků, kteří rozumějí komplexnosti kyber-fyzických systémů, umějí identifikovat hrozby na fyzické i digitální vrstvě a sestavovat ochranná opatření přizpůsobená energetickému sektoru.

Problém 2: Absence bezpečného, ale realistického testovacího prostředí pro Smart Grid

S rozvojem kyber-fyzických systémů v rámci Smart Grid je nezbytné testovat algoritmy, bezpečnostní protokoly a obranné mechanismy ve scénářích, které co nejvěrněji reflektují reálný provoz. Používání reálných infrastruktur k testování může vést k vážným rizikům: výpadky služby, finanční škody nebo ohrožení občanů.

Autoři ve své přehledové studii [193] o testovacích prostředích zaměřené na chytré sítě zdůrazňují, že testovací prostředí nejsou pouze užitečná, ale zcela nezbytná pro validaci řešení, jež mají být nasazena do produkční infrastruktury. Bez věrné simulace reálného provozu, protokolů a HW komponent je riskantní a nepraktické ověřovat bezpečnostní mechanismy přímo v živých systémech. Studium ukazuje, že nasazení na reálnou infrastrukturu by mohlo vést k výpadkům, haváriím, finančním ztrátám nebo legislativním problémům, a proto testbed plní klíčovou roli jako bezpečné prostředí pro vývoj, testování a školení.

Podobný pohled na to mají autoři v článku [42], který se soustředí na zranitelnost Smart Grid systémů a konstatují, že pro jejich seriózní analýzu a ochranu je nezbytné používat simulační prostředí „cyber-range“[5]. Jasně uvádějí, že testování v produkčním prostředí je z etických, technických i právních důvodů neproveditelné a tak testování zranitelnosti založené na simulaci představuje jedinou reálnou metodu, jak posoudit výkonnost ICS/OT mechanismů a identifikovat slabiny, aniž by se ohrozila reálná infrastruktura.

[5] Tréninkové prostředí pro simulaci kybernetických incidentů.

Problém 3: Citlivost dat a nedostupnost reálných datasetů

V kontextu Smart Grid je sběr, analýza a využívání dat pro účely výzkumu, detekce anomálií či trénink strojového učení zásadní. Nicméně tato data jsou často vysoce citlivá a obsahují informace o topologii sítě, chování zařízení i uživatelské zvyklosti, a jejich nepřiměřené zpřístupnění může způsobit nevratné škody na infrastruktuře nebo ohrožení osobního soukromí. Navíc český zákon o kybernetické bezpečnosti (ZoKB[6]) a připravovaná revize legislativního rámce pro kritickou infrastrukturu (NIS2[7]) omezují sdílení surových i anonymizovaných dat, což výrazně ztěžuje shromažďování autentických datasetů pro výzkum.

Autoři v článku [195] upozorňuje, že sběr dat z chytrých měřičů představuje riziko úniku informací o citlivých údajích a že požadavky na GDPR[8], NIS2, případně doplňující legislativu, významně omezují možnosti poskytovat data i za účelem výzkumu.

Podobně to vidí i autoři ve studii [50], kde shrnují, že dostupná veřejná sbírka dat pro OT systémy je velmi omezená, protože provozovatelé často nesdílí reálná provozní data z obavy o duševní vlastnictví, bezpečnostní rizika a reputační dopady. To znamená, že detekční systémy a modely strojového učení jsou testovány na úzce vymezených datasetech, což omezuje jejich schopnost generalizovat na nové reálné situace.

Autoři ve studii [49] a [170] popisují, že kvůli omezené dostupnosti skutečných provozních dat pro Smart Grid je jedinou možnou cestou pro vědecký výzkum generování datasetů přímo z testbedů. Autoři poukazují, že taková data obsahují jak normální stavy, tak i simulované útoky, a pro komunitu představují neocenitelný zdroj pro vývoj detekčních mechanismů.

[6] Zákon o kybernetické bezpečnosti, č. 181/2014 Sb.
[7] Evropská směrnice, která definuje požadavky na kybernetickou bezpečnost v kritické infrastruktuře.
[8] General Data Protection Regulation (Obecné nařízení o ochraně osobních údajů).

2 Cíle práce

Cílem této disertační práce je navrhnout a implementovat škálovatelnou a realistickou sandbox architekturu určenou pro výzkum kyber-fyzických systémů v oblasti moderních energetických sítí. Navržená architektura umožní bezpečné testování a analýzu kybernetických hrozeb, validaci mitigačních opatření a podporu vzdělávání odborného personálu v oblasti elektroenergetiky. Důraz je kladen na kybernetickou bezpečnost komunikačních a řídicích technologií s ohledem na specifika kritické infrastruktury. Práce přímo reaguje na klíčové problémy identifikované v předchozí kapitole, které aktuálně omezují efektivní rozvoj bezpečnosti a odolnosti Smart Grid infrastruktury:

- Nedostatečná připravenost personálu v oblasti OT kybernetické bezpečnosti, která je důsledkem chybějících nástrojů a prostředí umožňujících školení v realistickém prostředí.
- Absence bezpečného, ale realistického testovacího prostředí, které by umožnilo ověřovat bezpečnostní opatření bez ohrožení reálné infrastruktury.
- Omezená dostupnost realistických datasetů, potřebných pro vývoj, testování a validaci bezpečnostních mechanismů v prostředí Smart Grid.

Formální analýza technologického prostředí

Vytvořit abstraktní model vybraných částí energetické infrastruktury na základě architektury SGAM, zahrnující klíčová zařízení (např. RTU nebo IED) a komunikační standardy (IEC 61850 nebo IEC 60870-5-104). Analýza poskytne jednotný a srozumitelný přehled o technologickém prostředí, který je nezbytným základem pro efektivní školení odborníků. Přehledné uchopení architektury a souvisejících technologií umožní navrhnout školící a testovací scénáře, které budou realistické a budou zohledňovat specifika propojení IT a OT systémů. Tím přímo reaguje na Problém 1, kde je připravenost personálu, neboť bez této analytické fáze nelze vytvořit efektivní vzdělávací obsah ani pochopit komplexitu prostředí, ve kterém se odborníci pohybují. Zároveň tato analýza připraví podmínky pro návrh bezpečného testovacího prostředí (Problém 2).

Bezpečnostní analýza a identifikace nedostatků standardů

Provést detailní analýzu hrozeb pomocí metodik STRIDE a MITRE ATT&CK , a následně identifikovat, která rizika nejsou dostatečně pokryta stávajícími standardy. Výsledkem bude GAP analýza kyberbezpečnostních norem aplikovaných na energetickou infrastrukturu. Tato část umožní systematicky pojmenovat konkrétní zranitelnosti, které ohrožují Smart Grid infrastrukturu, a zároveň identifikovat oblasti, kde současné standardy poskytují nedostatečnou ochranu. Tímto cíl reaguje na Problém 2, neboť bez této analýzy nelze navrhnout smysluplné a realistické testovací prostředí. Zároveň pomáhá i při řešení Problému 3, protože identifikace bezpečnostních mezer umožní cíleně navrhnout mechanismy pro sběr relevantních dat bez nutnosti ohrožovat reálnou infrastrukturu.

Návrh a realizace sandbox architektury

Vyvinout realistické a modulární testovací prostředí (sandbox), umožňující simulaci provozu a útoků v bezpečném a kontrolovaném prostředí. Architektura bude podporovat interoperabilitu, škálovatelnost a různorodé výzkumné a tréninkové scénáře. Sandbox architektura poskytne bezpečný a zároveň realistický prostor pro výzkum i praktické ověřování bezpečnostních opatření, což v současné době v oblasti Smart Grid citelně chybí. Díky tomu bude možné školit odborníky, testovat zranitelnosti i ověřovat efektivitu obranných mechanismů bez zásahů do reálných systémů. Tento cíl reaguje Problém 1 (nutnost efektivního školení v realistickém prostředí) i Problém 2 (chybějící bezpečné testovací prostředí).

Scénáře pro školení a generování realistických datasetů

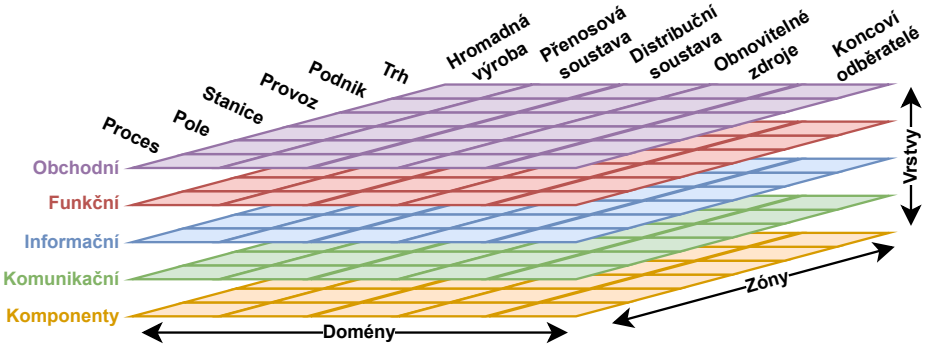
Navrhnout scénáře pro praktické školení odborníků a vývoj bezpečnostních opatření. Součástí bude generování reprezentativních datasetů v souladu s omezeními vyplývajícími z ochrany kritické infrastruktury a platné legislativy. Díky tomu bude možné překonat stávající bariéry v dostupnosti autentických dat a vytvořit podmínky pro vývoj, testování a validaci pokročilých detekčních mechanismů bez nutnosti ohrožovat provozní systémy nebo porušovat právní předpisy. Tento cíl tak přímo reaguje na Problém 1 (školení odborníků), Problém 2 (testování v realistickém prostředí) i Problém 3 (nedostupnost reálných datasetů).

3 Referenční model infrastruktury a komunikační architektura

S nástupem digitalizace v elektroenergetice a integrací heterogenních technologií vznikla potřeba jednotného rámce, který umožní systematické modelování architektury chytrých sítí. K tomu slouží architektonické modely, které umožňují formálně reprezentovat jednotlivé vrstvy energetického systému od fyzických zařízení přes komunikační infrastrukturu až po řídicí logiku a aplikační procesy. Pro oblast elektroenergetiky byl k tomuto účelu vyvinut SGAM (Smart Grid Architecture Model), který navazuje na principy modelu ISA-95 a reflektuje požadavky průmyslové konvergence IT a OT technologií v souladu s koncepcí Industry 4.0.

3.1 Smart Grid Architecture Model

SGAM [57] je formalizován v normě IEC SRD 63200 a byl navržen jako metodický rámec pro vizualizaci a standardizaci komplexních Smart Grid systémů. Hlavním cílem tohoto modelu je zajištění interoperability mezi jednotlivými technologiemi, zařízeními a vrstvami řízení v prostředí s více dodavateli a různorodými provozními režimy. Umožňuje modelovat architekturu pomocí tří dimenzí a pěti vrstev, které jsou navzájem provázané a tvoří jednotný referenční prostor. Díky této vícerozměrné struktuře je možné nejen popsat a analyzovat stávající infrastrukturu, ale také navrhovat nové systémy s ohledem na jejich funkční, komunikační i bezpečnostní požadavky. Model SGAM umožňuje identifikovat, ve které vrstvě se nacházejí konkrétní zařízení (např. ochrany, měřiče, komunikační jednotky), jakými protokoly komunikují (např. IEC 61850 nebo IEC 60870-5-104) a jaké bezpečnostní normy se jich týkají (např. IEC 62351 nebo IEC 62443). Struktura modelu SGAM je definován jako třírozměrný rámec, jak je zobrazeno na obrázku 3.1, jehož každá osa odpovídá jedné dimenzi architektury - Domény, Zóny a Vrstvy.



Obr. 3.1: Struktura SGAM modelu

SGAM model definuje pět vrstev, které reprezentují různé pohledy na systém chytré sítě od fyzické infrastruktury až po strategické řízení. Tyto vrstvy jsou orientovány ve směru hloubky a slouží ke strukturovanému zachycení funkcionality a datových vazeb.

- **Vrstva komponentů**: Zahrnuje veškerá fyzická zařízení systému například Inteligentní elektronická zařízení, Vzdálení terminálové jednotky, Rozhraní člověk-stroj, měřicí transformá-

tory, senzory. Je klíčová při návrhu architektury a při posuzování fyzické bezpečnosti a dostupnosti systémových prvků.

- **Komunikační vrstva**: Popisuje prostředky a protokoly sloužící pro přenos dat mezi jednotlivými komponentami. Zahrnuje jak linkové a síťové protokoly (např. Ethernet, TCP/IP), tak specifické průmyslové protokoly jako MMS, GOOSE nebo IEC 60870-5-104. Dále sem patří přenosové technologie (optika, metalika, BPL[1], Wi-Fi[2], LTE[3]) a zabezpečovací mechanismy (např. TLS [4], IPsec[5]).
- **Informační vrstva**: Zaměřuje se na strukturu a obsah přenášených informací. Obsahuje datové modely (např. CIM[6], SCL[7] z IEC 61850), formáty zpráv (např. XML, ASN.1[8]) a definice výměnných struktur (např. datasetů v GOOSE nebo logických uzlů v IED). Slouží jako vazba mezi logikou řízení a komunikační infrastrukturou.
- **Funkční vrstva**: Zachycuje logiku řízení, operace a interakce systémových funkcí nezávisle na jejich fyzickém umístění. Typickými příklady jsou automatická regulace napětí, řízení DER, detekce poruch, synchronizace sítě nebo predikce zátěže. Tato vrstva propojuje informační a obchodní logiku s reálnými procesy.
- **Obchodní vrstva**: Obsahuje ekonomické, regulační a organizační aspekty systémů. Popisuje vztahy mezi účastníky trhu , smluvní pravidla, obchodní strategie a provozní procesy z pohledu podnikání.

Domény v SGAM modelu reprezentují fyzické oblasti elektrizační soustavy, ve kterých dochází k výrobě, přenosu, distribuci a spotřebě elektrické energie. Domény tvoří horizontální osu modelu a sledují tok energie v síti.

- **Hromadná výroba**: Reprezentuje například jaderné, uhelné, plynové nebo vodní elektrárny.
- **Přenosová soustava**: Zahrnuje zařízení a procesy přenosu elektrické energie na velmi vysokém napětí. Patří sem rozvodny, transformátory a dispečerské řízení propojující regionální oblasti.
- **Distribuční soustava**: Pokrývá lokální rozvod elektřiny k odběratelům, typicky na hladinách VN a NN. Je charakteristická vyšší mírou decentralizace, integrací DER a vysokým počtem koncových zařízení.
- **Decentralizované zdroje**: Zahrnují lokální výrobní a akumulační jednotky jako jsou fotovoltaické elektrárny, větrné turbíny, bateriová úložiště nebo kogenerační jednotky. Často jsou připojeny v distribuční síti a vyžadují lokální řízení a ochranu.
- **Koncoví odběratelé**: Reprezentují koncové uživatele elektrické energie – domácnosti, firmy, průmyslové podniky. Zahrnují smart metering, řízení spotřeby a lokální automatizaci.

Zóny modelu SGAM rozdělují systém podle úrovně řízení a zpracování informací. Sledují hierarchii řízení od fyzických procesů po podnikové strategie a tržní mechanizmy.

- **Procesní úroveň (Proces)**: Nejnižší úroveň, která zahrnuje fyzikální jevy a zařízení pracující s elektrickým tokem. Patří sem vypínače, měřicí transformátory, vývody a ochranné prvky v reálném čase.
- **Úroveň pole (Pole)**: Obsahuje zařízení a systémy pro lokální řízení, jako jsou IED, relé, senzory a aktuátory. Tato úroveň realizuje primární ochranné a řídicí funkce bez nutnosti zásahu operátora.

[1] BPL – Broadband over Power Lines, vysokorychlostní komunikace po elektrickém vedení
[2] Wi-Fi – Wireless Fidelity, bezdrátová technologie pro přenos dat v lokální síti
[3] LTE – Long Term Evolution, standard mobilní sítě čtvrté generace (4G)
[4] TLS – Transport Layer Security, protokol pro zabezpečení datového přenosu
[5] IPsec – Internet Protocol Security, sada protokolů pro šifrování a autentizaci na síťové vrstvě
[6] CIM – Common Information Model, obecný model informací pro elektroenergetiku
[7] SCL – Substation Configuration Language, jazyk pro konfiguraci rozvoden dle normy IEC 61850
[8] ASN.1 – Abstract Syntax Notation One, standard pro popis struktury dat

- **Staniční úroveň (Stanice)**: Reprezentuje centralizované zpracování dat z pole pomocí RTU, SCADA nebo koncentrátorů. Na této úrovni dochází k agregaci měření, spínání a distribuci dat na vyšší vrstvy.
- **Provozní úroveň (Provoz)**: Zahrnuje dispečerské řízení provozu v reálném čase. Obsahuje systémy jako DMS[9] a EMS[10], které optimalizují provoz celé sítě.
- **Podniková úroveň (Podnik)**: Slouží k plánování, správě prostředků a strategickému řízení. Typicky zahrnuje ERP[11] systémy, fakturace, správa aktiv a systémovou integraci s IT.
- **Tržní úroveň (Trh)**: Nejvyšší úroveň, kde probíhá obchodování s elektřinou, aukce služeb výkonové rovnováhy a řízení flexibility. Zahrnuje i vztahy mezi různými účastníky trhu (obchodníci, TSO[12]/DSO[13]).

3.2 Klíčové prvky architektury elektroenergetických sítí

V prostředí elektroenergetiky existuje několik klíčových zařízení, která tvoří architekturu řídicích a komunikačních prvků pro dohled a ovládání. SGAM popsaný v předchozí kapitole umožňuje tato zařízení zařadit do různých zón a vrstev podle jejich funkce. Následující podkapitoly stručně charakterizují hlavní komponenty – Inteligentní elektronické zařízení, Vzdálená terminálová jednotka, Slučovací jednotka, Rozhraní člověk-stroj a Dispečerské řízení a sběr dat.

3.2.1 Inteligentní elektronické zařízení

Inteligentní elektronické zařízení (IED) je určené k ochraně, ovládání a automatizaci prvků elektrické sítě. IED získává data ze senzorů (např. proudových a napěťových transformátorů) a z připojených zařízení v síti a na základě zpracování těchto údajů může vydávat řídicí povely, typicky například rozpojit jistič při zjištění nadměrného proudu, podpětí nebo jiné poruchové události. Mezi běžné typy IED patří digitální ochranná relé, řídicí jednotky transformátorů, regulátory napětí nebo ovladače kondenzátorových baterií. Funkce a struktura IED jsou definovány v normách IEC 61850-5 [127] (funkční požadavky) a IEC 61850-7-4 [121] (logické uzly a datové třídy).

- **Vstupy**: Analogové vstupy z měřicích transformátorů (proudové a napěťové signály) a další senzorová data (např. teploty), dále digitální vstupy pro stavová hlášení (polohy spínačů, ochranné signály apod.). Vstupní datové struktury jsou modelovány podle logických uzlů stanovených v IEC 61850-7-4.
- **Výstupy**: Ovládací povely pro primární zařízení (např. sepnutí), signály pro vyšší systémy (alarmy, indikace) a případně analogové výstupy pro měření. Mechanismy pro výměnu výstupních dat jsou specifikovány v rámci ACSI (Abstract Communication Service Interface) dle IEC 61850-7-2 [119].
- **Komunikace**: Typicky ethernetové nebo sériové porty s podporou standardních protokolů. Vestavěná podpora bývá zejména pro MMS (v rámci IEC 61850), GOOSE a Sampled Values, což umožňuje IED komunikovat přímo s dalšími IED v rozvodně nebo s nadřazenými zařízeními (např. SCADA). Komunikační požadavky a chování jsou popsány v IEC 61850-5, mapování na síťové protokoly je řešeno v IEC 61850-8-1 [113].

[9] DMS – Distribution Management System, systém pro řízení distribuční sítě
[10] EMS – Energy Management System, systém pro řízení přenosové soustavy
[11] ERP – Enterprise Resource Planning, podnikové plánování zdrojů
[12] TSO – Transmission System Operator, provozovatel přenosové soustavy
[13] DSO – Distribution System Operator, provozovatel distribuční soustavy

- **Umístění v architektuře**: IED se nasazují převážně u rozvoden a stanic. V kontextu modelu SGAM spadají do procesní a polní zóny, kde přímo interagují s čidly a akčními členy (primárními prvky) a zajišťují lokální ochranné a řídicí funkce.

3.2.2 Vzdálená terminálová jednotka

RTU (Remote Terminal Unit) neboli vzdálená terminálová jednotka je specializované elektronické zařízení určené pro sběr dat v terénu a dálkové ovládání technologických uzlů, zejména v rámci SCADA systémů. Jedná se o jednotku, která bývá nasazena ve vzdálených lokalitách (např. v distribučních trafostanicích, rozvodnách apod.), která zprostředkovává komunikaci mezi lokálními senzory/zařízeními a centrálním dispečinkem. RTU typicky shromažďuje měřená data a stavové informace ze svého okolí a prostřednictvím komunikační linky je odesílá do SCADA systému. Zároveň přijímá ze SCADA řídicí povely, které vykonává například zapnutí či vypnutí jističe, změnu nastavení regulace, reset alarmu apod. Konstrukčně jde často o průmyslový počítač. Popis funkcí RTU je standardizován v rámci protokolů IEC 60870-5-101 [104] a IEC 60870-5-104 [114], které definují způsob přenosu měřených a stavových dat mezi RTU a nadřazeným SCADA systémem. V případě použití RTU ve staničním systému se mohou uplatnit i principy modelování dle IEC 61850-7-2 [119].

- **Vstupy**: Měřené veličiny a binární signály z prostředí například napětí, proud, kmitočet, teplota, poloha vypínačů, aktivace ochran či poruchové stavy. Vstupy mohou být připojeny přímo (I/O moduly), nebo zprostředkovány přes podřízené jednotky jako IED. Struktura vstupních dat, formát měřených veličin i přenos binárních stavů jsou definovány v normě IEC 60870-5-104 [114].
- **Výstupy**: Binární (digitální) výstupy, kterými RTU ovládá pole – zejména výkonové spínací prvky (vypínače, odpojovače), přepínače a pomocná zařízení. Typizace povelových rámců, sekvenční řízení a potvrzení povelů jsou specifikovány v normách IEC 60870-5-101 a IEC 60870-5-104.
- **Komunikace**: RTU jednotky bývají vybaveny ethernetovým, sériovým nebo bezdrátovým rozhraním a komunikují prostřednictvím IEC 60870-5-104, případně MMS v prostředí IEC 61850 [113]. RTU často slouží jako překladová vrstva mezi IED a nadřazenými systémy. Architektura, typická síťová topologie RTU a příklady jejich funkcí a integrace do SCADA systému jsou detailně popsány v technické specifikaci IEEE Std 1379-2000 [94].
- **Umístění v architektuře**: RTU jednotky se nasazují do vzdálených lokalit, např. trafostanic, rozvoden apod. V SGAM modelu se RTU pohybuje mezi procesní, polní a staniční zónou, přičemž slouží jako rozhraní mezi fyzickým světem a nadřazeným dispečerským řízením.

3.2.3 Slučovací jednotka

Merging Unit (MU) neboli slučovací jednotka je zařízení, které umožňuje realizovat digitální procesní sběrnici v rozvodnách převodem analogových měřicích signálů na standardizovaná digitální data, jak je např. definována v normě IEC 61850-9-2 [124]. MU je zpravidla umístěna mezi klasickými měřicími transformátory proudu a napětí a ochrannými či řídicími IED. Jeho úkolem je vzorkovat analogové signály (např. fáze proudu a napětí), případně doplnit binární informace (stav vypínače, pomocné kontakty) a sloučit je do časově synchronizovaného datového proudu.

- **Vstupy**: Analogové signály z měřicích převodníků (třífázové proudy a napětí), které jsou převáděny na digitální vzorky v souladu s požadavky normy IEC 61850-9-2. MU také mívají binární vstupy pro připojení signálů (např. stav vypínače, spouštěč ochrany apod.), jež mohou být přenášeny např. pomocí protokolu GOOSE [113].

- **Výstupy**: Digitální datové toky publikované do procesní sběrnice. Hlavním výstupem jsou vzorkované hodnoty proudů a napětí, které jsou vysílány formou multicastových zpráv Sampled Values definovaných v IEC 61850-9-2. Některé MU mohou současně generovat i binární výstupní zprávy pomocí GOOSE.
- **Komunikace**: Komunikační rozhraní MU je typicky realizováno prostřednictvím ethernetového portu s podporou Sampled Values, kde vyžadovaná přesná časová synchronizace jsou zajištěny protokolem PTP dle IEEE 1588 [96]. Komunikační charakteristiky, požadovaná latence a časová závislost této komunikace jsou popsány v normě IEC 61850-5 [127].
- **Umístění v architektuře**: Merging Unit se nasazuje v rozvodnách na procesní úrovni. Fyzicky bývá umístěna buď v blízkosti měřicích transformátorů, nebo v řídicí budově stanice poblíž ochranných přístrojů. V SGAM spadá MU do procesní zóny, neboť tvoří bezprostřední rozhraní mezi primární technologií (senzory, akční členy) a sekundární digitální infrastrukturou stanice.

3.2.4 Rozhraní člověk-stroj

HMI (Human-Machine Interface) je rozhraní, skrze které obsluha (operátor) komunikuje s řídicím systémem nebo zařízením. HMI poskytuje operátorovi informace o stavu systému či probíhajícího procesu a zároveň umožňuje zadávání vstupů, povelů nebo parametrů do systému. V praxi HMI představuje nejčastěji počítačový terminál s displejem a ovládacími prvky, na kterém běží vizualizační a ovládací software. Samotné HMI neprovádí řízení procesu automaticky, pouze zobrazuje data a zprostředkuje přenos akcí operátora do tohoto systému. Typickým příkladem HMI v energetice je například dispečerský ovládací panel SCADA systému nebo místní panel rozvodny (elektrické stanice), kde může pracovník zobrazit schéma zapojení, hodnoty proudů a napětí, stav zařízení, alarmy atd., a případně na dálku ovládat prvky (otevřít vypínač, změnit nastavení relé apod.). Komunikační propojení HMI s ostatními systémy je standardizováno např. pomocí MMS dle normy IEC 61850-8-1 [113] nebo IEC 60870-5-104 [114], které zajišťují přenos měřených i stavových dat a povelů.

- **Vstupy**: Vstupem do HMI jsou typicky uživatelské akce, například kliknutí, zadání příkazu, změna parametru nebo potvrzení alarmu. Fyzicky jsou realizovány prostřednictvím klávesnice, myši, dotykové obrazovky nebo speciálních ovládacích prvků. Zpracování těchto událostí je v systémech dle IEC 61850 modelováno pomocí ACSI rozhraní [119].
- **Výstupy**: HMI vizualizuje aktuální stav systému, kde zobrazuje hodnoty měření (např. napětí, proudy, výkon), topologii sítě, alarmy, chybové stavy, provozní režimy a další diagnostická data. Výstupem je tedy grafické zobrazení v reálném čase sloužící operátorovi k rozhodování, sledování systému a ručnímu řízení. Formát a struktura zobrazovaných dat jsou definovány v IEC 61850-7-3 [120].
- **Komunikace**: HMI rozhraní je připojeno k řídicímu systému prostřednictvím vnitřní sítě nebo sběrnice. V lokálních aplikacích komunikuje přímo se staničním řídicím systémem nebo IED, často pomocí MMS protokolu dle IEC 61850-8-1. V dispečerských centrech je HMI obvykle klientská aplikace napojená na centrální SCADA servery po LAN, kde se může uplatňovat IEC 60870-5-104. Pro samotnou vizualizaci může HMI využívat webové technologie nebo proprietární protokoly výrobce. Komunikační latence a požadavky na aktuálnost dat jsou popsány v IEC 61850-5 [127].
- **Umístění v architektuře**: HMI se vyskytuje na stanovištích obsluhy, lokálně v rozvodně nebo centrálně v dispečerském centru. Z pohledu SGAM lze HMI řadit do staniční zóny (lokální ovládání) či do provozní zóny (centrálního řízení).

3.2.5 Dispečerské řízení a sběr dat

SCADA (Supervisory Control and Data Acquisition) je nadřazený dohledový a řídicí systém, který z centrálního pracoviště monitoruje technologická zařízení a procesy a umožňuje jejich dálkové ovládání. V energetice představuje SCADA klíčový nástroj dispečerského řízení, typicky v národních nebo regionálních dispečincích provozovatelů přenosové a distribučních sítí. SCADA průběžně přijímá data z rozsáhlé sítě dálkových terminálů (RTU) nebo přímo z inteligentních zařízení v poli (IED) a ukládá je do databází. Na základě těchto informací pak operátoři skrze SCADA HMI dohlížejí na provoz a mohou na dálku vydávat povely k ovládání prvků (sepnutí/rozepnutí vedení, nastavení transformátorů apod.). Architektura SCADA systémů a jejich základní komponenty jsou popsány například v IEEE Std 1379-2000 [95].

SCADA se skládá z několika vrstev a komponent. Jádrem je řídicí jednotka, často realizovaná softwarově na SCADA serveru. Tato centrální jednotka označovaná též jako MTU (Master Terminal Unit) komunikuje se všemi podřízenými stanicemi a zpracovává od nich přijatá data. Data jsou ukládána v databázích (historian[14], real-time database[15]), odkud jsou dále přístupná pro vizualizaci, analýzy a archivaci. Důležitou součást tvoří operátorské stanice v dispečerské místnosti, kde operátoři mají jeden či více terminálů s grafickým rozhraním, kde vidí informace ze sítě a mohou ovládat zařízení na dálku.

- **Vstupy**: Vstupem do SCADA systému jsou data přijímaná z terénních zařízení, přenášená prostřednictvím průmyslových komunikačních protokolů. Nejčastěji se jedná o IEC 60870-5-104 [114] (v přenosové a distribuční síti) a MMS dle IEC 61850-8-1 [113] (v rámci staničních systémů). Přijatá data zahrnují provozní stavové informace (např. polohy vypínačů, poruchové stavy), měřené hodnoty (např. napětí, proud, kmitočet) a binární signály (např. alarmy, blokování). Vstupem mohou být rovněž operátorské akce zadané přes HMI, např. změny konfigurace, potvrzení alarmů nebo příprava ovládacích povelů, jak je definováno v rámci rozhraní ACSI dle IEC 61850-7-2 [119].
- **Výstupy**: Výstupy SCADA systému představují logické řídicí povely adresované podřízeným prvkům, které jsou odesílány prostřednictvím komunikačních protokolů, zejména IEC 60870-5-104, případně MMS dle IEC 61850-8-1. Tato data určují požadovaný stav nebo operaci (např. otevření vypínače, změna nastavení transformátoru, reset výstrahy) a jsou směrována do zařízení typu RTU nebo IED, které je vykonají. Kromě toho SCADA vizualizuje výstupy uživatelům (např. výsledky akcí, potvrzení změn, alarmové stavy) a poskytuje data dalším systémům, jako jsou EMS, DMS nebo nástroje plánování a reportingu.
- **Komunikační protokoly**: SCADA využívá řadu telemetrických protokolů pro komunikaci s RTU a IED v terénu. V Evropě je standardem IEC 60870-5-104. RTU jednotky v elektrických stanicích často zajišťují překlad mezi IEC 60870-5-104 a IEC 61850. U menších systémů může být IEC 60870-5-104 použit přímo až ke koncovým prvkům jako je IED. RTU v těchto případech integrují i ochranné funkce.
- **Umístění v architektuře**: SCADA představuje vrstvu provozního řízení, která sedí nad staničními a polními systémy: využívá údaje z jednotlivých stanic (RTU, IED) a vydává jim agregované povely. V SGAM modelu odpovídá provozní zóně.

[14] Systém pro sběr, ukládání a správu dat.
[15] Systém, který je schopen ukládat a zpracovávat data v reálném čase.

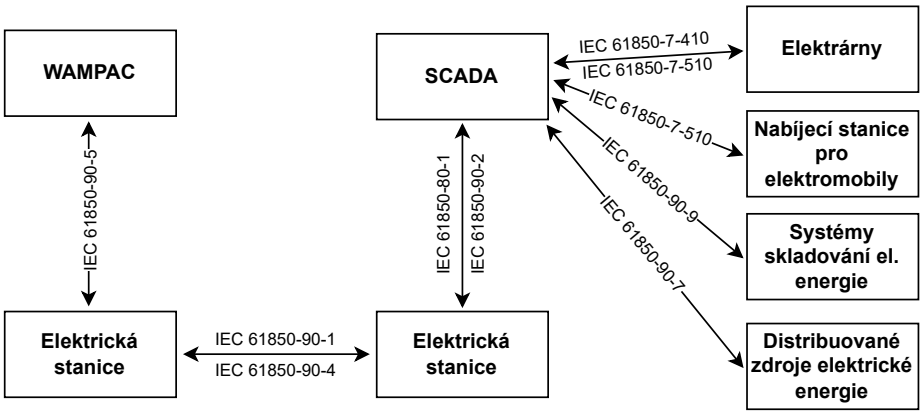
3.3 Komunikační protokoly v elektroenergetice

Tato kapitola představuje hlavní komunikační standardy používané v elektroenergetice, jejich strukturu, datové modely, aplikační vrstvy i specifická rozšíření pro bezpečnost a redundanci. Detailně jsou popsány protokoly definované v rámci standardů **IEC 61850** a **IEC 60870**, které tvoří komunikační páteř současných i budoucích chytrých energetických systémů.

3.3.1 Standard IEC 61850

IEC 61850 je mezinárodní norma, která definuje komunikační protokoly pro inteligentní elektronická zařízení v elektrických rozvodnách. Normy se zabývají datovou komunikací v přenosové a distribuční soustavě až po integraci distribuovaných energetických zdrojů do elektrické sítě. Obrázek 3.2 znázorňuje přehledovou architekturu komunikačních vazeb mezi jednotlivými komponentami elektroenergetické soustavy dle standardu IEC 61850 a jeho rozšíření. Norma původně zaměřená na automatizaci rozvoden byla postupně rozšířena o další části, které zajišťují interoperabilitu mezi systémy vyšších vrstev (SCADA, WAMPAC[16]) i mezi různými typy zařízení (např. distribuované zdroje, elektromobilita, úložiště energie). Ve středu diagramu se nachází Elektrická stanice, která využívá základní části IEC 61850-8-1 [113] a rozšíření IEC 61850-90-1 [122] a 90-4 [139] pro komunikaci s dispečerským systémem SCADA. Tato stanice také komunikuje s WAMPAC systémy pomocí profilu IEC 61850-90-5 [126], který je optimalizován pro vysokorychlostní přenos dat z PMU[17]. SCADA jako centrální řídicí systém plní roli integrátora. Komunikuje nejen s rozvodnami, ale i s nadřazenými nebo paralelními systémy. Pomocí různých částí standardu IEC 61850-7-410 [125], 7-510 [144], 90-7 [146] a 90-9 [140] je schopna navázat komunikaci s:

- **Elektrárnami**: prostřednictvím IEC 61850-7-410, která pokrývá modelování DER a elektrických výrobních jednotek,
- **Nabíjecími stanicemi pro elektromobily**: dle IEC 61850-7-510, která definuje objektové modely pro řízení nabíjecí infrastruktury,
- **Systémy skladování energie**: jsou modelovány a řízeny pomocí rozšíření IEC 61850-90-9,
- **Distribuovanými energetickými zdroji**: dle IEC 61850-90-7, které specifikuje způsob integrace a řízení DER v síti.



Obr. 3.2: Komunikační model IEC 61850

[16]Wide Area Monitoring, Protection and Control, System pro monitorování a řízení energetických sítí.

[17]Phasor Measurement Unit - zařízení, které měří fázory (napětí a proudu) v energetických soustavách s vysokou přesností a časovou synchronizací

IEC 61850 poskytuje úplný rámec pro návrh, specifikaci, implementaci a provozní požadavky systémů automatizace elektrické infrastruktury. To zahrnuje aspekty inženýrství, datové modely a bezpečnostní komunikační mechanismy. Hlavním využitím v současné době je v rámci elektrických stanic, kde zahrnuje specifické protokoly jako jsou GOOSE (Generic Object Oriented Substation Event) a Sampled Values, a nebo MMS (Manufacturing Message Specification).

Manufacturing Message Specification

Manufacturing Message Specification (MMS) [113] je komunikační protokol vyvinutý pro průmyslové a energetické aplikace, vycházející ze standardu ISO 9506 [155]. V rámci standardu IEC 61850, MMS zastupuje jeden z klíčových protokolů pro výměnu informací mezi zařízeními v elektrických rozvodnách nebo umožňuje komunikaci s nadřazeným dohledovým centrem. MMS byl vybrán pro standard IEC 61850 z důvodů jeho schopnosti podporovat komplexní a bezpečnou komunikaci mezi zařízeními různých výrobců, což je nezbytné pro interoperabilitu v moderních elektrických rozvodnách.

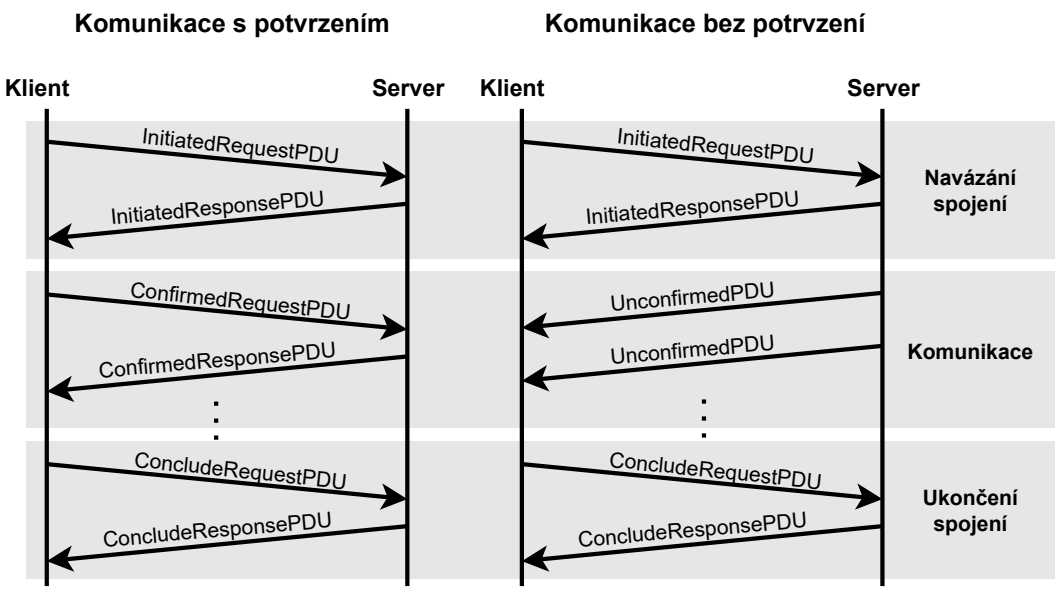
Jádrem MMS protokolu je Virtual Manufacturing Device (VMD), která představuje abstraktní reprezentaci průmyslového zařízení nebo systému. Tento koncept je klíčový pro poskytování jednotného a standardizovaného rozhraní pro komunikaci a interakci s různými fyzickými zařízeními v průmyslovém prostředí. VMD funguje jako abstrakce skutečných zařízení, umožňující MMS efektivně komunikovat s různými typy zařízení bez nutnosti znát detaily jejich interního fungování.

Samotná struktura MMS je založena na objektově orientovaném přístupu, který umožňuje reprezentaci širokého spektra datových typů a služeb. Protokol definuje různé typy objektů, které reprezentují různé funkce a data v systému. Každý objekt má své specifické vlastnosti a metody, což umožňuje detailní a efektivní manipulaci s daty a procesy. Reálná data, jako jsou měření, stavové informace, konfigurační parametry a další, jsou reprezentována a spravována prostřednictvím MMS Server Objektů. Tyto objekty fungují jako abstraktní vrstva, která mapuje reálná data do strukturované a přístupné formy. Data jsou tak snadno přístupná pro MMS klienty, kteří pak mohou číst nebo zapisovat tato data prostřednictvím standardizovaných MMS služeb. Díky této abstrakci umožňují objekty jednotný a konzistentní přístup k datům napříč různými typy a modely zařízení. Tím se zjednodušuje integrace různých systémových komponent a zajišťuje se vysoká úroveň interoperability a flexibility.

Komunikace V rámci ISO/OSI modelu se MMS řadí do aplikační vrstvy (7. vrstva ISO/OSI). V této vrstvě MMS poskytuje rozhraní pro výměnu dat a řízení komunikace mezi aplikacemi. MMS využívá klient-server model komunikace. Zprávy kategorizovány do dvou hlavních skupin: **Confirmed MMS Services** a **Unconfirmed MMS Services**, jak je zobrazeno na obrázku 3.3.

Confirmed MMS Services zahrnují zprávy, které vyžadují potvrzení od přijímače. Tyto služby jsou nezbytné pro operace, kde je důležité získat zpětnou vazbu o úspěchu nebo selhání požadavku. Například, služby jako Read a Write se používají k získání nebo změně dat v jiném zařízení, zatímco operace jako Create a Delete umožňují správu objektů v systému.

Unconfirmed MMS Services jsou zprávy, které nepotřebují potvrzení od přijímajícího zařízení. Tyto služby se využívají pro přenos informací, které nevyžadují okamžitou reakci, jako jsou informační zprávy nebo oznámení o událostech. Služby jako InformationReport a EventNotification poskytují důležité informace o stavu a událostech v systému bez potřeby zpětné vazby.



Obr. 3.3: Struktura komunikace protokolu MMS

Generic Substation State Events (GSSE) GSSE je definován pro velmi rychlý přenos binárních stavových informací, typicky ve formě bitových řetězců. Používá se zejména pro distribuci jednoduchých stavových signálů mezi zařízeními, jako jsou indikace zapnuto/vypnuto, stavy ochran nebo alarmy. GSSE je založen na pevném formátu a je popsán ve starší části standardu IEC 61850-8-1, ale jeho použití je postupně nahrazováno univerzálnějším GOOSE [113].

Generic Substation Events

Správný chod energetických systémů je závislý na rychlosti reakce zařízení, která zajišťují jejich řízení a ochranu. Tento požadavek se přenáší také na datovou komunikaci, kde je nezbytné rychlé doručení zpráv o událostech mezi zařízeními. Pro tyto účely definuje norma IEC 61850 komunikační model Generic Substation Events (GSE), který umožňuje rychlou a spolehlivou distribuci vstupních a výstupních hodnot v rámci celého systému. Model GSE podporuje decentralizovanou výměnu informací mezi zařízeními pomocí multicast nebo broadcast přenosu. GSE je specifikován v části IEC 61850-7-2 [119], která popisuje aplikační vrstvu komunikace. Model GSE se dělí na dvě varianty podle použité reprezentace a přenosu dat: **Generic Substation State Events (GSSE)** a **Generic Object Oriented Substation Events (GOOSE)**.

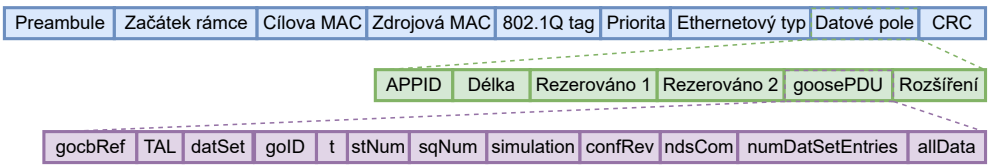
Generic Substation State Events GSSE je definován pro velmi rychlý přenos binárních stavových informací, typicky ve formě bitových řetězců. Používá se zejména pro distribuci jednoduchých stavových signálů mezi zařízeními, jako jsou indikace zapnuto/vypnuto, stavy ochran nebo alarmy. GSSE je založen na pevném formátu a je popsán ve starší části standardu IEC 61850-8-1, ale jeho použití je postupně nahrazováno univerzálnějším GOOSE.

Generic Object Oriented Substation Events GOOSE představuje zásadní prvek v komunikačních modelu standardu IEC 61850. Protokol byl navržen s cílem poskytnout rychlou, spolehlivou a efektivní komunikaci mezi inteligentními elektronickými zařízeními v rozvodně. GOOSE umožňuje v reálném čase sdílet důležité informace, jako jsou stavové změny, alarmy, měření a řídicí

signály, s minimálním zpožděním. Tato vlastnost je kritická pro aplikace vyžadující okamžité reakce, jako jsou např. systémy ochrany a automatizace rozvodných sítí. GOOSE je detailně definován v části IEC 61850-7-2 [119] a jeho komunikace na linkové vrstvě v IEC 61850-8-1 [113].

Zprávy GOOSE se obvykle přenášejí prostřednictvím ethernetové sítě a jsou distribuovány v multicastovém režimu, kde je využit komunikační model Vydavatel-Odběratel. Tento přístup zvyšuje efektivitu a snižuje reakční dobu v kritických situacích. V rámci protokolu GOOSE je kladen velký důraz na bezpečnost a spolehlivost. Mechanismy, jako jsou časové známky a sekvenční čísla, zajistí, že data jsou aktuální, přesná a vysílána ve správném pořadí. Tyto funkce jsou zásadní pro zajištění spolehlivosti a integritety dat v systémech, kde je důležitá rychlá reakce na události. GOOSE poskytuje také vysokou míru flexibility v konfiguraci, umožňující uživatelům nastavit priority, skupinové adresace a periodické vysílání zpráv podle specifických potřeb rozvodné sítě. Tato flexibilita a adaptabilita činí GOOSE nezbytným nástrojem pro moderní a efektivní správu a provoz elektrických rozvodných systémů.

Zprávy GOOSE využívají tři vrstvy referenčního modelu ISO/OSI, a to fyzickou, spojovou a aplikační vrstvu. Struktura od Ethernetového rámce až po GOOSE data je zobrazena na obrázku 3.4. Na spojové vrstvě je GOOSE zapouzdřena do Ethernetového rámce 802.3. V ethernetovém rámci je důležité pole **Ethernetový typ**, které určuje typ zapouzdřených dat. V případě GOOSE zprávy se jedná o typ s označením **0x88b8**.



Obr. 3.4: GOOSE struktura paketu

Hlavička zprávy se skládá:

- **APPID** (application identifier), které identifikuje cílovou aplikaci, skládá se ze dvou bitů a pro GOOSE Type 1 nabývá hodnoty 00 a pro GOOSE Type1A (Trip) hodnoty 10.
- **Délka** udává délku zprávy, která je limitovaná velikostí datové části ethernetového rámce.
- **Reserved1** a **Reserved2**. Reserved 1 je rozděleno na tři části Simulation, Reserved a Reserved Security. Simulation bylo v hlavičce specifikováno, aby umožnilo výkonné filtrování na úrovni spojové vrstvy. Reserved je vyhrazeno pro budoucí standardizované použití a v současné době musí být nastaveno na hodnotu 0. Reserved Security je vyhrazeno bezpečnostní normou IEC 62351-6 [141]. V případě, že je GOOSE přenášeno se zabezpečením, tak je nastaveno dle této normy, jinak je nastavena hodnota 0. Druhé rezervní pole Reserved 2 se nastavuje dle kritérií stejné bezpečnostní normy, pokud je GOOSE přenášeno se zabezpečením, v opačném případě je také nastaveno na hodnotu 0.

Následuje goosePDU obsahující strukturovaná přenášena data a je rozdělen pole:

- **gocbRef** (GOOSE Control Block Reference) odkazuje na konfigurační element GOOSE. Tento odkaz propojuje konkrétní GOOSE zprávu s její definicí v SCL souboru, čímž přijímajícímu zařízení umožňuje správně interpretovat strukturu a obsah zprávy.
- **TAL** (Time Allowed to Live) definuje časový interval, po kterém se zpráva stává neplatnou. Hodnota TAL slouží k detekci ztráty spojení nebo chyb v přenosu, jelikož po jejím překročení by měly být příslušné procesy uvedeny do bezpečného stavu.
- **DatSet** odkazuje na sadu dat, která je součástí zprávy, a obsahuje informace, které se mají sdílet. Každý dataset je definován v konfiguraci stanice a může zahrnovat kombinaci měřených

hodnot, binárních stavů a výstupních povelů.

- **goID** je identifikátor zprávy, který pomáhá při jejím sledování a identifikaci. Tento identifikátor zajišťuje jednoznačné rozlišení mezi více GOOSE instancemi běžícími v jedné síti.
- **stNum** (Status Number) je číslo, které se zvyšuje s každou novou zprávou a indikuje novou stavovou změnu. Díky stNum mohou přijímací zařízení rychle poznat, zda se obsah přenášených dat změnil oproti předchozímu stavu.
- **sqNum** (Sequence Number) je sekvenční číslo zprávy, které se zvyšuje s každým odesláním zprávy a slouží k určení pořadí zpráv. V kombinaci s parametrem stNum pomáhá při detekci ztracených nebo přijatých zpráv mimo pořadí.
- **simulation** určuje, zda byla (True) nebo nebyla (False) vydána zpráva simulační jednotkou. Díky tomu pole simulation umožňuje zařízením vysílat a přijímat GOOSE zprávy v kontrolovaném testovacím prostředí bez toho, aby tyto zprávy měly skutečný vliv na provoz rozvodny, což je zásadní pro školení a testování bez rizika pro reálný provoz.
- **confRev** (Configuration Revision) udává verzi konfiguračního souboru GOOSE zprávy. Hodnota se inkrementuje např. při změně nebo vymazání části datové sady a umožňuje příjemci ověřit, že pracuje s aktuální konfigurací.
- **ndsCom** (Needs Commission) je příznak nabývající hodnoty True nebo False a určuje, zda je potřeba zprávu dále konfigurovat nebo ověřit. To může být využito např. při procesu nasazování nebo úprav systému, kde mohou být vyžadovány další kroky pro zajištění správné funkčnosti, jako je rekonfigurace IED.
- **numDatSetEntries** (Number of DataSet Entries) specifikuje počet položek obsažených v DatSet, což umožňuje přijímacím zařízením pochopit rozsah přijatých dat. Tato informace je užitečná pro ověření úplnosti zprávy a konzistence s očekávanou konfigurací.
- **allData** obsahuje samotná data, která jsou přenášena, včetně měření, stavů a dalších relevantních informací. Struktura allData odpovídá definici datasetu a může zahrnovat jak okamžité hodnoty, tak indikátory událostí.
- **Rozšíření** představují volitelnou část GOOSE zprávy, která umožňuje přidat dodatečné informace specifické pro danou aplikaci nebo výrobce. Typicky se využívá pro přenos nestandardních diagnostických údajů, metadat o měření, informací o zdroji dat či dalších stavových indikátorů, které nejsou součástí základního datasetu. Rozšíření zachovávají kompatibilitu se standardními implementacemi. Zařízení, která je neznají, je mohou ignorovat, zatímco zařízení s jejich podporou je mohou využít pro detailnější analýzu nebo pokročilé funkce.

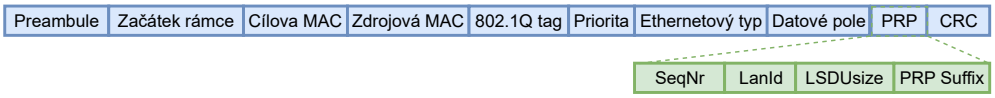
Parallel Redundancy Protocol (PRP) a High-availability Seamless Redundancy (HSR) v rámci protokolu GOOSE Pro zajištění vysoké dostupnosti a odolnosti proti výpadkům v průmyslových sítích, zejména v aplikacích typu ochrany a řízení elektrických rozvoden, jsou klíčové technologie bezproblémové redundance. Standard IEC 62439-3 [145] definuje dva základní mechanismy, které umožňují bezvýpadkové přepínání komunikačních cest v případě poruchy – Parallel Redundancy Protocol a High-availability Seamless Redundancy. Oba protokoly jsou navrženy tak, aby poskytovaly bezvýpadkové doručení datových rámců, což je zvláště důležité pro protokol GOOSE, kde se očekává extrémně nízká latence a vysoká spolehlivost.

PRP umožňuje simultánní přenos dvou identických kopií každého datového paketu přes dvě oddělené a nezávislé ěsítě. Pokud dojde k selhání v jedné síti, druhá síť zajistí, že data dorazí do cíle bez zpoždění, což zajišťuje bezproblémovou a nepřetržitou komunikaci. HSR je obdobný PRP, ale je navržen pro síťové topologie ve tvaru kruhu. Při HSR se každý paket posílá dvěma směry po kruhu a dorazí do cíle oběma cestami. Pokud dojde k výpadku na jedné části kruhu, pakety stále dorazí do cíle druhou cestou.

Protokol GOOSE je určen pro rychlý a spolehlivý přenos událostí a stavových informací v elektrických rozvodnách. Spolehlivost a nepřetržitá dostupnost jsou pro GOOSE zásadní, zvláště v aplikacích jako je ochrana a automatizace rozvodných systémů. PRP a HSR lze použít v rámci ethernetového rámce s GOOSE, aby se zvýšila spolehlivost a dostupnost síťové komunikace. V případě výpadku v jedné části sítě zajistí PRP nebo HSR, že GOOSE zprávy budou stále doručeny do cíle bez zpoždění nebo ztráty dat.

V případě využití PRP je ethernetový rámec rozšířen o pole PRP, jak je zobrazeno na obrázku 3.5, která obsahuje pole:

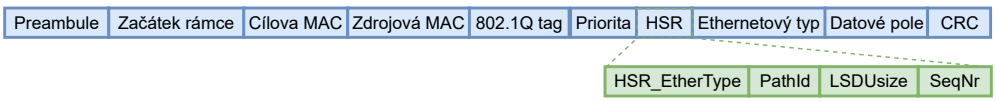
- **SeqNr** (Sequence Number) je sekvenční číslo, které se používá k identifikaci jednotlivých Ethernetových rámců v rámci PRP. Toto číslo umožňuje přijímacímu zařízení rozlišit mezi dvěma kopiemi toho samého rámce, které dorazily přes odlišné redundantní cesty.
- **LanID** (LAN Identifier) identifikuje, přes kterou síť (LAN a nebo LAN B) byl rámec odeslán. Tato informace je klíčová pro správné zpracování redundantních rámců a zajišťuje, že systém může efektivně spravovat přenos dat přes obě sítě.
- **LSDU Size** (Length of Service Data Unit) udává délku datového obsahu obsaženého v Ethernetovém rámci. Tento údaj je důležitý pro správné zpracování a dekódování přijatých dat.
- **PRP Suffix** je speciální přípona přidávaná na konec Ethernetového rámce v rámci PRP. Obsahuje výše zmíněné informace (SeqNr, LanID a LSDU Size) a je klíčová pro funkci PRP, neboť umožňuje redundantní a bezpečný přenos dat.



Obr. 3.5: PRP rozšíření Ethernetového rámce

Rozšíření ethernetového rámce dle HSR je velmi podobné, jak je zobrazeno na obrázku 3.6, která obsahuje pole:

- **HSR_EtherType** (HSR Ethernet Type) pole slouží jako identifikátor, který umožňuje síťovým zařízením rozpoznat HSR rámec a správně ho zpracovat podle pravidel HSR protokolu.
- **PathId** (Path Identifier) je identifikátor cesty, který označuje, kterou cestou kruhové topologie HSR byl rámec odeslán. V HSR sítích, kde jsou data posílána dvěma směry, toto pole pomáhá sledovat cestu každého rámce a zajišťuje správné doručení dat i v případě výpadku na jedné z cest.
- **LSDUsize** (Length of Service Data Unit) určuje délku datového obsahu přenášeného v rámci HSR rámce. Tato informace je nezbytná pro správné zpracování dat přijímanými zařízeními.
- **SeqNr** (Sequence Number) je sekvenční číslo rámce, které se používá pro identifikaci a řazení přijatých rámců. V HSR sítích, kde mohou být data doručována oběma směry kruhu, SeqNr pomáhá zajistit, že jsou data správně mapována a žádný rámec není ztracen nebo duplikován.

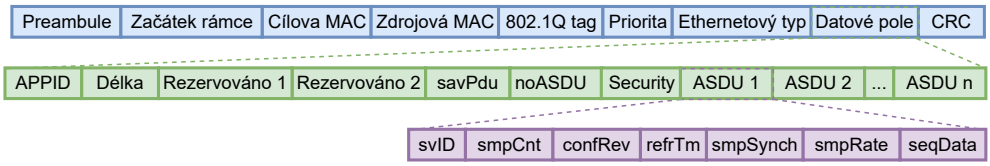


Obr. 3.6: HSR rozšíření Ethernetového rámce

Sampled Values

Protokol Sampled Values (SV), definovaných ve standardu IEC 61850-9-2 [124], je v rámci standardu IEC 61850 zásadní pro přenos digitalizovaných analogových dat, jako jsou napětí, proud a další měřené fyzikální veličiny. Tento protokol je navržen pro rychlý a real-time přenos měřených dat, což je nezbytné pro aplikace vyžadující okamžité reakce, jako jsou systémy ochrany a kontrolní systémy. SV poskytuje standardizovaný formát pro digitalizovaná data, což umožňuje kompatibilitu a jednotnou komunikaci mezi různými zařízeními a systémy. Zprávy SV jsou typicky distribuovány pomocí multicastu přes Ethernet, což umožňuje efektivní a simultánní doručení dat více přijímačům.

Struktura zpráv SV, obsahuje datové sady s digitalizovanými hodnotami měřených veličin, jako jsou proudy a napětí. Každá zpráva obsahuje také časovou značku, která udává přesný čas vzorkování, což je zásadní pro synchronizaci a správné vyhodnocení měření v reálném čase. Kromě toho zprávy SV nesou identifikátor přenášené datové sady a konfigurační revizi, která umožňuje přijímajícím zařízením správně interpretovat strukturu dat. Identifikace typu zprávy v Ethernetovém rámci je provedena pomocí pole Ethernetový typ s hodnotou **0x88ba**. Struktura celého ethernetového rámce a do něj zapouzdřené protokolu Sampled Values je zobrazena na obrázku 3.7.



Obr. 3.7: Struktura SV zprávy

- **APPID** (Application Identifier) je identifikační číslo aplikace, které určuje, že rámec patří do skupiny Sampled Values. Toto pole pomáhá zařízením v síti rozpoznat a správně zpracovat SV data.
- **Délka** Udává délku rámce SV. Toto pole je důležité pro zajištění správného zpracování rámce přijímacím zařízením.
- **Reserved1**je rezervováno pro budoucí použití nebo pro specifické implementace. Obvykle jsou nastavena na předem definovanou hodnotu a přijímací zařízení je obvykle ignoruje.
- **Reserved2** má stejnou funkci jako předchozí pole – je určeno pro budoucí rozšíření nebo specifické účely a standardní implementace jej nevyužívají.
- **savPdu** (Sampled Values Protocol Data Unit) obsahuje vlastní data Sampled Values. savPdu je struktura, která obsahuje všechny vzorkované hodnoty a související informace, jako jsou například měřené hodnoty napětí nebo proudu.
- **noASDU** (Number of ASDU) Udává počet Application Service Data Units (ASDU) v rámci rámce. ASDU jsou základní datové bloky používané v protokolu SV pro přenos měřených hodnot.
- **Security** je určeno pro bezpečnostní informace, jako jsou šifrování a autentizace. V některých implementacích může být toto pole využito pro zabezpečení datového přenosu.

ASDU 1 - ASDU n (Application Service Data Unit) je aplikační datová jednotka, kde se jednanáí o sekvenci ASDU, což jsou jednotlivé bloky dat obsahující měřené hodnoty. Každé ASDU může obsahovat data z různých měřicích bodů nebo různé typy měřených hodnot. Rozělení každého ASDU je následující:

- **svID** (Sampled Values Identifier) identifikuje konkrétní proud Sampled Values. svID je unikátní identifikátor, který umožňuje příjemcům rozpoznat a správně přiřadit příchozí data k odpovídajícímu zdroji nebo zařízení.
- **smpCnt** (Sample Count) udává pořadové číslo vzorku v rámci proudu vzorkování. Toto číslo pomáhá při synchronizaci a sekvenčním zpracování vzorků.
- **confRev** (Configuration Revision) udává verzi konfigurace datové sady. Slouží k ověření, že přijímač interpretuje přijatá data podle správné verze konfigurace.
- **refrTm** (Reference Time) udává časové razítko pro vzorky, což je důležité pro synchronizaci a časovou korelaci dat ve více systémech nebo aplikacích.
- **smpSynch** (Sample Synchronization) určuje, zda jsou vzorky synchronizovány s časovým zdrojem, jako je například GPS[18]. Toto je zásadní pro aplikace, kde je potřeba přesné časové zarovnání dat.
- **smpRate** (Sample Rate) Udává kmitočet, s jakou jsou vzorky generovány. Toto pole je důležité pro interpretaci tempa přenosu dat a pro plánování zpracování dat.
- **seqData** (Sequence of Data) obsahuje skutečná měřená data, která jsou součástí každého ASDU. Může zahrnovat různé typy měřených hodnot, jako jsou napětí, proud a další relevantní informace.

Substation Configuration Language

Substation Configuration Language (SCL) se zabývá konfigurací, správou a výměnou informací mezi zařízeními v elektrických rozvodnách. SCL je založen na XML[19] a poskytuje standardizovaný způsob popisu zařízení, datových modelů a komunikačních vztahů, což zajišťuje interoperabilitu mezi zařízeními od různých výrobců. To umožňuje snadno konfigurovat a integrovat různá zařízení a systémy. Formální definice SCL a jeho struktur je uvedena ve standardu IEC61850-6 [117] a obsahuje:

- **Hlavička**: Tato část obsahuje obecné informace o dokumentu, jako jsou metadata, verze a další atributy, které identifikují dokument a popisují jeho účel.
- **Popis Rozvodny**: V této části jsou definovány fyzické aspekty rozvodny, včetně její struktury, konfigurace a spojení mezi jednotlivými komponentami. Zde mohou být zahrnuty detaily o rozvaděčích, polích, zařízeních a jejich propojení.
- **IED Konfigurace**: V této sekci jsou specifikovány konfigurace jednotlivých Inteligentních Elektronických Zařízení (IEDs), včetně jejich funkčních schopností, datových modelů a komunikačních vztahů. Tato část obsahuje podrobné informace o každém IED, včetně jeho logických uzlů a datových prvků.
- **Datový model**: Tato část obsahuje definice datových typů a šablon, které se používají v rámci dokumentu. To může zahrnovat strukturované datové typy, logické uzly a specifické typy dat používané v IEDs.
- **Komunikační konfigurace**: Zde jsou definovány informace o síťové komunikaci, včetně mapování dat na komunikační protokoly (např. MMS, GOOSE, SV) a konfigurace síťových zařízení.
- **Další Informace**: Kromě výše uvedených hlavních částí může SCL XML dokument obsahovat další sekce pro specifické účely, jako jsou konfigurace časových značek, seznamy povolení a omezení, a další specifické informace související s konkrétní instalací rozvodny.

[18] Global Positioning System, satelitní navigační systém.

[19] eXtensible Markup Language, rozšiřitelný značkovací jazyk pro uchovávání a přenosu dat ve strukturované podobě.

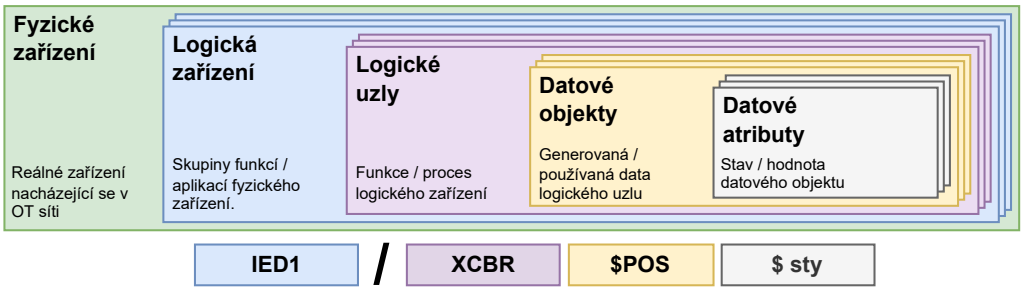
SCL obsahuje čtyři klíčových souborové formáty, které poskytují standardizovanou metodu pro popis konfigurace, schopností a vztahů mezi různými zařízeními a komponentami v elektrických rozvodnách. Formáty jsou rozděleny podle účelu, od dokumentace schopností jednotlivých IEDs, přes detailní konfigurace pro specifické nasazení, až po celkovou konfiguraci rozvodny a systémové specifikace. Popis všech čtyř formátů je uveden níže.

- **IED Capability Description** (ICD) popisuje schopnosti a možnosti konkrétní IED. Obsahuje informace o funkcích, datových modelech a komunikačních schopnostech IED a je využíván výrobci pro dokumentaci schopností jejich zařízení.
- **Configured IED Description** (CID) soubory obsahují konfiguraci specifického IED pro určité nasazení. Zahrnuje detailní konfigurační nastavení jako jsou adresy, asociace datových bodů a další specifické informace a používá se pro nahrání konfigurace do IED před jeho nasazením v terénu.
- **Substation Configuration Description** (SCD) soubory poskytují komplexní pohled na celou konfiguraci elektrické stanice, obsahují informace o všech IEDs v systému, jejich vzájemných komunikačních vztazích, síťové infrastruktuře a propojení s různými částmi systému. Jsou zásadní pro návrh a integraci rozvodné stanice jako celku.
- **System Specification Description** (SSD) soubory popisují požadavky a specifikace celého systému nebo projektu před jeho detailní konfigurací. Zahrnují obecné informace o systému, požadavky na funkčnost, bezpečnostní aspekty a využívají se během počátečních fází projektování a plánování elektrické stanice.

Datový model

Datový model IEC 61850 uvedený ve části IEC61850-7-1 [123], je je navržen tak, aby pokryl různé aspekty komunikace a funkčnosti v elektrických rozvodnách. Tento hierarchický datový model umožňuje velmi detailní a strukturovaný přístup k reprezentaci a správě všech aspektů elektrické rozvodné sítě. Díky tomu je možné efektivně řídit, monitorovat a analyzovat různé funkce a procesy probíhající v rozvodně. Struktura je rozdělena do vrstev uvedených na obrázku 3.8, z nichž každá reprezentuje jednu úroveň abstrakce a funkcionality.

- **Fyzická zařízení** (Physical Devices): reprezentuje skutečná fyzická zařízení v rozvodně, jako jsou vypínače, transformátory nebo ochranná relé. Každé zařízení má své jedinečné identifikační údaje a funkce.
- **Logická zařízení** (Logical Devices) jsou skupiny funkcí nebo aplikací, které jsou součástí fyzických zařízení. Například v rámci jednoho fyzického zařízení může být několik logických zařízení zodpovědných za různé úlohy, jako je měření, ochrana nebo řízení.
- **Logické uzly** (Logical Nodes) rozkládají funkce logických zařízení na specifičtější úrovně. Každý logický uzel odpovídá určité funkci nebo procesu, jako je například ochrana proti přetížení, měření napětí nebo kontrola výkonu.
- **Datové objekty** (Data Objects) jsou konkrétní prvky dat, které logické uzly používají nebo generují. Mohou zahrnovat různé typy dat, jako jsou měření, stavy, nastavení nebo alarmy.
- **Datové atributy** (Data Attributes) jsou specifické hodnoty nebo stavy jednotlivých datových objektů, jako jsou například hodnota napětí, stav alarmu nebo konfigurační nastavení.



Obr. 3.8: Datový model IEC 61850

Bezpečnost standardu IEC 61850

Standard IEC 61850, který je široce využíván pro komunikaci v digitálních rozvodnách a dalších částech elektroenergetické infrastruktury, se ve svém původním návrhu nezaměřuje na kybernetické zabezpečení přenášených dat ani na autentizaci komunikujících zařízení. Pro zajištění odpovídající úrovně ochrany v energetických komunikačních systémech byla proto vytvořena sada standardů IEC 62351, která definuje bezpečnostní mechanismy pro jednotlivé protokoly a vrstvy, včetně zabezpečení komunikačních služeb a datových modelů definovaných v IEC 61850.

IEC 62351-4: Bezpečnost klient/server komunikace Standard IEC 62351-4 [136] specifikuje bezpečnostní opatření pro klient/server komunikaci používanou v průmyslových a energetických systémech, zejména pro protokol MMS dle IEC 61850-8-1 a IEC 61850-8-2. Cílem je zajistit autentizaci účastníků, důvěrnost a integritu přenášených dat a minimalizovat riziko útoků typu Man-in-the-Middle, spoofing nebo manipulace s daty. Dokument definuje tři klíčové bezpečnostní profily:

- **T-profile** (Transport Security Profile) zabezpečuje fyzickou a transportní vrstvu pomocí protokolu TLS (Transport Layer Security) s podporou moderních kryptografických algoritmů a vzájemnou autentizací pomocí certifikátů X.509. Primárně se vztahuje na MMS nad TCP/IP a chrání před odposlechem a modifikací komunikace na síťové úrovni. T-profile je vhodný pro scénáře, kdy je důležitá ochrana během přenosu, ale neřeší detailně aplikační kontext.
- **A-profile** (Application Security Profile) se zaměřuje na aplikační vrstvu a provádí autentizaci během navazování spojení pomocí ACSE (Association Control Service Element). Poskytuje kontrolu identity komunikačních partnerů, ale nezajišťuje šifrování ani integritu přenášených dat. Proto se v praxi samostatně používá zřídka, typicky pouze v izolovaných a fyzicky zabezpečených sítích.
- **E2E profil** (End-to-End Security Profile) přidává ochranu přímo na úrovni aplikačních dat, zajišťuje jejich kryptografickou integritu, autenticitu a případně i důvěrnost mezi koncovými body bez ohledu na to, kolik mezi nimi existuje síťových uzlů. Lze jej použít samostatně nebo v kombinaci s T-profile pro dosažení vícevrstvého zabezpečení.

Použití A-profile bez dalších vrstev ochrany je považováno za nedostatečné, protože neposkytuje kryptografické zabezpečení přenášených dat. Nejvyšší úroveň zabezpečení se v praxi dosahuje kombinací E2E a T-profile, kdy T-profile chrání transportní kanál a E2E profil zajišťuje integritu a autenticitu samotného datového obsahu.

V rámci IEC 62351-4 jsou tzv. **aplikační profily**, které definují konkrétní implementační sadu bezpečnostních mechanismů určenou pro daný typ mapování standardu IEC 61850. Každý aplikační

profil jednoznačně specifikuje, který bezpečnostní profil (T, A, E2E) se použije, jakým způsobem se provádí autentizace a šifrování, a jaké kryptografické algoritmy a parametry jsou povoleny.

- **IEC 61850-8-1**: Definuje čtyři možnosti zabezpečení — bez zabezpečení, pouze TLS (T-profile), TLS s ACSE (kombinace T-profile a A-profile) a End-to-End. Toto pořadí odpovídá rostoucí úrovni ochrany a umožňuje volbu kompromisu mezi výkonem, složitostí implementace a požadavky na bezpečnost.
- **IEC 61850-8-2**: Zaměřuje se na komunikaci prostřednictvím webových služeb (Web Services), které inherentně nepoužívají ACSE. Proto je zde dostupné pouze End-to-End zabezpečení s možností doplnění o transportní šifrování pomocí HTTPS/TLS. Tento přístup lépe odpovídá prostředí, kde se očekává komunikace přes ne zcela důvěryhodné sítě, včetně internetu.

IEC 62351-6: Bezpečnost GOOSE a SV Tato část standardu [141] se zaměřuje na ochranu protokolů GOOSE a Sampled Values. Tyto protokoly jsou navrženy tak, aby pracovaly s minimální latencí a vysokou spolehlivostí, přičemž reakční doba systému často musí zůstat v řádu jednotek milisekund. Jakékoliv dodatečné zpracování, jako je šifrování nebo autentizace, proto může negativně ovlivnit časovou odezvu a tím i schopnost systému reagovat na poruchy. IEC 62351-6 proto definuje optimalizované bezpečnostní mechanismy, které mají poskytovat ochranu, aniž by zásadně narušily časové požadavky.

- **Replay ochrana a struktura zpráv:** GOOSE a SV komunikace ve výchozím stavu neprovádí potvrzení ani kryptografickou autentizaci. Přijímací zařízení detekuje aktuálnost zpráv pomocí časového razítka (`t`) a čísel `stNum` a `sqNum`, které indikují změnu stavu a pořadí přenosu. IEC 62351-6 doplňuje metodiku ochrany před replay útoky založenou na kontrole těchto polí a definici časového okna, ve kterém je zpráva považována za platnou. Pole **Rezervováno 1** a **Rezervováno 2** v těhto protokolech jsou vyhrazena pro budoucí bezpečnostní rozšíření, např. pro vložení kryptografických značek integrity.
- **T-profile na 2. vrstvě:** Standard připouští možnost aplikace T-profile (TLS) i na GOOSE a SV, pokud to fyzická a logická infrastruktura dovoluje. V praxi se tento přístup uplatňuje zřídka, protože TLS byl navržen pro spojovanou komunikaci na vyšších vrstvách a jeho režie může způsobit nepřijatelná zpoždění. Nasazení se proto zvažuje jen v prostředích, kde je možné garantovat dostatečnou kapacitu a velmi nízkou latenci.
- **Možnost směrování na L3:** Původní návrh GOOSE a SV využívá L2 pro rychlé doručení v rámci lokální sítě. IEC 62351-6 zavádí volitelnou možnost směrování přes síťovou vrstvu (L3) pomocí IP multicastu, což umožňuje propojení mezi geograficky vzdálenými segmenty. Tento režim je však označen jako experimentální, protože směrování může přidat proměnlivé zpoždění a vyžaduje kontrolu QoS a latence v celé přenosové cestě.
- **Role VLAN:** V reálných implementacích se nejčastěji uplatňuje segmentace a priorizace pomocí **VLAN** (IEEE 802.1Q). GOOSE a SV rámce mohou být odděleny do samostatných VLAN s nastavením priorit (IEEE 802.1p) tak, aby měly přednost před méně kritickým provozem. Tento postup snižuje riziko zahlcení sítě a minimalizuje zpoždění bez nutnosti složitých kryptografických operací.

3.3.2 Standard IEC 60870

Standard IEC 60870 představuje soubor mezinárodních protokolů a směrnic zaměřených na řešení této potřeby. Hlavním cílem tohoto standardu je definovat univerzální metody pro dálkové ovládání,

monitorování a automatické získávání dat v energetických systémech, zejména v oblasti přenosu a distribuce elektrické energie.

IEC 60870 se skládá ze šesti hlavních částí, z nichž každá pokrývá specifické aspekty systémů dálkového ovládání dat. Tento soubor standardů zahrnuje protokoly, které jsou základem pro komunikaci a výměnu dat mezi řídicími centry a zařízeními v terénu. Tyto protokoly jsou navrženy tak, aby podporovaly vysokou úroveň kompatibility a funkčnosti mezi různými hardwarovými a softwarovými systémy. Cílem je zajistit, aby zařízení od různých výrobců mohla spolehlivě a bez problémů komunikovat mezi sebou, což je zásadní pro integraci a efektivní provoz moderních energetických sítí.

Standard IEC 60870-5

Standard se zabývá protokoly pro komunikaci a je rozdělena do několika dílčích částí, které se specializují na různé aspekty a metody komunikace. Tento standard je primárně určen pro zajištění spolehlivého a bezpečného přenosu dat mezi řídicími centry a vzdálenými jednotkami, ale je možné jej využít i pro komunikaci mezi zařízeními např. elektrické stanici. Hlavní část standardu je rozdělena do sedmi částí.

IEC 60870-5-1 [99] popisuje fungování fyzické vrstvy a vrstvy datového spoje, které poskytují výběr ze čtyř typů rámců datového spoje (FT1.1, FT1.2, FT2 a FT3) s pevnou a proměnnou délkou. IEC 60870-5-2 [100] se věnuje přenosovým postupům spoje, včetně servisních primitiv a vyvážených/nevyvážených přenosových postupů, a popisuje, zda může být přenos iniciován pouze hlavní stanicí, nebo kteroukoli stanicí. IEC 60870-5-3 [101] specifikuje obecnou strukturu dat na aplikační úrovni a pravidla pro tvorbu jednotek aplikačních dat. IEC 60870-5-4 [102] poskytuje definici informačních prvků na aplikační úrovni, včetně generických prvků jako celá čísla, bitové řetězce a časové prvky. IEC 60870-5-5 [105] popisuje funkce přenosového protokolu, včetně inicializace stanice, metod získávání dat, synchronizace hodin, přenosu příkazů a souborů. IEC 60870-5-6 [115] poskytuje směrnice pro zkoušení shody pro doprovodné normy. IEC TS 60870-5-7 [129] se zaměřuje na bezpečnostní rozšíření protokolů IEC 60870-5-101 a IEC 60870-5-104 s použitím IEC 62351 pro zajištění bezpečnosti komunikace.

V rámci standardu IEC 60870-5 existují několik důležitých protokolů, každý zaměřený na specifickou oblast aplikace v energetických systémech. IEC 60870-5-101 [104] je základním standardem pro sériovou komunikaci, poskytující spolehlivý přenos dat mezi řídicími stanicemi a vzdálenými jednotkami. IEC 60870-5-102 [108] se zaměřuje na přenos integrovaných součtových hodnot v elektrizační soustavě, což je klíčové pro efektivní sběr a analýzu dat o spotřebě a distribuci elektrické energie. IEC 60870-5-103 [109] se soustředí na komunikaci s ochrannými zařízeními v energetických sítích, umožňující rychlý a spolehlivý přenos informací o stavu a poruchách. IEC 60870-5-104 [114] rozšiřuje možnosti IEC 60870-5-101 pro použití v sítích TCP/IP, což umožňuje komunikaci přes internet nebo jiné IP sítě.

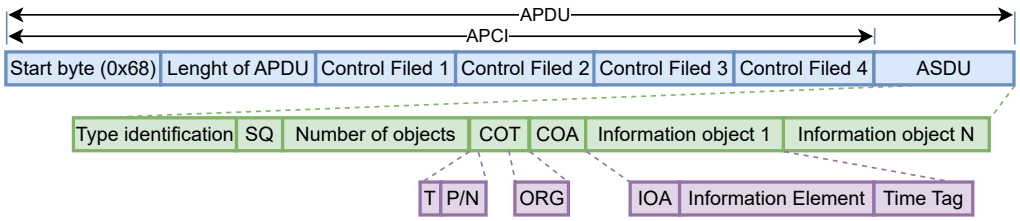
Kromě těchto hlavních protokolů IEC 60870-5 zahrnuje také rozšířeni v podobě IEC 60870-5-601 [133], který se zabývá zkušebními případy pro zkoušení shody zařízení a systémů pro dálkové ovládání a SCADA systémy. Dále také rozšíření IEC 60870-5-604 [134], který poskytuje standardní metodu testování implementací IEC 60870-5-104.

Standard IEC 60870-5-104

IEC 60870-5-104 (zkráceně IEC 104) je komunikační protokol pro dálkové řízení a monitorování v elektroenergetice, definovaný jako součást standardů IEC 60870-5. Jedná se o rozšíření staršího protokolu IEC 6087-5-101, který byl vytvořen pro komunikaci po sériové lince. IEC 104 rozšiřuje

tento protokol na možnost přenosu přes model ISO/OSI. Přenos dat proto probíhá přes transportní protokol TCP (standardně na portu 2404) a protokol IP. Komunikační model IEC 104 je postaven na architektuře klient–server. V běžném použití plní řídicí centrum (např. SCADA) roli klienta a iniciuje spojení, zatímco vzdálené terminálové zařízení (např. RTU) funguje jako server.

Z hlediska struktury zprávy je každý rámec v IEC 104 tvořen jednotkou APDU (Application Protocol Data Unit), která se skládá ze dvou částí APCI (Application Protocol Control Information) a ASDU (Application Service Data Unit). APCI je řídící hlavička a ASDU datová část, která nese přenášené infromace. Struktura celého rámce je uvedena na obrázku 3.9.



Obr. 3.9: Struktura paketu IEC 104

- **Start Byte (0x68)** je pevně daný úvodní bajt, který označuje začátek IEC104 zprávy. Všechny IEC104 rámce začínají hexadecimální hodnotou – 0x68, která příjemci signalizuje, že následuje řídicí blok (APCI) dle specifikace tohoto protokolu.
- **Length of APDU** určuje délku následující části rámce v bajtech, tedy celkovou délku řídicí a datové části rámce (APCI + ASDU).
- **Control Field 1–4 (APCI)** tvoří aplikační řídicí informace protokolu. Obsahují informace o typu rámce (I, S, U rámec) a pořadová čísla pro potvrzování přenášených zpráv.
  - **Control Field 1 a 2** obsahují pořadové číslo odesílané zprávy (Send Sequence Number, N(S)), které je důležité pro řízení toku a detekci chyb.
  - **Control Field 3 a 4** obsahují očekávané potvrzovací číslo zprávy od protistrany (Receive Sequence Number, N(R)), čímž se potvrzuje přijetí předchozích zpráv.
- **Type Identification** je pole v ASDU, které určuje typ přenášené datové jednotky – např. jednopólový binární signál, analogová hodnota, příkaz atd. Jedná se o 1 bajt, jehož hodnota definuje strukturu následujícího datového pole.
- **Sequence of Elements (SQ)** je 1-bitový příznak v poli následujícím po Type ID. Udává, zda je seznam objektů v ASDU strukturován jako jednotlivé položky (SQ=0) s vlastní adresou, nebo jako posloupnost hodnot od jedné společné adresy (SQ=1).
- **Number of Objects** je 7-bitové pole ve stejném bajtu jako SQ. Udává, kolik informačních objektů (např. měření, stavů nebo příkazů) se v datové jednotce nachází.
- **Cause of Transmission (COT)** je dvoubajtové pole, které definuje důvod přenosu zprávy. Například: 3 = spontánní zpráva, 5 = požadavek na celkový stav (General Interrogation), 6 = odpověď na GI, 20 = aktivace příkazu. Pole také obsahuje několik bitových příznaků:
  - **T** (Test) – označuje, že se jedná o testovací zprávu (např. pro kontrolu komunikace),
  - **P/N** (Positive/Negative confirm) – rozlišuje mezi pozitivním a negativním potvrzením,
  - **ORG** – signalizuje, zda byl přenos vyvolán systémem nebo externí entitou (např. jinou stanicí).
- **Common Address (COA)** je dvoubajtové pole, které identifikuje zařízení (např. RTU, podstanici), ze kterého zpráva pochází, resp. kterému je určena. Slouží k adresaci v rámci jedné sítě.

- **Information Object** je základní datová jednotka. Každý objekt obsahuje:
  - **Information Object Address (IOA)** má velikost 3 bajty a jednoznačně identifikuje konkrétní měřicí bod nebo ovládané zařízení (např. binární vstup, analogový kanál, výstupní relé).
  - **Information Element** obsahují vlastní data daného typu – např. binární hodnota (zapnuto/vypnuto), analogová hodnota (plovoucí řádová čárka), nastavovaná hodnota apod. Struktura tohoto pole závisí na hodnotě Type ID.
  - **Time Tag** je volitelná součást informačního objektu. Je reprezentována strukturou o velikosti 7 bajtů a obsahuje přesný čas události: milisekundy, minuty, hodiny, den, měsíc a rok.

Komunikace v IEC 104 je realizována prostřednictvím tří specifických typů rámců, které se liší podle svého účelu a struktury řídicí části (APCI). Každý typ rámce je určen pro jinou fázi nebo typ přenosu a využívá jiný formát řídicích bajtů:

- **I-rámec (Information Transfer Frame)** je určen pro přenos dat (ASDU) a obsahuje pořadové číslo odesílané zprávy (N(S)) a potvrzovací číslo přijaté zprávy (N(R)).
- **S-rámec (Supervisory Frame)** slouží pouze pro potvrzení přijatých zpráv bez odesílání nových dat. Obsahuje pouze potvrzovací číslo (N(R)).
- **U-rámec (Unnumbered Frame)** je nesekvenční řídicí rámec používaný pro řízení spojení. Obsahuje řídicí příkazy jako STARTDT, STOPDT a TESTFR.

IEC 104 umožňuje přenos různých typů zpráv v závislosti na typu události, provozním režimu a požadavcích na sběr nebo řízení dat. Jednotlivé typy komunikace odpovídají běžným scénářům v prostředí SCADA–RTU:

- **Spontánní zprávy** jsou odesílány RTU automaticky při změně hodnoty nebo stavu (např. při změně binárního vstupu).
- **Periodické reporty** poskytují pravidelné zasílání stavových a měřených hodnot v konfigurovaných časových intervalech.
- **Dotazy typu General Interrogation (GI)** iniciuje SCADA stanice pro získání kompletního aktuálního stavu RTU.
- **Příkazy** slouží k aktivnímu řízení zařízení z dispečerského systému, např. spínání výstupů nebo zadávání analogových hodnot.
- **Synchronizace času** umožňuje aktualizaci systémového času v RTU zasláním přesně časovaného rámce s časovým razítkem.

Bezpečnost standardu IEC 60870-5

Sama o sobě norma IEC 62351-5 [148] k implementaci zabezpečení IEC 104 nestačí, protože se jedná o normu, která specifikuje zprávy, postupy a algoritmy pro zabezpečení provozu všech protokolů založených na IEC 60870-5 nebo z ní odvozených. Cílem IEC 62351-5 je zajistit, aby data přenášená mezi zařízeními v rámci těchto protokolů byla autentizovaná a integrovaná, čímž se zabrání možnosti jejich manipulace nebo padělání. Norma popisuje všechna rozšíření TLS[20], která musí být podporována s cílem vyměňovat potřebné dodatečné informace během procesu handshake, potřebu podpory více certifikačních autorit, minimální velikost certifikátu, sady šifer, podporované a zastaralé kryptografické algoritmy včetně podpisových algoritmů a podporované mechanismy změny klíče.

Na základě IEC 62351-5 byla IEC 60870-5 rozšířena o část IEC 60870-5-7, kde řeší převod implementace IEC 62351-5 pro protokoly IEC 60870-5-101/102/103/104. Specificky je účelem tohoto

[20]Použití TLS, jeho verzí, kryptografických algoritmů a dalších řeší IEC 62351-3 [147].

standardu umožnit příjemci komunikace IEC 60870-5 ověřit, že data byla přenesena oprávněným uživatelem a že nebyla při přenosu modifikována. Poskytuje metody pro ověření nejen zařízení, ale také samotných uživatelů, pokud je tato možnost podporována v systému SCADA.

Dle standardu IEC 62351-5 je obecná zpráva mapovaná na konkrétní zprávu **S_KR_NA_l**, která bude odeslána protokolem IEC-60870-104. Původní zpráva 62351-5, která má v tomto případě pouze jedno pole, je opatřena záhlavím specifickým pro protokol IEC 60870-104. Výchozí metoda ověřování je tzv. Agresivní režim (Aggresive mode) pro stanice implementující tuto normu. Inicializační proces, v němž se vyměňují údaje o výzvě, se provádí pomocí kombinace standardních zpráv IEC-60870-104 a nových zpráv dle IEC 60870-5-7.

Standard IEC 60870-6

Standard IEC 60870-6, známý také pod názvem TASE (Telecontrol Application Service Element), je klíčový pro výměnu dat a informací mezi různými energetickými systémy a má zásadní význam pro koordinaci a optimalizaci provozu v nadnárodních energetických systémech. IEC 60870-6 pokrývá široký rozsah aspektů, od základních protokolů a definic služeb až po specifické uživatelské konvence a pokročilé funkční profily.

V současné době se standard skládá ze dvanácti části. IEC 60870-6-1 [152] stanovuje aplikační kontext a požadavky pro dálkové ovládání, uvádí strukturu funkcí, charakteristiky existujících protokolů a definuje funkční profily. IEC 60870-6-2 [153] se věnuje použití základních norem OSI vrstev 1-3 pro efektivní mezipodnikovou komunikaci. IEC 60870-6-501 [106] (Definice služby) definuje služby pro výměnu provozních dat v systémech dálkového ovládání, zdůrazňující jednoduchost a udržovatelnost. IEC 60870-6-502 [107] (Definice protokolů) specifikuje protokoly pro efektivní výměnu provozních dat mezi systémy dálkového ovládání. IEC 60870-6-503 [130] (Služby a protokoly) popisuje metody výměny časově kritických dat řídicího centra s podporou pro různé architektury. IEC 60870-6-504 (Uživatelské konvence) je technická zpráva definující pravidla pro použití rozhraní TASE.1. IEC TR 60870-6-505 [112] (Uživatelská příručka) poskytuje návod pro hodnocení, pořizování a konfiguraci TASE.2. IEC 60870-6-601 [103] se zaměřuje na funkční profil pro přenosové služby v koncových systémech s trvalým přístupem k datové síti, což je důležité pro Smart Grid. IEC 60870-6-602 [111] popisuje přenosové profily pro WAN, klíčové pro distribuované aplikace SCADA/EMS. IEC 60870-6-701 [110] definuje funkční profil pro poskytování aplikační služby TASE.1 mezi dvěma koncovými systémy řídicích center. IEC 60870-6-702 [131] specifikuje funkční profil pro poskytování aplikační služby TASE.2, zahrnující prezentační a relační služby mezi koncovými systémy. Nakonec, IEC 60870-6-802 [132] se zaměřuje na objektové modely TASE.2, specifikující metody výměny dat pro podporu různých architektur a aktualizací od předchozího vydání.

3.4 Model komunikačních vrstev v elektroenergetice

Komunikační infrastruktura v elektroenergetice je vícevstvá a založená na rozhraních mezi jednotlivými technologickými úrovněmi. Podkapitola se zaměřuje na rozbor komunikační architektury od nejnižší procesní vrstvy až po integrační a řídicí vrstvy na základě standardů IEC 61850 a IEC 60870-5-104. Tato architektura je zobrazena na obrázku 3.10 a je specifikována v několika částech normy:

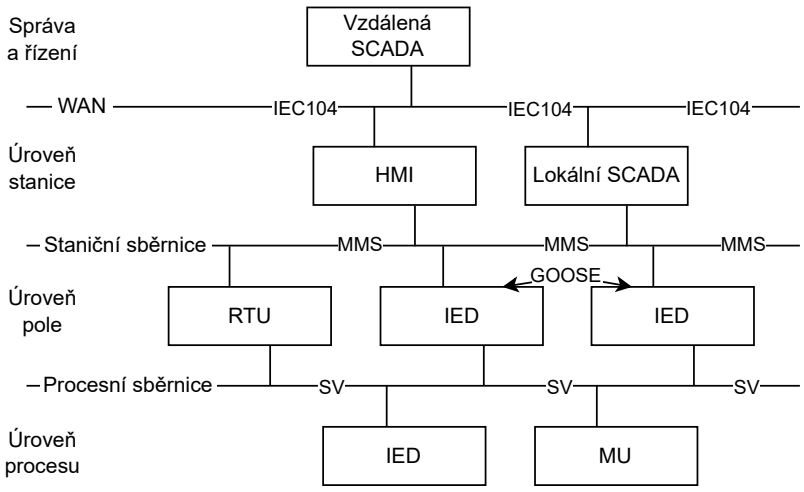
- **IEC 61850-1** definuje základní přehled a koncepční rámec standardu, včetně vysvětlení architektury rozvodny, kde rozlišuje staniční a procesní úroveň komunikace a jejich vzájemné vazby,

- **IEC 61850-7-1** stanovuje abstraktní komunikační modely, které slouží jako základ pro výměnu informací mezi zařízeními jako jsou IED, Merging Units a SCADA/HMI systémy,
- **IEC 61850-8-1** specifikuje mapování abstraktních služeb na protokol MMS a obsahuje detaily k použití GOOSE v rámci staniční sběrnice, včetně formátu zpráv a pravidel výměny,
- **IEC 61850-9-2** popisuje mechanismus přenosu vzorkovaných měřených hodnot přes procesní sběrnici pomocí Sampled Values, typicky mezi měřicími transformátory (např. Merging Units) a IED zařízeními,
- **IEC 60870-5-104** definovaný mimo rámec IEC 61850, je standardem využívaným pro dálkový přenos dat z rozvodny na vyšší úroveň řízení (SCADA/dispečink), a slouží tak jako integrační rozhraní mezi staničním systémem a nadřazenými systémy.

Architekt rozvodny definuje tzv. Procesní a Staniční sběrnici, zahrnující komunikaci mezi měřicími a ochrannými zařízeními (IED, MU) a staničními systémy HMI/SCADA pomocí protokolů GOOSE, MMS a SV. Na vyšších úrovních pak dochází transformaci na protokol IEC 60870-5-104, který zajišťuje datovou výměnu mezi staničním řídicím systémem a nadřazenými SCADA nebo dispečerskými centry.

Standard IEC 61850 představuje komplexní rámec pro automatizaci elektrických stanic, který zahrnuje jak datový model, tak komunikační protokoly a systémovou architekturu. Jednou z jeho klíčových vlastností je vrstvená struktura komunikace, která odráží reálnou strukturu datové komunikace v rozvodnách a trafostanicích. Komunikace se zde neodehrává pouze na jedné úrovni, jak je zobrazeno na obrázku 3.10, ale probíhá mezi různými subsystémy od nejnižší procesní vrstvy (měření) až po staniční vrstvu (lokální řízení) a dále k dispečerským systémům prostřednictvím nadřazených protokolů (např. IEC 60870-5-104). V rámci této hierarchie IEC 61850 rozlišuje dvě základní komunikační sběrnice:

- **Procesní sběrnice**: zajišťuje komunikaci mezi zařízeními na úrovni procesu, typicky mezi Slučovací jednotky a Inteligentní elektronická zařízení. Z protokolů se využívá hlavně SV a GOOSE a to pro ochranné a měřicí účely.
- **Staniční sběrnice**: zajišťuje komunikaci mezi IED, staničním HMI, SCADA a dalšími zařízeními vyšší úrovně. Zde je využíván hlavně protokoly GOOSE a MMS.



Obr. 3.10: Model elektrické rozvodny dle IEC 61850

3.4.1 Procesní sběrnice

Procesní sběrnice tvoří nejnižší komunikační vrstvu v rámci architektury elektrických stanic podle standardu IEC 61850. Jejím hlavním účelem je zajistit rychlou a spolehlivou výměnu dat mezi zařízeními. Tato vrstva je klíčová zejména pro ochranné a měřicí funkce, které vyžadují přenos informací s minimální latencí a maximální spolehlivostí.

Přenosové protokoly

Komunikace na procesní sběrnici se řídí specifikacemi definovanými v rámci IEC 61850-8-1 (pro GOOSE) a IEC 61850-9-2 (pro SV). Přenos obou služeb je realizován dle modelu ISO/OSI na druhé (spojové) vrstvě [154], kde jsou zprávy zapouzdřeny do ethernetových rámců, bez využití vyšších protokolových vrstev. Toto řešení umožňuje dosažení velmi rychlého přenosu a zpracování dat.

GOOSE zprávy GOOSE zprávy jsou určeny pro rychlé a spolehlivé šíření stavových informací mezi IED v rozvodnách, typicky pro přenos ochranných a řídicích signálů, jako jsou například TRIP, BLOCK nebo CLOSE.

- **Komunikační režim:** Multicastový přenos založený na modelu vydavatel-odběratel (publisher-subscriber). GOOSE zprávy jsou vysílány periodicky. Při změně hodnoty (například trip signálu) se zpráva odešle opakovaně s exponenciálně rostoucím intervalem, po dosažení časového okna přechází do režimu pravidelného vysílání beze změny.
- **Zajištění doručení:** Žádná zpětná vazba, žádné potvrzení; spolehlivost je zajištěna opakováním. Odběratel spoléhá na změnu čísla sekvence (sqNum).
- **Latence:** Standard IEC 61850 definuje tři typy časových požadavků:
  - Type 1A (velmi rychlý přenos) – typicky pro ochrany, požadavek < 3 ms,
  - Type 1B (rychlý přenos) – například pro interlocking, požadavek < 10 ms,
  - Type 2 – řízení, požadavek < 100 ms.
- **Synchronizace:** GOOSE zprávy striktně nevyžadují časovou synchronizaci, ale obsahují číslo změny stavu (stNum), číslo sekvence (sqNum) a časové razítko (t).
- **Typické použití:** Stavové signály v ochranách (TRIP, BLOCK, INTERLOCK), binární vstupy, stav IED, aktivace logických funkcí.

SV zprávy SV zprávy jsou určeny pro přenos vzorkovaných měřených hodnot (proudů, napětí, fázorů) ze slučovacích jednotek směrem k ochranným a měřicím IED.

- **Komunikační režim:** Přenos je, stejně jako u GOOSE, založen na modelu vydavatel-odběratel. Vysílání probíhá v pevných časových intervalech, přenos je kontinuální bez ohledu na změnu měřených veličin.
- **Zajištění doručení:** Žádné potvrzení; ztráta rámce je tolerována (např. interpolací), ale častější výpadky vedou k chybnému chování ochran.
- **Latence:** Typická latence ve stanici je v jednotkách milisekund. Nejde o absolutně nejnižší latenci, ale o zachování její stability. Podle kmitočetu (50 Hz) sledovaného vedení standard stanovuje požadovaný počet vzorků na cyklus:
  - při 80 vzorcích/cyklus $\rightarrow$ cca 4000 rámců/s,
  - při 256 vzorcích/cyklus $\rightarrow$ cca 12 800 rámců/s.
- **Synchronizace:** Přesné časové razítkování hodnot obvykle pomocí protokolu IEEE 1588v2 (PTP) nebo IRIG-B. Zprávy obsahují časové razítko, identifikaci kanálu, vzorkovací číslo

a synchronizační příznaky. Pokud není časová synchronizace mezi odesílatelem a příjemcem zajištěna, může docházet k zahazování paketů.
- **Typické použití:** Přenos digitálních měření ze slučovacích jednotek do ochranných a měřicích IED. Slouží jako vstup do ochranných algoritmů (např. distanční ochrana, diferenciální ochrana).

Princip a logické vazby

Procesní sběrnice plní v rámci rozvodny roli výkonné komunikační vrstvy, která propojuje zařízení určená pro měření, ochranu a řízení s cílem umožnit rychlou výměnu informací bez závislosti na klasickém kabelovém propojení. Na této sběrnici probíhá jak přenos vstupních dat (měřených veličin), tak aktivace výstupních funkcí (například vypnutí vývodu při poruše).

Základní logické vazby jsou následující:
- **MU → IED (datový tok SV):** Merging Unit sbírá analogové signály (proudy, napětí) z transformátorů a převádí je na digitální datový tok Sampled Values. Tyto zprávy jsou periodicky vysílány a poskytují přesné měření v reálném čase pro více IED současně.
- **IED → IED (datový tok GOOSE):** Každé IED může generovat ochrannou nebo stavovou informaci ve formě GOOSE zprávy (například signalizaci detekované poruchy). Tato zpráva je přenášena multicastem, což znamená, že ji může přijímat více dalších IED bez nutnosti přímého spojení. Například: IED 1 detekuje poruchu → vyšle GOOSE trip signál → IED 2 aktivuje vypínací výstup.
- **MU → více IED paralelně:** Díky multicastovému přenosu může být jeden stream SV využit více IED současně. To umožňuje redundanci v ochranách (například hlavní a záložní ochrana pracují s totožnými daty).
- **Synchronizace:** Přestože GOOSE zprávy striktně nevyžadují časovou synchronizaci, SV zprávy ano. Všechny IED musí být časově sladěny s MU, aby mohly zpracovávat měřené hodnoty přesně ve stejném okamžiku. Například pro výpočet diferenciální ochrany je nezbytné, aby oba konce vedení vzorkovaly synchronně.

3.4.2 Staniční sběrnice

Staniční sběrnice představuje střední komunikační vrstvu v rámci architektury elektrických stanic dle standardu IEC 61850. Slouží k výměně informací mezi IED, přístupem k řídicímu a vizualizačnímu systému (HMI, SCADA) a umožňuje také přenos diagnostických dat, konfigurací a příkazů mezi stanicí a dispečinkem. Na rozdíl od procesní sběrnice, která zajišťuje vysokorychlostní přenosy v rámci ochran a měření, je staniční sběrnice orientována spíše na řízení, signalizaci a přístup člověka do systému (rozhraní člověk–stroj, operátorské funkce a alarmů).

Přenosové protokoly

Staniční sběrnice využívá protokoly vyšších vrstev ISO/OSI modelu, zpravidla běžící nad TCP/IP. Klíčovým standardem je MMS, který je součástí IEC 61850-8-1. Pro externí komunikaci je běžně využíván protokol IEC 60870-5-104, případně TASE.2. V určitých případech se na staniční sběrnici uplatňuje i GOOSE, zejména pro výměnu logických signálů.

MMS (Manufacturing Message Specification) Výhodou MMS je, že všechny přenášené proměnné jsou objektově modelovány a pojmenovány, což usnadňuje interoperabilitu napříč dodavateli a umožňuje automatické mapování SCADA bodů.

- **Komunikační model:** Strukturovaná komunikace typu klient–server. Každé IED implementuje serverovou část, která zpřístupňuje své datové objekty, služby a funkce dle datového modelu IEC 61850.
- **Klientské zařízení:** HMI panel, SCADA systém, gateway nebo inženýrské stanice.
- **Funkce:** Čtení a zápis proměnných, přenos změn hodnot, alarmy, sekvence událostí, řízení výstupů, přenos záznamů.
- **Vlastnosti:** Komunikační model je asynchronní s podporou spontánních hlášení změn.

IEC 60870-5-104 Protokol 104 se běžně nasazuje v gateway zařízení, které mapuje interní datový model (např. MMS) do jednodušších struktur podle 104 a přeposílá je dál do SCADA.

- **Využití:** Komunikace stanice s nadřazeným dispečinkem (SCADA).
- **Komunikační model:** Klient–server komunikace nad TCP/IP.
- **Funkce:** Přenos měření, stavů, binárních a analogových hodnot, alarmů a příkazů.
- **Vlastnosti:** Neposkytuje objektový model jako IEC 61850, ale jednotlivé proměnné jsou identifikovány pomocí ASDU adres.

Princip a logické vazby

Staniční sběrnice tvoří komunikační páteř pro logiku řízení a dohled nad staniční infrastrukturou. Na rozdíl od procesní sběrnice, která je vysoce deterministická a časově přísně řízená, slouží staniční sběrnice k distribuci informací mezi vyššími funkcemi řízení, operátory a dispečinkem. Její funkcionalita je klíčová pro vizualizaci stavu zařízení, správu a konfiguraci jednotlivých IED, přenos ovládacích příkazů, potvrzení a koordinaci ochranných a řídicích funkcí mezi poli.

Základní logické vazby na staniční sběrnici jsou následující:

- **IED ↔ HMI/SCADA (MMS):** Operátor prostřednictvím HMI nebo SCADA vidí stav všech IED, může ovládat vypínače, analyzovat události a číst alarmy. Například: IED 1 indikuje přetížení → odešle hlášení přes MMS → HMI zobrazí alarm a trend proudu.
- **IED ↔ Gateway ↔ SCADA dispečink (IEC 60870-5-104):** Gateway slouží jako překladač, vezme data z interní MMS komunikace a převede je do IEC 104 formátu pro odeslání na dispečink. Například: SCADA vyšle příkaz „vypnout vývod“ → příkaz projde přes 104 → gateway → MMS zápis do IED.
- **HMI/PC ↔ IED (MMS):** Inženýr připojený k síti má přístup ke konfiguraci, záznamům a stavům IED. Může například načíst záznam poruchy, provést diagnostiku nebo aktualizovat firmware bez fyzického zásahu.
- **IED ↔ IED (MMS nebo GOOSE):** Mezi jednotlivými poli může docházet k přímé výměně signálů. Například Pole 1 blokuje možnost připojení Pole 2 při určitém stavu. Signál „zablokuj vypnutí“ může být šířen jako GOOSE nebo zapisován přes MMS.
- **Události a alarmové toky:** Staniční sběrnice je nositelem událostní logiky – hlášení změn stavů, historických sekvencí, alarmů, poruchových záznamů. Tato data slouží k pozdější analýze provozu nebo incidentů.

3.5 Analýza bezpečnosti datových toků v elektroenergetice

Komunikační infrastruktura elektroenergetické soustavy je komplexní systém, ve kterém probíhá interakce mezi řídicími centry, rozvodnami a koncovými zařízeními. Každý z těchto prvků je potenciálním cílem kybernetického útoku, a proto je nutné analyzovat nejen to, jak komunikace technicky probíhá, ale i kde vstupují jednotlivé subjekty a kde se nacházejí zranitelná rozhraní.

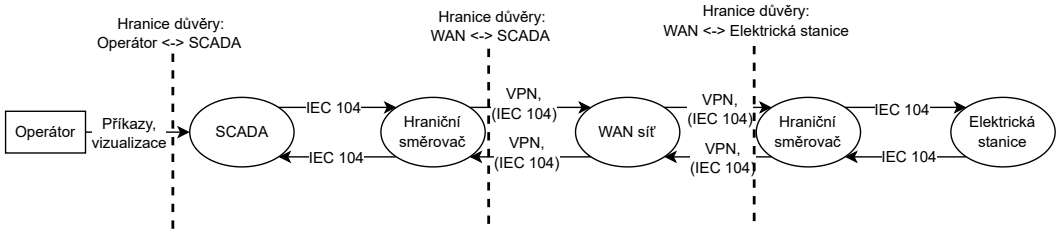
Z těchto důvodů bude pro účely bezpečnostní analýzy využit model Data Flow Diagramu (DFD) dle metodiky NIST SP800-154 [178]. DFD slouží k datově orientovanému modelování hrozeb a identifikaci tzv. hranic důvěry (trust boundaries), tedy bodů, kde dochází ke změně úrovně bezpečnosti a je třeba zajistit zvláštní ochranu, například autentizaci, šifrování či řízení přístupů. Na základě toho byla vytvořena dvojice modelů, které nejsou vytvářeny mechanicky podle síťové nebo systémové architektury, ale vycházejí z bezpečnostního pohledu na možné způsoby ohrožení systému. Každý z modelů reflektuje specifický scénář:

- **Model 1** se zabývá útoky, které přicházejí z vnější sítě (např. internet),
- **Model 2** se zabývá lokálními útoky, kdy má útočník přímý síťový přístup do stanice.

3.5.1 Model 1 – Vzdálené hrozby

První model, který je zobrazen na obrázku 3.11, popisuje komunikaci mezi operátorem, řídicím SCADA systémem a elektrickou stanicí dle IEC 60870-5-104 a struktury uvedené v článku [2]. Předpokládá se, že útočník nemá fyzický přístup k infrastruktuře, ale může komunikovat přes veřejnou nebo sdílenou síť (například internet nebo poskytovatele WAN připojení).

Model vychází z architektury běžné dispečerské komunikace, kde je SCADA systém propojen s rozvodnou prostřednictvím VPN tunelu, který zajišťuje šifrování a autentizaci komunikace (například v protokolu IEC 60870-5-104). Vstupní bod útočníka je tedy na úrovni WAN sítě nebo v rámci přístupu operátora do SCADA systému.



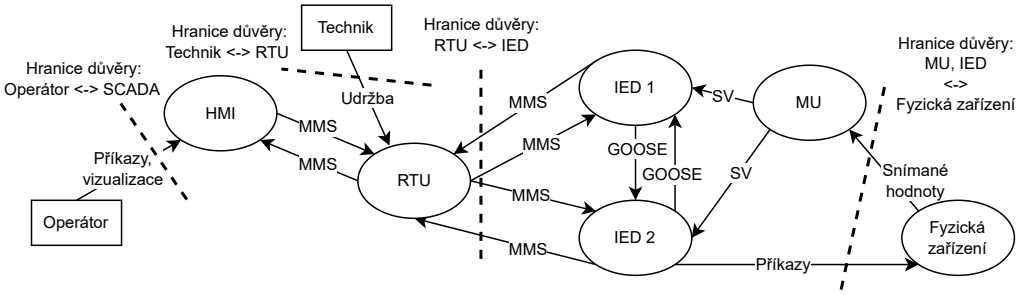
Obr. 3.11: DFD model pro vzdálené hrozby

Zásadním prvkem modelu je rozpoznání a explicitní vyznačení tří klíčových hranic důvěry:

- **Operátor ↔ SCADA systém:** Tato hranice odděluje člověka (operátora) od plně automatizovaného řídicího systému. I když se nachází ve stejném fyzickém nebo síťovém prostoru, je tato hranice klíčová. Přístup operátora je zprostředkován skrze HMI nebo SCADA rozhraní, a právě zde může docházet k lidské chybě, neoprávněnému zásahu nebo zneužití přihlašovacích údajů.
- **SCADA systém ↔ WAN síť:** Zde dochází ke změně úrovně bezpečnosti z vnitřního dispečerského systému, který je pod kontrolou provozovatele do WAN infrastruktury. Komunikace mezi dispečinkem a rozvodnou je nejčastěji zajištěna pomocí přes VPN.
- **WAN síť ↔ Elektrická stanice:** Analogická k předchozí – představuje druhý konec VPN tunelu. Brání tomu, aby se do staniční infrastruktury dostal neautorizovaný provoz, ať už přímo nebo v rámci útoku typu Man-in-the-Middle (MITM).

3.5.2 Model 2 – Lokální hrozby

Druhý model, který je zobrazen na obrázku 3.12, je zaměřen na vnitřní strukturu rozvodny dle IEC 61850-8-1, 9-2 a struktury uvedené v článku [13], kde hrozby vznikají v situaci, kdy má útočník fyzický nebo přímý síťový přístup k zařízení. Tento přístup může být důsledkem slabého fyzického zabezpečení (například neuzamčený rozvaděč), kompromitovaného zařízení připojeného do interní sítě, nebo selhání v řízení přístupu.



Obr. 3.12: DFD model pro lokální hrozby

Model identifikuje čtyři klíčové hranice důvěry:

- **Operátor ↔ HMI:** Podobně jako u modelu 1 jde o rozhraní mezi člověkem a systémem. I když je přístup omezen na lokální HMI panel, stále je zde riziko lidské chyby nebo zneužití účtu. Operátor může ovlivnit chování ochranné logiky, spustit nebo zrušit příkaz, zobrazit záznamy nebo provést zásah, aniž by to bylo autorizováno.
- **Technik ↔ RTU/IED (Technický přístup):** Technik s konfiguračním přístupem má možnost změnit nastavení ochrany, upravit logiku, nahrát nový firmware nebo importovat chybný konfigurační soubor. Pokud je tento přístup zneužit nebo kompromitován, může dojít k zásadnímu narušení funkce ochranného systému.
- **RTU ↔ Ochranná zařízení (IED):** Přestože se zařízení často nacházejí v jedné fyzické lokalitě, z hlediska sítě a funkcí se jedná o samostatné entity. IED realizují rychlé ochranné funkce nezávisle na RTU, která plní spíše koordinující a monitorovací roli. Tato hranice chrání ochranné systémy před zahlcením, špatným nastavením nebo neautorizovaným zásahem z řídicí vrstvy.
- **MU/IED ↔ Fyzická zařízení:** Jde o přechod z digitálního prostředí do reálného světa. Vstupní hodnoty (proudy, napětí) a výstupní příkazy (TRIP, CLOSE) vstupují nebo vystupují z fyzického zařízení. Tato hranice je často podceňována, ale její narušení může znamenat manipulaci s měřením (například simulovaný proud) nebo znemožnění ochranné akce (například výpadek spínacího signálu).

3.6 Modely teorie front pro analýzu přenosu zpráv v elektroenergetice

Při kvantitativním hodnocení přenosu zpráv v komunikační infrastruktuře energetických systémů je vhodné využít teorie front [163], která umožňuje popsat chování systému z hlediska vytížení, doby zpracování požadavků a pravděpodobnosti vzniku zpoždění nebo ztrát. Pro účely této práce jsou uvažovány základní stacionární modely teorie front, které jsou dostatečné pro analytický popis zátěžových stavů v síťových prvcích a serverových zařízeních.

3.6.1 Přehled používaných modelů

V této práci se využívají standardní modely označované Kendallovou notací[21]. Modely pokrývají běžné scénáře přenosu zpráv v protokolech jako GOOSE, SV, MMS nebo IEC 104, a to jak v deterministickém, tak v náhodném režimu generování zpráv.

- **M/M/1**: náhodné příchody požadavků, náhodná doba obsluhy, jeden obslužný kanál,
- **M/D/1**: náhodné příchody požadavků, deterministická doba obsluhy, jeden obslužný kanál,
- **D/D/1**: deterministické příchody i doba obsluhy, jeden obslužný kanál.

3.6.2 Definice základních parametrů modelů

Pro všechny uvažované modely se používají následující parametry:

- λ [1/s] – intenzita příchodů požadavků do systému,
- μ [1/s] – kapacita obsluhy systému,
- ρ – vytížení systému, definované jako:

$$\rho = \frac{\lambda}{\mu} \quad [-], \tag{3.1}$$

- L [-] – průměrný počet požadavků v systému (fronta + obsluha),
- L_q [-] – průměrný počet požadavků ve frontě,
- W [s] – průměrná doba, kterou požadavek stráví v systému,
- W_q [s] – průměrná doba čekání požadavku ve frontě.

3.6.3 Základní vztahy pro model M/M/1

Model M/M/1 je jedním z nejjednodušších a nejčastěji používaných modelů teorie front. Předpokládá, že příchody požadavků do systému se řídí Poissonovým procesem[22] s intenzitou λ a doba obsluhy má exponenciální rozdělení s parametrem μ. K dispozici je jeden obslužný kanál a systém je analyzován ve stacionárním režimu ($\rho < 1$). Základní analytické vztahy jsou následující:

- Průměrný počet požadavků v systému (ve frontě i obsluze), což udává průměrný počet požadavků, které se nacházejí v systému v daném okamžiku:

$$L = \frac{\rho}{1-\rho} \quad [-], \tag{3.2}$$

- Průměrný počet požadavků ve frontě, což udává, kolik požadavků průměrně čeká na obsluhu:

$$L_q = \frac{\rho^2}{1-\rho} \quad [-], \tag{3.3}$$

- Průměrná doba, kterou požadavek stráví v systému, což udává celkovou dobu, kterou požadavek v systému stráví – tedy dobu čekání i dobu obsluhy:

$$W = \frac{1}{\mu - \lambda} \quad [\text{s}], \tag{3.4}$$

- Průměrná doba čekání ve frontě, což udává dobu, kterou požadavek průměrně stráví čekáním ve frontě před začátkem obsluhy:

$$W_q = \frac{\rho}{\mu - \lambda} \quad [\text{s}], \tag{3.5}$$

[21] Kendallova notace zapisuje modely teorie front ve tvaru $A/S/c$, kde A je typ příchodů, S typ obsluhy a c počet serverů; M značí Markovský (exponenciální) proces, D deterministickou dobu a G obecné rozdělení. Např. $M/M/1$ značí exponenciální příchody i obsluhu a jeden server.

[22] Poissonův proces je náhodný proces popisující počet událostí nastávajících v čase s konstantní průměrnou intenzitou λ a s nezávislými intervaly mezi událostmi, které mají exponenciální rozdělení.

3.6.4 Základní vztahy pro model M/D/1

Model M/D/1 předpokládá, že požadavky přicházejí náhodně (podle Poissonova procesu s intenzitou λ), avšak doba obsluhy každého požadavku je deterministická (konstantní) a rovná $1/\mu$. Tento model lépe vystihuje systémy, kde je obsluha pravidelná a přesně časově definovaná, například některé přenosy GOOSE nebo SV zpráv. Pro přibližné výpočty lze využít Kingmanovu aproximaci délky fronty:

$$L_q \approx \frac{\rho^2(1+C_s^2)}{2(1-\rho)} \quad [-], \tag{3.6}$$

kde C_s^2 je variační koeficient doby obsluhy. V případě deterministické obsluhy platí $C_s^2 = 0$, čímž se vztah zjednoduší:

$$L_q \approx \frac{\rho^2}{2(1-\rho)} \quad [-]. \tag{3.7}$$

Ostatní vztahy (například $W = L/\lambda$ nebo $W_q = L_q/\lambda$) zůstávají shodné s modelem M/M/1, a lze je využít pro výpočet doby v systému a čekací doby.

3.6.5 Základní vztahy pro model D/D/1

Model D/D/1 představuje plně deterministický systém, ve kterém požadavky přicházejí v pravidelných časových intervalech a doba jejich obsluhy je rovněž konstantní. Jedná se o ideální scénář provozu, který nastává například u synchronizovaných přenosů, typicky u předem načasovaných Sampled Values zpráv. Za předpokladu, že intenzita příchodů nepřekračuje kapacitu systému ($\rho < 1$), platí následující vztahy:

$$L_q = 0 \quad [-], \tag{3.8}$$

$$L = 1 \quad [-], \tag{3.9}$$

$$W = \frac{1}{\mu} \quad [\mathrm{s}], \tag{3.10}$$

$$W_q = 0 \quad [\mathrm{s}], \tag{3.11}$$

kde:

- L_q udává, že nevzniká žádná fronta, jelikož každý požadavek je obsloužen přesně při svém příchodu,
- $L = 1$ znamená, že v systému se v daný okamžik nachází vždy právě jeden požadavek a to ten, který je aktuálně obsluhován,
- W odpovídá deterministické době obsluhy,
- $W_q = 0$ znamená nulovou čekací dobu.

Pokud však $\rho \geq 1$, systém se dostává do přetížení, požadavky se začnou kumulovat a deterministický charakter přenosu je narušen. Model D/D/1 tak slouží zejména jako referenční případ ideálního provozu bez zpoždění v reálně synchronizovaných systémech.

3.7 Analytický model GOOSE zpráv s využitím teorie front

GOOSE zprávy umožňující rychlý a spolehlivý přenos binárních stavových informací mezi zařízeními. Z hlediska návrhu, simulace je vhodné definovat způsob jejich generování a současně kvantitativně modelovat dopady tohoto přenosu na síťovou infrastrukturu, konkrétně na přepínače a další síťové prvky.

3.7.1 Model generování GOOSE zpráv

Způsob generování GOOSE zpráv odpovídá specifikaci definované v normě IEC 61850-8-1 a je navržen tak, aby bylo možné rychle a spolehlivě přenášet binární stavové informace mezi zařízeními elektrické stanice. Generování zpráv probíhá ve dvou základních režimech, které odrážejí aktuální stav sledovaného systému:

- **Klidový režim (periodické vysílání)** Pokud nedochází ke změně sledovaného stavu, IED zařízení generuje GOOSE zprávy v pravidelných časových intervalech. Tyto periodické zprávy slouží k obnově informací v síti a zajišťují, že i při absenci událostí zůstává příjemce informován o aktuálním stavu. Generování je deterministické s konstantní periodou T_p [s], což odpovídá příchodům zpráv s intenzitou:

$$\lambda_p = \frac{1}{T_p} \quad [1/\text{s}]. \tag{3.12}$$

  Hodnota T_p je konfigurovatelná a její velikost závisí na konkrétní aplikaci, obvykle se pohybuje v rozmezí od jednotek sekund po desítky sekund.

- **Událostní režim (burst vysílání po změně stavu)** Pokud dojde k detekci změny sledovaného stavu, například změny polohy spínacího prvku, přechází IED zařízení do tzv. burstového režimu vysílání. V tomto režimu jsou zprávy generovány v rychlém sledu s postupně rostoucími intervaly mezi jednotlivými zprávami. Tento mechanismus zajišťuje, že informace o změně stavu se co nejrychleji rozšíří v síti a zároveň je dostatečně redundantní, aby byla zajištěna její spolehlivá distribuce. Pro první fázi burstového režimu lze intenzitu příchodů zpráv aproximovat jako:

$$\lambda_e = \frac{1}{T_{\min}} \quad [1/\text{s}], \tag{3.13}$$

  kde $T_{\min}$ [s] je minimální interval mezi prvními zprávami po změně stavu, typicky v řádu milisekund (například 5 ms). Následně se intervaly mezi zprávami postupně zvětšují dle geometrické řady, dokud není dosaženo maximálního intervalu, po kterém se zařízení vrací zpět do klidového režimu.

Tento mechanismus generování zpráv lze z hlediska matematického modelování popsat jako dvoustavový stochastický proces, kde stav systému určuje aktuální režim generování zpráv. Přechody mezi klidovým a událostním režimem je možné formalizovat pomocí Markovského modelu, konkrétně dvoustavového Markov Modulated Poisson Process (MMPP). Tento přístup umožňuje realisticky popsat proměnlivou intenzitu příchodů GOOSE zpráv v závislosti na aktuálním dění v síti a lépe predikovat chování systému zejména při simulaci zátěžových nebo krizových stavů.

3.7.2 Aplikace teorie front na GOOSE komunikaci

Pro kvantitativní popis chování přenosu GOOSE zpráv z hlediska zátěže sítě, latence a pravděpodobnosti přetížení lze využít standardní modely teorie front uvedené v kapitole 3.6. Výběr konkrétního modelu závisí na režimu generování zpráv a požadované úrovni přesnosti:

- **M/D/1 model** Použitelný pro popis klidového režimu, kdy jsou GOOSE zprávy generovány v pravidelných intervalech T_p [s]. Příchody požadavků jsou deterministické s intenzitou:

$$\lambda_p = \frac{1}{T_p} \quad [1/\text{s}], \tag{3.14}$$

- **M/M/1 model** Aproximuje situace burstového režimu po změně stavu, kdy dochází k rychlému a náhodnému generování zpráv. Příchody požadavků lze aproximovat Poissonovým procesem s intenzitou:

$$\lambda_e = \frac{1}{T_{\min}} \quad [1/\text{s}]. \tag{3.15}$$

  V reálném provozu však zprávy nepřicházejí čistě náhodně ani čistě deterministicky, ale jejich intenzita se dynamicky mění podle aktuálního dění v síti. Tento přechod mezi klidovým a událostním režimem lze vhodně popsat pomocí dvoustavového Markovského modelu s modulovanou intenzitou příchodů (MMPP).
- **Dvoustavový MMPP model** reflektuje skutečnost, že intenzita generování zpráv závisí na stavu systému. Systém přechází mezi dvěma stavy:
  - **Klidový stav**: periodické zprávy s nízkou intenzitou příchodů λ_p [1/s],
  - **Událostní stav**: burstové zprávy s vysokou intenzitou příchodů λ_e [1/s].

  Přechody mezi stavy jsou popsány Markovským procesem se dvěma stavy, kde:
  - Stav S_1 odpovídá klidovému režimu s intenzitou příchodů λ_p [1/s],
  - Stav S_2 odpovídá událostnímu režimu s intenzitou příchodů λ_e [1/s].

  Přechody mezi stavy jsou určeny přechodovými pravděpodobnostmi v diskrétním čase, vyjádřenými maticí:

$$P = \begin{bmatrix} 1 - p_{pe} & p_{pe} \\ p_{ep} & 1 - p_{ep} \end{bmatrix}, \tag{3.16}$$

  kde:
  - p_{pe} [-] je pravděpodobnost přechodu z klidového do událostního stavu,
  - p_{ep} [-] je pravděpodobnost návratu z událostního do klidového stavu.

  Tento model zachycuje proměnlivou intenzitu příchodů zpráv v závislosti na stavu systému a umožňuje lépe predikovat chování přenosové infrastruktury, včetně situací, kdy vlivem událostí či kybernetických útoků dochází k dočasnému přetížení systému.

3.7.3 Vliv redundantních topologií (PRP, HSR)

V praxi se pro zvýšení spolehlivosti přenosu GOOSE zpráv běžně využívají redundantní topologie dle normy IEC 62439-3, konkrétně:

- **PRP (Parallel Redundancy Protocol)** – zprávy jsou odesílány paralelně dvěma nezávislými cestami. Z hlediska modelování lze situaci aproximovat jako dvě nezávislé fronty se stejnými parametry λ [1/s] a μ [1/s], přičemž čas doručení zprávy je dán minimem z časů obou cest:

$$T_{\text{doručení}} = \min(T_1, T_2) \quad [\text{s}]. \tag{3.17}$$

- **HSR (High-availability Seamless Redundancy)** – zprávy obíhají v kruhové topologii. Výslednou latenci lze aproximovat jako součet časů přenosu přes jednotlivé uzly:

$$T_{\text{doručení}} = N \cdot T_{\text{uzel}} \quad [\text{s}], \tag{3.18}$$

  kde N je počet uzlů a T_{uzel} [s] je čas průchodu jedním uzlem.

3.7.4 Modelování kybernetických útoků na GOOSE komunikaci

V kontextu kybernetické bezpečnosti je nutné zohlednit vliv nelegitimního provozu, zejména útoků typu DoS, které uměle navyšují intenzitu příchodů GOOSE zpráv. Rozšířený model intenzity příchodů je pak definován jako:

$$\lambda_{\text{total}} = \lambda_p + \lambda_e + \lambda_a \quad [1/\text{s}], \tag{3.19}$$

kde:

- λ_p [1/s] je intenzita periodických zpráv,
- λ_e [1/s] je intenzita burst zpráv po změně stavu,
- λ_a [1/s] je intenzita nelegitimních zpráv generovaných útokem.

Při zvýšení λ_{total} nad kapacitu obsluhy μ [1/s] dochází k nárůstu latence, hromadění zpráv ve frontách a potenciálnímu narušení deterministického chování systému.

3.8 Analytický model SV zpráv s využitím teorie front

Sampled Values zprávy dle standardu IEC 61850-9-2 představují mechanismus pro přenos digitalizovaných měřených hodnot, zejména proudů a napětí, mezi slučovacími jednotkami a ochrannými či řídicími zařízeními v rámci automatizovaných systémů elektrických stanic. Přenos SV zpráv je realizován na úrovni L2 multicastu s vysokou frekvencí a přísnými časovými požadavky, což klade výrazné nároky na kvalitu a kapacitu komunikační infrastruktury.

3.8.1 Model generování SV zpráv

SV zprávy jsou generovány kontinuálně v pravidelných časových intervalech, přičemž každý rámec obsahuje vzorkované hodnoty aktuálního stavu sledovaných veličin. Počet generovaných rámců za sekundu je dán vzorkovací frekvencí:

$$f_s = N \cdot f_{\text{mains}} \quad [\text{Hz}], \tag{3.20}$$

kde:

- f_s je výsledná frekvence vzorkování [Hz],
- N je počet vzorků na periodu síťového kmitočtu [-],
- f_{mains} je síťová frekvence [Hz], typicky 50 nebo 60 Hz.

Každý rámec je odesílán s konstantní periodou:

$$T_{SV} = \frac{1}{f_s} \quad [\text{s}]. \tag{3.21}$$

3.8.2 Aplikace teorie front na SV komunikaci

Příchody požadavků do systému jsou pravidelné s intenzitou:

$$\lambda_{SV} = \frac{1}{T_{SV}} = f_s \quad [1/\text{s}], \tag{3.22}$$

kde:

- λ_{SV} je intenzita příchodů SV rámců do systému [1/s],
- T_{SV} je perioda generování rámců [s],
- f_s je vzorkovací frekvence [Hz].

Kapacita obsluhy výstupního portu přepínače je definována jako:

$$\mu = \frac{C_{\text{port}}}{S_{\text{frame}}} \quad [1/\text{s}], \tag{3.23}$$

kde:

- C_{port} je propustnost portu [b/s],
- S_{frame} je velikost jednoho SV rámce [bit].

Vytížení systému:

$$\rho = \frac{\lambda_{SV}}{\mu} \quad [-]. \tag{3.24}$$

3.8.3 Modelování kybernetických útoků na SV komunikaci

Celkovou intenzitu příchodů do systému lze popsat jako:

$$\lambda_{\text{total}} = \lambda_{SV} + \lambda_{\text{background}} + \lambda_a \quad [1/\text{s}], \tag{3.25}$$

kde:

- $\lambda_{\text{background}}$ je intenzita ostatního běžného provozu [1/s],
- λ_a je intenzita nelegitimního provozu generovaného útokem [1/s].

3.8.4 Vliv redundantních topologií (PRP, HSR)

- **PRP**: čas doručení rámce odpovídá minimu ze dvou nezávislých cest:

$$T_{\text{doručení}} = \min(T_1, T_2) \quad [\text{s}]. \tag{3.26}$$

- **HSR**: rámce obíhají kruhovou topologií, celková latence je součtem latencí uzlů:

$$T_{\text{doručení}} = N \cdot T_{\text{uzel}} \quad [\text{s}], \tag{3.27}$$

  kde N je počet uzlů [-] a T_{uzel} [s] je doba zpracování rámce na jednom uzlu.

3.9 Analytický model MMS zpráv s využitím teorie front

Protokol MMS (Manufacturing Message Specification) dle normy IEC 61850-8-1 představuje standardizované komunikační rozhraní pro výměnu dat mezi zařízeními v rámci automatizovaných systémů elektrických stanic. Umožňuje přenos stavových informací, měřených dat, alarmových zpráv, ovládacích příkazů i zpráv souvisejících s konfigurací a řízením zařízení.

Komunikace MMS je realizována v architektuře klient-server, typicky mezi:

- **Klienty**: SCADA systémy, HMI, inženýrské stanice,
- **Servery**: IED zařízení, řídicí jednotky, RTU.

Přenosy zpráv lze rozdělit do několika kategorií (viz níže) dle způsobu iniciace a charakteru provozu, přičemž každý typ představuje odlišnou zátěž na komunikační infrastrukturu a vyžaduje specifický přístup z hlediska teorie front.

3.9.1 Periodické reporty

V klidovém režimu dochází k automatickému zasílání stavových informací a měřených hodnot ze serveru k nadřazeným systémům v pravidelných časových intervalech T_p. Příchody zpráv jsou deterministické s intenzitou:

$$\lambda_p = \frac{1}{T_p} \quad [1/\mathrm{s}]. \tag{3.28}$$

3.9.2 Událostní přenosy

Při detekci změny sledovaného stavu generuje server okamžité zprávy, jejichž četnost závisí na aktuálním dění v síti. Tyto přenosy lze modelovat jako Poissonovský proces s intenzitou:

$$\lambda_e \quad [1/\mathrm{s}]. \tag{3.29}$$

Vhodným modelem je **M/M/1**, který umožňuje analyzovat dobu odezvy, vznik front a potenciální přetížení při zvýšeném výskytu událostí.

3.9.3 Ovládací příkazy

Iniciace ovládacích příkazů je nepravidelná a závisí na operátorovi či automatizační logice. Příchody těchto zpráv lze aproximovat jako Poissonovský proces s intenzitou:

$$\lambda_c \quad [1/\mathrm{s}]. \tag{3.30}$$

Pro jejich modelování lze využít **M/M/1** model, případně rozšířený model s prioritní frontou, pokud je v infrastruktuře implementována preferenční obsluha těchto zpráv.

3.9.4 Dotazy na hodnoty

Dotazy na konkrétní hodnoty, generované ze strany klienta, jsou iniciovány nepravidelně podle aktuálních požadavků. Intenzitu těchto příchodů označujeme jako:

$$\lambda_r \quad [1/\mathrm{s}], \tag{3.31}$$

kde jejich chování lze aproximovat modelem **M/M/1**.

3.9.5 Managementové zprávy a udržování spojení

Managementové zprávy zajišťují navázání, udržování a ukončování komunikace mezi klientem a serverem. Intenzitu těchto zpráv označujeme jako:

$$\lambda_m \quad [1/\mathrm{s}]. \tag{3.32}$$

Za běžného provozu je jejich objem zanedbatelný, nicméně při nestabilitě sítě či útocích může jejich počet výrazně vzrůst. Pokud je potřeba jejich dopad zohlednit, lze využít **M/M/1** model.

3.9.6 Modelování zátěžových stavů a kybernetických útoků

V reálném provozu může být komunikace MMS negativně ovlivněna zátěžovými situacemi a kybernetickými útoky, které vedou ke zvýšení objemu přenášených zpráv a přetížení infrastruktury. Typickými scénáři jsou:

- Generování falešných událostí zvyšujících intenzitu událostních přenosů,
- Zneužití ovládacích příkazů k zahlcení systému,
- Automatizované generování dotazů na hodnoty (skriptované útoky),
- Útoky na navazování a udržování spojení, vedoucí k nárůstu managementových zpráv.

Tyto jevy lze kvantitativně modelovat zavedením dodatečné intenzity:

$$\lambda_a \quad [1/\mathrm{s}], \tag{3.33}$$

která reprezentuje nelegitimní provoz generovaný útokem.

3.9.7 Agregovaný model přenosu zpráv v rámci protokolu MMS

Celkovou intenzitu příchodů zpráv protokolu MMS do klíčových prvků infrastruktury lze popsat součtem intenzit jednotlivých typů přenosů:

$$\lambda_{\text{MMS-total}} = \lambda_p + \lambda_e + \lambda_c + \lambda_r + \lambda_m + \lambda_a \quad [1/\mathrm{s}], \tag{3.34}$$

kde:

- λ_p [1/s] je intenzita příchodů periodických reportů,
- λ_e [1/s] je intenzita událostních přenosů,
- λ_c [1/s] je intenzita ovládacích příkazů,
- λ_r [1/s] je intenzita dotazů na hodnoty,
- λ_m [1/s] je intenzita managementových zpráv,
- λ_a [1/s] je intenzita nelegitimního provozu generovaného kybernetickým útokem.

Za předpokladu, že jednotlivé příchody lze aproximovat jako vzájemně nezávislé Poissonovské procesy, je výsledná intenzita rovněž Poissonovská a systém lze zjednodušeně modelovat jako agregovaný **M/M/1** model s intenzitou $\lambda_{\text{MMS-total}}$ a kapacitou obsluhy μ odpovídající výkonu konkrétního zařízení nebo síťového prvku. Tento přístup umožňuje:

- Kvantitativně predikovat chování systému při kombinaci různých typů MMS přenosů,
- Odhadnout hraniční zatížení, při kterém dochází k nárůstu latence a ztrátě zpráv,
- Zohlednit dopady zvýšeného provozu, například při poruchách, testech nebo útocích,
- Návrh a ověření mitigací v experimentálním prostředí.

3.10 Analytický model IEC 104 zpráv s využitím teorie front

Protokol IEC 104 představuje jeden z klíčových standardů pro dálkovou komunikaci mezi dispečerskými centry a vzdálenými zařízeními energetické infrastruktury, jako jsou rozvodny, transformační stanice, RTU nebo IED. Tento protokol využívá k přenosu dat protokolovou sadu TCP/IP, což zajišťuje spolehlivý přenos dat, ovšem zároveň je systém podřízen omezením a zpožděním spojeným s IP sítí.

Z hlediska návrhu a provozu komunikační infrastruktury je důležité nejen kvalitativně popsat jednotlivé typy přenosu zpráv, ale také kvantitativně analyzovat jejich dopad na zátěž serverů,

gateway zařízení a přístupových bodů. K tomuto účelu lze využít teorii front, která umožňuje formálně modelovat příchody požadavků, dobu jejich zpracování a chování systému při různém stupni zatížení.

Přenos zpráv v IEC 104 lze rozdělit do několika základních kategorií podle způsobu iniciace a charakteru přenosu. Každý typ přenosu klade na systém jiné požadavky a vyžaduje specifický přístup k jeho matematickému modelování.

3.10.1 Spontánní přenosy

Spontánní přenosy představují zprávy, které vzdálená zařízení (RTU nebo IED) automaticky generují a odesílají dispečerskému systému v okamžiku, kdy dojde ke změně sledovaného stavu. Tento typ přenosu slouží k zajištění okamžité informovanosti o událostech v elektrizační soustavě bez ohledu na nastavení periodických přenosů nebo dotazů ze strany SCADA systému.

Typickými příklady spontánních přenosů jsou:

- Změna polohy spínacích prvků (vypínače, odpojovače),
- Aktivace ochran a bezpečnostních prvků,
- Překročení limitních hodnot napětí, proudu nebo výkonu,
- Výskyt alarmových nebo poruchových stavů,
- Změna vstupů či výstupů zařízení sítě.

Četnost těchto přenosů je nepravidelná a závisí na aktuálním dění v síti. V klidovém stavu může být počet spontánních zpráv minimální, naopak při poruchách či spínacích operacích se jejich počet výrazně zvyšuje. Intenzita těchto příchodů je označena jako λ_s a lze jejich dopad modelovat pomocí **M/M/1** modelu:

$$\lambda_s = \frac{N_s}{T_s} \quad [1/\text{s}], \tag{3.35}$$

kde:

- N_s [-] je počet spontánních přenosů v čase T_s,
- T_s [s] je interval sledování spontánních událostí,
- λ_s [1/s] ke intenzita spontánních přenosů.

3.10.2 Periodický reporting

Periodický reporting představuje mechanismus, kdy vzdálená zařízení (např. RTU nebo IED) automaticky odesílají stavové informace a měřené hodnoty dispečerskému systému v pravidelných, předem definovaných časových intervalech T_p [s]. Tento přenos je nezávislý na aktuálním dění v síti a slouží k udržení aktuálního přehledu o stavu elektrizační soustavy. Intenzita příchodů periodických zpráv je dána vztahem:

$$\lambda_p = \frac{1}{T_p} \quad [1/\text{s}]. \tag{3.36}$$

3.10.3 General interrogation a selektivní dotazy

Protokol IEC 104 umožňuje také aktivní vyžádání dat ze strany dispečerského systému v případě potřeby. Rozlišujeme:

- **General interrogation (obecný dotaz)**: kompletní vyžádání všech aktuálních stavových informací a měřených hodnot od konkrétního zařízení, typicky - po navázání spojení, při restartu zařízení, na žádost operátora při podezření na chybu nebo nesrovnalosti v datech.

- **Selektivní dotazy**: požadavek na konkrétní hodnotu nebo informaci z vybraného zařízení, např. stav konkrétního vypínače, aktuální hodnotu proudu v určitém vedení, stav určitého binárního vstupu.

Četnost těchto požadavků je nepravidelná a závisí na potřebách systému nebo operátora. Intenzita jejich příchodů je označena jako λ_g. Modelování lze provést pomocí **M/M/1** modelu.

$$\lambda_g = \frac{N_g}{T_g} \quad [1/\text{s}], \tag{3.37}$$

kde:

- N_g [-] je počet požadavků v intervalu T_g,
- T_g [s] je časový interval sledování,
- λ_g [1/s] je intenzita general nebo selektivních dotazů.

3.10.4 Potvrzovací zprávy a řízení spojení

Součástí protokolu IEC 104 je také výměna zpráv souvisejících s řízením spojení a potvrzováním přenosu. Tyto zprávy zajišťují správnou funkčnost komunikačního kanálu mezi SCADA systémem a vzdálenými zařízeními. Patří sem například - potvrzení o přijetí datových zpráv (ACK), potvrzení o přijetí ovládacích příkazů, testovací rámce ověřující dostupnost linky, zprávy související se zahájením a ukončením spojení. Objem těchto zpráv je za běžného provozu obvykle malý, nicméně při výpadcích, nestabilitě nebo cílených útocích může výrazně vzrůst.

Intenzita těchto zpráv je označena jako λ_m. Pokud je jejich objem významný, lze jejich dopad modelovat pomocí **M/M/1** modelu:

$$\lambda_m = \frac{N_m}{T_m} \quad [1/\text{s}], \tag{3.38}$$

kde:

- N_m [-] je počet managementových zpráv v intervalu T_m,
- T_m [s] je časový interval sledování,
- λ_m [1/s] je intenzita managementových zpráv.

3.10.5 Zohlednění zátěžových stavů a kybernetických scénářů

Provoz protokolu IEC 104 může být výrazně ovlivněn kombinací běžného provozu, zátěžových stavů a kybernetických útoků. Mezi nejčastější scénáře patří:

- Generování falešných událostí, které navyšují intenzitu spontánních přenosů,
- Zneužití general interrogation požadavků k zahlcení infrastruktury (DoS útoky),
- Manipulace s řízením spojení, vedoucí k nadměrnému počtu managementových zpráv,
- Kombinované útoky narušující dostupnost a stabilitu komunikace.

Intenzitu takto generovaného nelegitimního provozu lze označit jako λ_a a lze jejich dopad modelovat pomocí **M/M/1** modelu:

$$\lambda_a = \frac{N_a}{T_a} \quad [1/\text{s}], \tag{3.39}$$

kde:

- N_a [-] je počet nelegitimních zpráv (útokem) v čase T_a,
- T_a [s] je doba trvání pozorovaného útoku,
- λ_a [1/s] je intenzita nelegitimního provozu].

3.10.6 Agregovaný model přenosu zpráv v rámci protokolu IEC 104

Celkovou intenzitu příchodů zpráv protokolu IEC 104 do klíčových síťových prvků lze vyjádřit jako:

$$\lambda_{\text{IEC104-total}} = \lambda_s + \lambda_p + \lambda_g + \lambda_m + \lambda_a \quad [1/\text{s}], \tag{3.40}$$

kde:

- λ_s [1/s] je intenzita spontánních přenosů,
- λ_p [1/s] je intenzita periodického reportingu,
- λ_g [1/s] je intenzita dotazů (general interrogation, selektivní dotazy),
- λ_m [1/s] je intenzita managementových zpráv,
- λ_a [1/s] je intenzita nelegitimního provozu (útoky).

Při předpokladu nezávislosti jednotlivých typů přenosů lze systém zjednodušeně modelovat jako agregovaný **M/M/1** model s výslednou intenzitou $\lambda_{\text{IEC104-total}}$ a kapacitou obsluhy μ. Tento přístup umožňuje:

- Kvantitativní predikci chování systému při kombinaci různých typů přenosů,
- Odhad mezních stavů přetížení a ztrátovosti,
- Zohlednění dopadů kybernetických útoků a zátěžových scénářů,
- Návrh a ověření mitigací v experimentálním prostředí.

4 Bezpečnostní rámec a analýza zranitelností v elektroenergetické

Zajištění kybernetické bezpečnosti představuje v prostředí energetických sítí klíčovou výzvu. Tato kapitola shrnuje základní standardy, které definují požadavky na zabezpečení průmyslových řídicích systémů, a popisuje historické incidenty, které ovlivnily přístup k ochraně těchto systémů. Následně kapitola přechází k vlastní analýze kybernetických hrozeb s využitím strukturovaných metodik, jako jsou STRIDE a MITRE ATT&CK.

4.1 Standardy kybernetické bezpečnosti v energetice

V oblasti energetických sítí hrají standardy kybernetické bezpečnosti zásadní roli při zajištění spolehlivosti a odolnosti průmyslových řídicích systémů [16]. Poskytují jednotný rámec pro návrh, implementaci a ověřování bezpečnostních opatření, která reagují na specifická rizika spojená s provozem kritické infrastruktury. Tyto standardy definují požadavky na ochranu komunikačních kanálů, řízení přístupu, integritu a důvěrnost dat, stejně jako na prevenci a detekci kybernetických hrozeb. V následujících podkapitolách jsou popsány klíčové normy a doporučení, které se v praxi uplatňují při zabezpečení energetických systémů, včetně mezinárodně uznávaných rámců jako IEC 62443, IEC 62351, NIST SP 800-82, IEEE 1686 a doporučení agentury ENISA.

4.1.1 Standard IEC 62443

IEC 62443 [118] je standard zaměřený na kybernetickou bezpečnost průmyslových řídících systémů, včetně energetických infrastruktur. Standard se zaměřuje na širokou škálu kybernetických hrozeb, od neautorizovaného přístupu až po sabotáž. Zahrnuje také fyzické útoky na zařízení a zranitelnosti v komunikačních protokolech. Tato norma zdůrazňuje zranitelnosti v operačních technologiích, jako jsou SCADA systémy, a hrozby spojené s připojenými zařízeními v průmyslových sítích.

IEC 62443 se zaměřuje na širokou škálu kybernetických hrozeb, které mohou ohrozit bezpečnost průmyslových řídicích a automatizačních systémů. Hlavní hrozby uvedené ve standardu zahrnují:

- **Neautorizovaný přístup a zneužití systému**: Standard [128, 151, 150] explicitně uvádí, že neautorizovaný přístup k průmyslovým systémům může vést k manipulaci s operacemi, měřenými daty nebo konfiguracemi. Tato hrozba může zahrnovat vnější i vnitřní útoky, kdy útočníci získají neoprávněný přístup k zařízení nebo komunikačním kanálům.
- **Sabotáže a manipulace s daty**: IEC 62443 [128, 143] zdůrazňuje hrozbu sabotáže, kdy útočníci mohou manipulovat s daty nebo kontrolními příkazy, což může ovlivnit bezpečnost a stabilitu celého systému. Tento typ útoku může zahrnovat podvržení příkazů nebo změny v měřených hodnotách, které jsou použity pro rozhodování v reálném čase.
- **Zranitelnosti v komunikačních protokolech**: V rámci standardu [137, 138] je uvedeno, že zranitelnosti v komunikačních protokolech představují riziko, ale konkrétní protokoly jako IEC 61850 nebo IEC 60870 nejsou specifikovány v detailu. Nicméně standard doporučuje bezpečnostní opatření, která ochrání komunikaci mezi zařízeními.
  - **Šifrování**: Pro ochranu přenášených dat je doporučeno v [128, 138] šifrování komunikačních kanálů, aby se zajistila důvěrnost a integrita dat během přenosu.
  - **Autentizace a kontrola přístupu**: Doporučuje se autentizace a kontrola přístupu pro zařízení i uživatele, aby se zajistilo, že pouze autorizovaní účastníci mohou komunikovat a provádět operace v systému [128, 138].

  - **Integrita dat**: Je doporučeno v [128, 138] použití metod na ochranu integrity dat, jako jsou digitální podpisy a kontrolní součty, aby se zajistilo, že data nebyla během přenosu manipulována.
- **Útoky na zařízení (IED)**: IEC 62443 [138, 128] zmiňuje rizika spojená s inteligentními elektronickými zařízeními, která mohou být napadena nebo zneužita k šíření útoků po síti. Standard se zaměřuje na ochranu zařízení proti neautorizovanému přístupu a zajištění jejich integrity.

IEC 62443 obsahuje konkrétní mitigace zaměřené na ochranu systémů a zařízení před kybernetickými hrozbami. Mezi klíčová opatření uvedená ve standardu patří:

- **Segmentace sítí**: Standard [128] doporučuje segmentaci sítí na různé bezpečnostní zóny, které umožňují oddělení kritických a méně citlivých částí infrastruktury. Tento přístup pomáhá zamezit šíření útoků mezi různými částmi systému.
- **Autentizace a řízení přístupu**: Pro ochranu systémů doporučuje [128, 151] autentizaci pro všechna zařízení a uživatele, kteří mají přístup k citlivým informacím nebo řízení zařízení. To zahrnuje implementaci vícefaktorové autentizace a digitálních certifikátů.
- **Šifrování**: Pro ochranu dat se doporučuje [138] použití šifrování všech přenosů mezi zařízeními, aby se zajistila důvěrnost a integrita komunikace.
- **Monitorování a detekce anomálií**: Doporučuje se [128] nasazení monitorovacích nástrojů, které detekují anomálie v síti a mohou identifikovat potenciální kybernetické útoky nebo narušení bezpečnosti.
- **Fyzická bezpečnost**: Standard [151] zdůrazňuje důležitost fyzické ochrany zařízení a přístupových bodů k citlivým systémům, aby se zabránilo neautorizovanému fyzickému přístupu a manipulaci.
- **Zálohování a obnova po havárii**: Pro případ kybernetického útoku nebo jiné havárie doporučuje [151] zavedení pravidelných záloh a plánů pro obnovu po havárii, které zajistí kontinuitu provozu.

4.1.2 Standard IEC 62351

IEC 62351 [116] je standard zaměřený na ochranu kybernetické bezpečnosti v oblasti energetických sítí, zvláště na kontrolní a automatizační systémy. Hlavním cílem tohoto standardu je zajistit bezpečnost přenosu dat a komunikace mezi zařízeními, aby se zabránilo nežádoucí manipulaci nebo útokům. Standard se zaměřuje na specifikování bezpečnostních opatření pro komunikační protokoly, které se v energetických systémech používají. IEC 62351 se zaměřuje na zajištění bezpečnosti několika komunikačních protokolů, které se používají v přenosových a distribučních soustavách. Nezahrnuje však podrobné instrukce k implementaci každého protokolu nebo nepopisuje konkrétní metodiky pro některé velmi specifické hrozby, jako jsou například DDoS útoky nebo malware. Zmiňuje však ochranu proti neautorizovanému přístupu, manipulaci s daty a integritě komunikace. Specifikace bezpečnostních opatření pro následující protokoly jsou:

- **IEC 61850** (MMS, GOOSE, SV): IEC 62351 zahrnuje specifikace pro bezpečnostní prvky jako je autentizace zařízení [149], šifrování komunikace [136, 141], a integrita dat [141].
- **IEC 60870**: standard doporučuje opatření, jako je šifrování [147] a autentizace [148, 149], aby se zajistila bezpečnost při přenosu dat mezi SCADA systémy a zařízeními.

IEC 62351 definuje několik konkrétních opatření, jak chránit přenos dat a komunikaci proti kybernetickým hrozbám. Mezi hlavními mitigacemi, které standard popisuje, najdeme:

- **Šifrování a integrita dat** [147, 136, 141]: Šifrování je klíčovým bezpečnostním opatřením pro ochranu důvěrnosti a integrity přenášených dat. Standard doporučuje použití TLS a dal-

ších šifrovacích protokolů pro zabezpečení komunikace mezi zařízeními a SCADA systémy. Pro zajištění integrity přenášených dat jsou doporučeny technologie jako digitální podpisy a kontrolní součty, které umožňují ověřit, že data nebyla během přenosu změněna.

- **Autentizace a kontrola přístupu** [142, 149]: IEC 62351 požaduje, aby byla implementována autentizace jak pro zařízení, tak pro uživatele, kteří mají přístup k citlivým informacím nebo řízení zařízení. To zahrnuje použití digitálních certifikátů a šifrovaných klíčů pro zabezpečení autentizace mezi zařízeními. Standard doporučuje použití kontrolních mechanismů přístupu k zařízením a síťovým prostředkům, aby byl přístup omezen pouze na autorizované uživatele a zařízení. To zahrnuje správu uživatelských práv a implementaci zásad pro řízení přístupu na základě rolí (RBAC)[1].
- **Monitoring a detekce** [135]: Standard doporučuje implementaci systémů pro monitorování komunikace a detekci anomálií v reálném čase. To pomáhá včas identifikovat potenciální útoky, jako jsou MITM nebo podvržení příkazů.

Standard IEC 62351 explicitně řeší kybernetické hrozby v souvislosti s přenosem a řízením dat v energetických systémech. Norma popisuje následující klíčové typy kybernetických útoků:

- **Replay útoky** [141]: Opakované přehrání zachycené zprávy (např. GOOSE nebo SV) umožňuje útočníkovi znovu spustit dříve vydaný příkaz. Proti tomu IEC 62351–6 popisuje ochranu pomocí sekvenčních čísel (stNum, smpCnt), časových značek, HMAC[2] a digitálních podpisů. Pokud přijde zpráva s nižším číslem, starším časem nebo neplatným HMAC, je automaticky zamítnuta, čímž se opakování zabrání.
- **Spoofing** [141]:Útočník se snaží vydávat za legitimní zařízení, aby zasílal falešné měření či řídicí příkazy. IEC 62351–6 vyžaduje digitální podpisy (např. RSA-PSS/SHA-256) v „security extension“ poli zprávy GOOSE/SV, což zaručuje, že pouze certifikovaný odesílatel může zprávu podepsat, tím se podsouvání falešných dat zabrání.
- **Man-in-the-Middle** [147, 136, 149]: Pasivní i aktivní útok, kdy útočník zachytí nebo modifikuje komunikaci. Části IEC 62351–3 a 4 zavádějí TLS pro ochranu TCP/IP protokolů (např. MMS nebo GOOSE přes UDP), včetně vzájemné autentizace pomocí X.509 certifikátů a ověřování integrity kanálu. Část IEC 62351-9 pak definuje správu certifikátů a životní cyklus klíčů, čímž se snižuje riziko MITM.
- **Denial-of-Service (DoS)** [135, 147]: Cílem je zahlcení nebo zahlcování zařízení (např. SYN flood, přetížení bufferu), což může přerušit komunikaci. IEC 62351-7 zavádí SNMP[3]/MIB[4] monitorování provozu (např. anomalie v počtu paketů), což umožňuje sledovat náznaky DoS. Část IEC 62351–3 navíc doporučuje ochrany na úrovni TLS, aby se riziko DoS snížilo.
- **Eavesdropping (odposlech)** [147, 136]: Pasivní útok, kdy útočník pouze naslouchá komunikaci a získává citlivé informace. Šifrování pomocí TLS (IEC 62351–3 a 4) brání tomuto typu útoků tím, že zajišťuje, že zachycená data nelze přečíst.
- **False Data Injection (vkládání falešných dat)** [141]: Cílené vkládání škodlivých dat do přenosu, které mohou změnit chování systému. IEC 62351–6 chrání pomocí digitálních podpisů a HMAC, které ověřují původ a integritu dat, pokud nelze legitimně ověřit podpis, systém je zamítne.

[1]RBAC (Role-Based Access Control) je model řízení přístupu, kde jsou oprávnění přiřazena rolím a uživatelé získávají práva na základě svých rolí.

[2]Hash-based Message Authentication Code, Kryptografická autentizační technika, která používá hash funkci a tajný klíč.

[3]Simple Network Management Protocol, protokol pro monitorování a správu síťových zařízení.

[4]Management Information Base, typ databáze v ASCII textovém formátu.

4.1.3 Standard NIST 800-82

NIST SP 800-82 [194] poskytuje podrobný průvodce pro kybernetickou bezpečnost průmyslových kontrolních systémů, včetně energetických infrastruktur. Standard poskytuje komplexní rámec pro ochranu ICS systémů, včetně návrhu bezpečnostních opatření, která pomáhají chránit komunikační kanály, zařízení a operační technologie. NIST SP 800-82 uvádí různé kybernetické hrozby, které mohou ohrozit ICS systémy. Hrozby specifikované v tomto dokumentu zahrnují:

- **Neautorizovaný přístup a zneužití systému**: Standard uvádí, že neautorizovaný přístup k ICS systémům může vést k manipulaci s daty, zařízeními nebo k ovládání systémů, což může mít závažné důsledky pro bezpečnost a stabilitu celého systému. Doporučuje se použití autentizace a kontroly přístupu k ochraně proti těmto hrozbám.
- **Manipulace s daty a příkazy**: Manipulace s měřenými daty nebo příkazy pro zařízení je uvedena jako riziko, které může ohrozit integritu operací. NIST SP 800-82 zdůrazňuje nutnost ochrany integrity dat a doporučuje metody, jako je digitální podpis nebo šifrování, pro zajištění, že data nebyla změněna nebo podvržena.
- **Man-in-the-Middle**: Útoky typu MITM jsou přímo zmiňovány ve NIST SP 800-82, kde standard zmiňuje riziko, že útočník může zachytit a změnit data mezi komunikujícími stranami. Zdůrazňuje se šifrování a autentizace jako primární opatření k prevenci těchto útoků.
- **Zranitelnosti v komunikačních protokolech**: NIST SP 800-82 uvádí, že zranitelnosti v komunikačních protokolech, jako je Modbus, DNP3, IEC 61850, a další, mohou představovat bezpečnostní riziko. Standard doporučuje, aby byla implementována opatření pro ochranu komunikace, včetně šifrování, autentizace a kontroly integrity dat, pro zajištění, že komunikace mezi zařízeními není kompromitována

NIST SP 800-82 uvádí konkrétní bezpečnostní opatření k ochraně přenosu dat a komunikace před kybernetickými hrozbami:

- **Šifrování**: Šifrování je klíčovým opatřením k ochraně důvěrnosti a integrity přenášených dat. Standard doporučuje použití TLS a dalších šifrovacích protokolů k zabezpečení komunikace mezi zařízeními ICS a systémy.
- Autentizace zařízení a uživatelů: NIST SP 800-82 doporučuje, aby byla implementována autentizace jak pro zařízení, tak pro uživatele, kteří mají přístup k citlivým informacím nebo řízení zařízení. To zahrnuje použití digitálních certifikátů a bezpečné správy klíčů.
- **Integrita dat**: k zajištění integrity přenášených dat standard doporučuje použití digitálních podpisů a hashovacích funkcí k ověření, že data nebyla během přenosu změněna.
- **Monitorování a detekce**: Standard doporučuje implementaci systémů pro monitorování komunikace a detekci anomálií v reálném čase. To pomáhá identifikovat potenciální hrozby, jako jsou MITM útoky nebo manipulace s daty.
- **Kontrola přístupu**: Standard doporučuje implementaci mechanismů řízení přístupu k omezení přístupu k zařízením a síťovým prostředkům, zajišťující, že pouze autorizovaní uživatelé a systémy mají přístup k citlivým datům ICS. To zahrnuje řízení přístupu na základě rolí (RBAC) a správu privilegovaných práv.

4.1.4 Standard IEEE 1686

IEEE 1686-2022 [43] je standard zaměřený na ochranu kybernetické bezpečnosti v oblasti IED, která se používají v energetických systémech. Tento standard definuje specifikace pro funkce a schopnosti IED, které jsou nezbytné pro zajištění ochrany proti kybernetickým hrozbám. Standard stanovuje požadavky na autentizaci, autorizaci, integritu dat, důvěrnost dat a reakci na bez-

pečnostní incidenty. Standard řeší kybernetické hrozby v souvislosti s ochranou IED v průmyslových kontrolních systémech. Hlavní hrozby zahrnují:

- **Neautorizovaný přístup k zařízení**: Hrozby spojené s neautorizovaným přístupem, který může vést k manipulaci s daty nebo změnám v konfiguraci zařízení. Tento problém je klíčově řešen autentizací, která je nezbytná pro prevenci těchto útoků.
- **Manipulace s daty**: Manipulace s měřenými daty nebo podvržení řídicích příkazů je výslovně uvedena jako riziko. Standard doporučuje implementaci opatření k ochraně integrity dat, která pomáhají předcházet těmto hrozbám.
- **Man-in-the-Middle**: Hrozba MITM, kde útočník může zachytit a změnit data mezi dvěma komunikujícími stranami, je zmíněna jako potenciální vektor útoku. Šifrování a autentizace jsou uvedeny jako základní opatření pro zamezení těchto útoků.

Standard IEEE 1686-2022 definuje několik konkrétních mitigačních opatření, jak chránit přenos dat a komunikaci proti kybernetickým hrozbám:

- **Šifrování**: Šifrování je klíčovým bezpečnostním opatřením pro ochranu důvěrnosti a integrity přenášených dat. IEEE 1686-2022 doporučuje použití SSL/TLS a dalších šifrovacích protokolů pro zabezpečení komunikace mezi zařízeními a SCADA systémy.
- **Autentizace zařízení a uživatelů**: IEEE 1686-2022 požaduje, aby byla implementována autentizace jak pro zařízení, tak pro uživatele, kteří mají přístup k citlivým informacím nebo řízení zařízení. To zahrnuje použití digitálních certifikátů a šifrovaných klíčů pro zabezpečení autentizace mezi zařízeními.
- **Integrita dat**: Pro zajištění integrity dat jsou doporučeny technologie jako digitální podpisy a kontrolní součty, které umožňují ověřit, že data nebyla během přenosu změněna.
- **Monitorování a detekce anomálií**: Standard doporučuje implementaci monitorovacích systémů pro detekci anomálií v reálném čase. To pomáhá identifikovat potenciální útoky, jako jsou MITM nebo podvržení příkazů.
- **Kontrola přístupu**: IEEE 1686 doporučuje použití kontrolních mechanismů přístupu k zařízením a síťovým prostředkům, aby byl přístup omezen pouze na autorizované uživatele a zařízení. To zahrnuje správu uživatelských práv a implementaci zásad pro řízení přístupu na základě rolí (RBAC).

4.1.5 ENISA

ENISA[5] (European Union Agency for Cybersecurity) je agentura Evropské unie, která se zaměřuje na zajištění kybernetické bezpečnosti v EU. Agentura poskytuje podporu členským státům EU, soukromému sektoru, a dalším organizacím při vývoji a implementaci politik a nástrojů pro kybernetickou bezpečnost. ENISA pravidelně vydává reporty (Threat Landscape), osvědčené postupy (best practices), které slouží jako cenné zdroje pro organizace, vlády a jednotlivce, kteří se zabývají kybernetickou bezpečností. Tyto dokumenty poskytují konkrétní návod a doporučení k ochraně před kybernetickými hrozbami a zajištění bezpečnosti informačních systémů.

Best practices Dokumenty vydávané ENISA poskytují nástroje a doporučení pro zajištění kybernetické bezpečnosti. Cílem těchto dokumentů je podpořit efektivní řízení rizik a poskytovat osvědčené metody pro prevenci a reakci na kybernetické hrozby.

Best Practices for Cyber Crisis Management [76]: Tento dokument se soustředí na řízení celkového cyklu kyberkrizí, od prevence po obnovu, a vyzdvihuje význam mezinárodní koordinace při krizových situacích. Zmiňuje i specifické nástroje jako jsou krizové týmy a simulace krizí.

[5] https://www.enisa.europa.eu/

Good Practice Guide on NCSS [69]: Tento dokument je zaměřen na rozvoj a implementaci národních kybernetických bezpečnostních strategií a klade důraz na ochranu národních infrastruktur a spolupráci na evropské úrovni. Zmiňuje i specifika ochrany dodavatelských řetězců a implementaci regulací jako je NIS Directive.

Good Practices for Supply Chain Cybersecurity [75]: Tento dokument se zaměřuje na specifické hrozby spojené s kybernetickou bezpečností dodavatelských řetězců a doporučuje opatření pro řízení rizik u subdodavatelů, včetně hodnocení jejich kybernetických schopností a zabezpečení spravovaných služeb.

Good Practices for Security of Internet of Things [70]: Tento dokument se zaměřuje na specifické bezpečnostní výzvy spojené s IoT[6] zařízeními v kontextu inteligentní výroby. Důraz je kladen na ochranu zařízení a komunikačních kanálů mezi nimi, včetně zranitelností ve firmwaru a útoků typu Man-in-the-Middle.

Communication network interdependencies in Smart Grids [68]: Tento dokument se soustředí na ochranu komunikačních odkazů v rámci smart grids. Zmiňuje specifické technologické a organizační metody, jak chránit komunikační interdependence a jak se vyhnout kaskádovým poruchám v těchto systémech.

Z pohledu kybernetické bezpečnosti se všechny uvedené dokumenty zaměřují na ochranu kritické infrastruktury před různými kybernetickými hrozbami a vývojem účinných opatření pro řízení kyberkrizí. Shodují se v několika klíčových oblastech:

- **Identifikace a analýza kybernetických hrozeb**: Všechny dokumenty se zaměřují na identifikaci a analýzu různých hrozeb, které mohou ohrozit kritické systémy, jako jsou energetické sítě, zdravotní péče, doprava, IoT zařízení a dodavatelské řetězce. Hrozby zahrnují útoky typu ransomware, malware, phishing, útoky na IoT zařízení, a manipulace s daty.
- **Mitigační opatření**: Všechny dokumenty zdůrazňují důležitost prevence a připravenosti prostřednictvím implementace opatření, která zahrnují hodnocení rizik, testování zranitelností, školení pracovníků, a rozvoj krizových plánů. V mnoha případech jsou doporučována cvičení a simulace pro testování krizových plánů.
  - **Hodnocení rizik a analýza zranitelností**: Všechny dokumenty kladou důraz na pravidelnou analýzu a hodnocení rizik, které zahrnuje identifikaci potenciálních hrozeb, zranitelností a slabých míst v systémech. Tato hodnocení jsou nezbytná pro pochopení, jaké konkrétní hrozby mohou ohrozit bezpečnost dané infrastruktury (např. energetické sítě, IoT zařízení) a jaký bude jejich dopad v případě realizace útoku.
  - **Školení pracovníků**: Školení a vzdělávání pracovníků o kybernetické bezpečnosti je neoddělitelnou součástí prevence. Všechny dokumenty doporučují implementaci pravidelných školení, která by měla být zaměřena na:
    - **Zvýšení povědomí o kybernetických hrozbách**: Zajištění informovanosti o aktuálních trendech v kybernetických hrozbách jako jsou phishing, malware, ransomware a další typy útoků.
    - **Trénink specifických dovedností**: Školení zaměstnanců v tom, jak správně reagovat na incidenty, jak používat bezpečnostní nástroje, jak monitorovat podezřelé aktivity a jak správně implementovat bezpečnostní politiky.
    - **Pravidelné opakování školení**: Zajištění, aby byli zaměstnanci stále informováni o nových hrozbách a technologiích ochrany.
  - **Krizové plány**: Důležitým bodem ve všech dokumentech je vypracování krizových plánů. Tyto plány by měly obsahovat konkrétní kroky pro reagování na kybernetické incidenty a měly by být pravidelně aktualizovány, aby odpovídaly aktuálním hrozbám.

[6] Internet of Things, síť propojených zařízení schopných sběru a výměny dat prostřednictvím internetu.

  - **Cvičení a simulace**: Simulace a cvičení jsou považovány za klíčové pro ověření efektivity krizových plánů a připravenosti organizace na kyberkrizi. Všechny dokumenty se shodují na tom, že cvičení by měla být pravidelná a realistická, aby byly všechny možné scénáře skutečně prověřeny.
- **Spolupráce mezi veřejným a soukromým sektorem**: Všechny dokumenty zmiňují význam spolupráce mezi státními institucemi, soukromými subjekty a mezinárodními organizacemi při sdílení informací a koordinaci reakce na kyberkrize.
- **Obnova a analýza po incidentu**: Po každé kyberkrizi je doporučeno provést analýzu incidentu, která identifikuje příčiny a přispěje k prevenci budoucích problémů. Obnova kritických systémů je kladena na důraz v každém dokumentu, včetně návrhu mechanismů pro obnovu služeb a integrity dat.

ENISA Threat Landscape report (2020-2024) V průběhu let 2020 až 2024 se kybernetické hrozby, které byly identifikovány ve zprávách ENISA Threat Landscape (zprávy a za roky 2020 až 2024 - [71, 72, 73, 74, 77]), vyvíjely, ale některé útoky se opakují a jsou tak považovány za nejčastější a nejzávažnější.

Ransomware a Malware se ukazují jako nejběžnější a nejzávažnější hrozby, které byly přítomné každý rok. Tyto útoky stále představují obrovské riziko pro organizace, zvláště když ransomware stále více cílí na kritickou infrastrukturu a data. Vysoká frekvence DDoS útoků ukazuje na stálé nebezpečí této hrozby, která se objevuje ve všech letech. DDoS útoky, které se zaměřují na přetížení a znepřístupnění systémů, jsou totiž častým nástrojem kyberzločinců a hacktivistů.

Vedle těchto hrozeb se v novějších letech stále častěji objevují i jiné formy útoků. Social Engineering, tedy manipulace s lidmi za účelem získání citlivých informací, se stává stále častější metodou. Tato technika, která je často používána v rámci Phishingu nebo Spear-phishingu, vykazuje rostoucí trend v roce 2022 a 2023. Stejně tak Supply Chain Attacks (útoky na dodavatelské řetězce), které mohou využívat Malware (např. v infikovaných aktualizacích softwaru), Phishing (např. pro získání přihlašovacích údajů subdodavatelů) nebo Exploity (např. pro zneužití neopravených zranitelností u třetích stran), a Information Manipulation (např. např. šíření falešných provozních hlášení či zkreslování datových záznamů) jsou v posledních letech více zmiňovány.

V případě manipulace s informacemi se útočníci často spoléhají na techniky, jako jsou dezinformace a deepfake, které se používají k šíření nepravdivých informací nebo zkreslení reality. Například deepfake technologie mohou být využívány k vytváření falešných videí, která ovlivní veřejný obraz osobností nebo organizací. Phishing může být také součástí této manipulace, kdy útočníci získávají citlivé informace, které následně využívají k šíření dezinformací nebo ovlivnění klíčových rozhodovacích procesů.

Data Breach (únik dat) a Information Leakage (únik informací) se staly také významnými hrozbami v oblasti kybernetické bezpečnosti. Úniky dat mohou nastat prostřednictvím technik jako Phishing nebo Ransomware, nebo mohou být způsobeny Exploity, které zneužívají zranitelnosti v systémech a umožňují útočníkům odcizit citlivá data. V roce 2022 a 2023 se tyto útoky staly častějšími a ukazují na rostoucí potřebu ochrany citlivých informací před neoprávněným přístupem.

Únik informací může nastat prostřednictvím neúmyslného odhalení citlivých dat, které nejsou nutně ukradeny, ale mohou být zpřístupněny nevhodně. Například prostřednictvím neopatrného odesílání e-mailů, kdy citlivé informace omylem pošle zaměstnanec na nesprávnou adresu, nebo nešifrovaných přenosů dat, které umožňují, aby byla citlivá data zachycena během přenosu, nebo špatně zabezpečených databází, které jsou omylem zpřístupněny veřejnosti.

4.2 Útoky na elektroenergetické systémy

Elektroenergetické systémy představují klíčovou kritickou infrastrukturu, jejíž propojení s korporátními a externími sítěmi výrazně zvyšuje riziko kybernetických útoků. Tyto útoky mohou mít dalekosáhlé důsledky od ztráty dat až po fyzické destrukce zařízení nebo dlouhodobé narušení dodávek energie. Tato kapitola popisuje nejznámější zdokumentované útoky. U každého útoku je uveden popis, zdokumentované fáze útoku a zaznamenané dopady (technické, ekonomické, geopolitické).

4.2.1 Stuxnet

Stuxnet [167] je považován za jeden z prvních známých kybernetických útoků, který cílil na fyzickou infrastrukturu a způsobil skutečné fyzické škody. Objevený v roce 2010, Stuxnet byl sofistikovaný malware navržený specificky k sabotáži íránského jaderného programu tím, že narušil centrifugy používané k obohacování uranu. Jeho objevení odhalilo novou éru kybernetické války, kde digitální útoky mohou mít bezprostřední a vážné důsledky v reálném světě.

Stuxnet údajně ohrozil íránské PLC[7], shromažďoval informace o průmyslových systémech a způsobil, že se rychle se točící odstředivky roztrhly Anatomie malwaru zahrnuje tři moduly: červ, který provádí všechny rutiny související s hlavním užitečným zatížením útoku; odkazový soubor, který automaticky provádí šíření kopií červa; a komponentu rootkit zodpovědnou za skrytí všech škodlivých souborů a procesů. Obvykle se do cílového prostředí zavádí prostřednictvím infikovaného USB flash disku. Červ se poté šíří po síti a vyhledává software Siemens Step7 v počítačích, které řídí PLC. Při neexistenci kteréhokoli kritéria se Stuxnet stane v počítači spícím. Pokud jsou obě podmínky splněny, Stuxnet zavádí infikovaný rootkit do softwaru PLC a Step7, modifikuje kód a dává neočekávané příkazy PLC a vrací uživatelům zpět smyčku normálních operačních hodnot. Stuxnet se skládá s celkem šesti fází [165]:

1. Infikování: V první fázi je pomocí USB flash disku nebo jiného media infikován počítač s operačním systém Windows červem tak, že vkládá do databáze počítače škodlivé digitální certifikáty. Tento krok pokračuje na všechny dostupné počítače v sítí. Certifikáty se tváří jako důvěryhodné a tím je usnadněn přístup do zařízení a není upozorněn detekční systém.
2. Prohledávání: V druhé fázi červ kontroluje, zda je zařízení součástí průmyslového řídícího systému od společnosti Siemens.
3. Aktualizace: V případě, že je nalezen požadovaný typ zařízení, červ proveden pokus o připojení do Internetu a stažení jeho nejnovější verze. V opačném případě se neprovádí žádá činnost na daném zařízení.
4. Kompromitace: Další fázi červa je napadení vybraných zařízení (především se jedná o PLC) tzv. zero-day zranitelností, která nejsou identifikované a analyzované.
5. Kontrola: V této fázi již Stuxnet přechází od analýzy k ovládání samotných zařízení. Z počátku je sledováno chování na základě, kterého převzata kontrola nad danými zařízeními tak, aby došlo k jejich selhání.
6. Poškození: Během části kontrola/ovládání páté fáze probíhá paralelně generování falešných zpráv ostatním prvkům sítí, které se jeví jako legitimní s normálními hodnotami.

Dopad Útok Stuxnet měl dalekosáhlé dopady, nejen tím, že fyzicky poškodil íránské jaderné centrifugy, ale také tím, že změnil povahu kybernetické války a bezpečnostní politiky. Jeho úspěch ukázal, že kybernetické útoky mohou být použity k dosažení strategických vojenských cílů bez tradičního ozbrojeného konfliktu.

[7] Programmable Logic Controller je průmyslový počítač, určený k řízení prvků v průmyslu.

- Fyzické Poškození Infrastruktury [167]: Stuxnet úspěšně poškodil přibližně 1 000 íránských jaderných centrifug, což výrazně zpomalilo schopnost Íránu obohacovat uran.
- Počátek kybernetických válek [165]: Útok odstartoval éru kybernetické války, kde státy začaly otevřeně vyvíjet a používat kybernetické zbraně proti infrastruktuře jiných zemí.
- Mezinárodní Reakce a Kybernetická Obrana [165]: Stuxnet vyvolal globální diskusi o potřebě lepší ochrany kritické infrastruktury a průmyslových kontrolních systémů před kybernetickými útoky.
- Normy [165]: Útok přispěl k zintenzivnění úsilí o vytvoření mezinárodních norem.

4.2.2 Shamoon

Útok Shamoon [206], také známý jako Disttrack, je druh destruktivního malware, který byl poprvé identifikován v roce 2012 společností Seculert[8]. Jeho hlavním cílem byly energetické společnosti v Saúdské Arábii, přičemž nejvýznamnějším obětí se stala společnost Saudi Aramco, největší světový exportér ropy. Útok byl cílen na 32bitové a 64bitové verze operačního systému Microsoft Windows v IT sítích, které byly napojené na OT systémy. Útok Shamoon byl zvláštní svou schopností přepsat soubory na pevném disku infikovaných počítačů a zanechat je nefunkční tím, že je nahradil obrazem vypálené americké vlajky. V době incidentu se jednalo o jeden nejdestruktivnějších kybernetických útoků na průmyslové společnosti v historii. Shamoon se skládá s celkem šesti fází [65].

1. Infikování (Phising): V první fázi útoku jsou zasílány zaměstnancům cílové organizace emaily se škodlivými dokumenty, které se jeví jako běžné soubory balíku Microsoft Office.
2. Spuštění: Infikovaná příloha po otevření dokumentu vyvolá na pozadí prostředí PowerShell a umožní vzdálený přístup z příkazového řádku do kompromitovaného počítače.
3. Nasazení I: Útočníci nyní mohou komunikovat s ohroženým počítačem a vzdáleně na něm provádět příkazy. To vede k nasazení dalších nástrojů a malwaru do dalších prvků v síti nebo k eskalaci oprávnění v síti.
4. Prohledávání: V této fázi útočník analyzuje připojení napadené sítě k dalším systémům a vyhledává přístup na kritické prvky.
5. Nasazení II: Útočník provedené nahrání malwaru Shamoon na prvky s operačním systémem Windows.
6. Šířená a poškození: V poslední fázi se malware Shamoon šíří po síti (po vymazání se šíří na další zařízení), maže data pevných disků a nahrazuje je vlastními daty.

Dopad Poškození více než 30 000 počítačů v případě ropné společnosti Saudi Aramco [206]. Dle vyjádření společnosti byly napadeny jen kancelářské počítače a do původního stavu byl systém obnoven do jednoho týdne. Podle odhadů bezpečnostních analytiků se však mohla obnova pohybovat v řádů týdnů až jednoho měsíce.

- Zničení Dat: V případě Saudi Aramco útok Shamoon zničil data na přibližně 30 000 počítačích, což způsobilo významný výpadek IT systémů.
- Ekonomické Ztráty: Přestože útok neovlivnil produkci ropy, způsobil významné ekonomické ztráty spojené s obnovou IT infrastruktury.
- Reputační Škody: Útok také poškodil reputaci postižených společností a zdůraznil jejich zranitelnost vůči kybernetickým útokům.

[8]Seculert byla společnost zabývající se cloudovými technologiemi v oblasti kybernetické bezpečnosti se sídlem v Petah Tikva v Izraeli.

4.2.3 Flame

Flame [56], známý také jako Flamer nebo sKyWIper, je vysoce sofistikovaný a komplexní malware, který byl poprvé identifikován a analyzován v roce 2012 bezpečnostními a výzkumnými skupinami, mezi kterými hrál klíčovou roli Kaspersky Lab. Flame byl primárně navržen k širokému spektru špionážních aktivit, včetně zaznamenávání klávesnicových úhozů, pořizování snímků obrazovky, aktivace mikrofonů k odposlechu, sledování síťové komunikace a krádeže informací z infikovaných systémů. Jeho aktivita byla zaznamenána hlavně na Blízkém východě, zejména v Íránu, kde byl použit pro rozsáhlou špionážní kampaň proti vládním organizacím, vzdělávacím institucím a individuálním uživatelům.

Flame představuje milník v evoluci malwaru a kybernetické války, ukazujíc na složitost a rozmanitost nástrojů, které mohou být použity pro státní špionáž a kybernetické operace. Útok pomocí malware Flame (také známého jako Flamer nebo sKyWiper) využíval řadu sofistikovaných technik a vektorů pro infiltraci a špionáž v cílených systémech. Zde jsou klíčové aspekty jeho vektoru útoku [56]:

1. Sociální inženýrství a phishing: Flame mohl být šířen prostřednictvím phishingových emailů a sociálního inženýrství, kde útočníci manipulovali s uživateli, aby nevědomky spustili škodlivý kód.
2. Využití zranitelností: Flame využíval zranitelnosti v operačních systémech Windows k replikaci a šíření mezi počítači v síti. Jednou z klíčových taktik bylo zneužití zranitelností v síťovém stacku Windows pro šíření bez nutnosti uživatelské interakce.
3. Padělané certifikáty: K maskování své škodlivé aktivity a k obcházení bezpečnostních kontrol používal Flame padělané certifikáty, které vypadaly, jako by byly vydány důvěryhodným certifikačním orgánem. Tím mohl obejít některé mechanismy zabezpečení.
4. Modulární struktura: Flame byl navržen jako modulární framework, což umožňovalo útočníkům na dálku instalovat nové škodlivé moduly nebo aktualizovat stávající. Tato flexibilita umožňovala adaptaci útoku na konkrétní cíle nebo úkoly.
5. Klíčové loggery a screenshoty: K získávání informací Flame využíval klíčové loggery a nástroje pro pořizování screenshotů, které umožňovaly útočníkům sledovat aktivity uživatelů a sbírat citlivé informace.
6. Síťový sniffing: Flame byl také schopen provádět síťový sniffing, což mu umožňovalo zachytávat a analýzovat síťový provoz v infikované síti a získávat další citlivé informace.

Dopad Dopad kybernetického útoku Flame byl významný jak z hlediska škod, které způsobil na cílových systémech, tak z hlediska širších důsledků pro kybernetickou bezpečnost a mezinárodní vztahy. Zde jsou některé z dopadů kybernetického útoku Flame:

- Krádež citlivých údajů [56]: Škodlivý software Flame byl navržen tak, aby z infikovaných počítačů odcizil citlivá data, včetně dokumentů, e-mailů a další komunikace. Předpokládá se, že útok ohrozil citlivé informace vládních agentur a dalších organizací v několika zemích.
- Sofistikovanost útoku [56]: Kybernetický útok Flame byl velmi sofistikovaný a využíval pokročilé techniky, aby se vyhnul detekci a rychle se šířil infikovanými sítěmi. Předpokládá se, že útok provedla dobře financovaná a dobře organizovaná skupina se značnými odbornými znalostmi v oblasti kybernetické bezpečnosti.
- Mezinárodní napětí [62]: Předpokládá se, že kybernetický útok Flame byl součástí rozsáhlejší kybernetické špionážní kampaně, která byla obecně připisována Spojeným státům a Izraeli. Útok zvýšil napětí mezi těmito zeměmi a Íránem a upozornil na možnost kybernetického konfliktu mezi státy.

- Zvýšený důraz na kybernetickou bezpečnost [62]: Kybernetický útok Flame spolu s dalšími významnými kybernetickými útoky zvýšil povědomí o důležitosti kybernetické bezpečnosti a o potřebě zdokonalit bezpečnostní opatření na ochranu před kybernetickými hrozbami. Útok podnítil vývoj nových obranných opatření a technologií, včetně zdokonaleného monitorování sítí a možností reakce na incidenty.

4.2.4 Havex

Kybernetický útok Dragonfly/Havex [181] byl objeven v roce 2014 společností Symantec, která se zabývá kybernetickou bezpečností. Útok byl zaměřen na společnosti v energetickém sektoru, zejména na průmyslové řídicí systémy. Hlavním účelem bylo ukrást citlivá data z infikovaných systémů. Malware byl schopen pořizovat snímky obrazovky, zaznamenávat stisky kláves a krást přihlašovací údaje. Ukradená data pak byla exportována na příkazové a řídicí servery provozované útočníky.

Dragonfly byl navržen tak, aby cílil zejména na průmyslové řídicí systémy používané v energetice. Po infikování těchto systémů malwarem mohli útočníci získat kontrolu nad systémy a potenciálně způsobit fyzické škody nebo narušit provoz. Průběh útoku se skládál s celkem tří fází [181]:

1. V první fázi je využit útok phising, který rozesílá email vybraným uživatelům. Email obsahuje infikovaný PDF soubor, který po otevření umožňuje sbírat informace o webové komunikaci uživatele.
2. Analýza: Data od uživatelů jsou analyzována a specifické webové stránky jsou infikovány malwarem. Cílem je při další návštěvě webové stránky přesměrovat uživatele na škodlivou stránku, která umožní stažení malwaru pro vzdálený přístup.
3. Kompromitace: Po dosažení přistup na zařízení oběti je provedeno nakažení legitimního softwaru, který si mohou klienti nainstalovat a tím např. povolit přístup do svého zařízení.

Dopad Útok byl cílen na několik společností a vždy byli použity jiném metody pro získání vzdáleného přístupu. V případě jednoho cíle bylo provedeno více než 200 stažení infikovaného softwaru než poskytovatel objevil chybu. V dalších případech byl infikovaný software dostupný v řádu dnů až týdnů než byl odhalen. Samotný dopad na cílené prvky není znám. Zde jsou hlavní dopady útoku:

- Narušení provozu [181]: Havex byl navržen tak, aby z infikovaných systémů ukradl citlivá data a potenciálně získal kontrolu nad průmyslovými řídicími systémy. Útok měl potenciál způsobit fyzické škody nebo narušit provoz, ačkoli neexistují žádné důkazy, že k tomu došlo.
- Hospodářský dopad [60]: Havex byl zaměřen na společnosti v energetickém odvětví, které je kritickou součástí světové ekonomiky. Útok měl potenciál způsobit značné hospodářské škody, pokud by se mu podařilo narušit provoz nebo způsobit fyzické škody.
- Zvýšené povědomí o kybernetické bezpečnosti [60]: Spolu s dalšími významnými útoky na kritickou infrastrukturu zvýšil povědomí o důležitosti kybernetické bezpečnosti a o potenciálu kybernetických útoků způsobit fyzické škody a narušení.
- Přisuzování odpovědnosti a mezinárodní vztahy [161]: Havex byl široce připisován skupině s podezřením na vazby na Rusko, což zvýšilo obavy z možných státem sponzorovaných kybernetických útoků na kritickou infrastrukturu. Útok vedl ke zvýšení napětí mezi Ruskem a západními zeměmi a zdůraznil potřebu zlepšení mezinárodní spolupráce v otázkách kybernetické bezpečnosti.
- Vývoj obranných opatření [60]: Havex podnítil vývoj nových obranných opatření a technologií, včetně zdokonaleného monitorování sítí a schopností reakce na incidenty.

4.2.5 Steel mill in Germany

Kybernetický útok [54] byl zaměřen na ocelárnu v Německu v rokce 2014 a byl proveden pomocí spear-phishingového e-mailu, který obsahoval škodlivou přílohu. Po otevření přílohy se útočníkům podařilo získat přístup k průmyslovým řídicím systémům ocelárny. Útok způsobil ocelárně značné škody, včetně poškození vysoké pece, které vedlo k neplánovanému odstavení ocelárny. Útok způsobil také fyzické poškození dalších zařízení v huti. Průběh útoku se skládal z těchto fázi [173]:

1. Spear-phishingový e-mail: zaměřený na vybrané zaměstnance s cílem zjištění přihlašovacích údajů. E-mail byl pečlivě vytvořen tak, aby vypadal jako legitimní zpráva, a byl zaměřen konkrétně na zaměstnance ocelárny.
2. Napadení IT: Po otevření škodlivé přílohy došlo ke stažení a instalaci malwaru do počítače oběti. Malware byl navržen tak, aby se rychle šířil sítí ocelárny a dokázal ohrozit její průmyslové řídicí systémy.
3. Napadení OT: není známa technika, kterou se útočníci dostali do OT části sítě, ale museli využít některou z bran mezi IT a OT. Zřejmě pro napadení IT sekce byl proveden podrobný průzkum, kterým útočníci zjistil možné slabiny OT sítě jako jsou např. špatně zabezpečené nebo neoddělené stanice, které mají přístup do obou sítí. Nebo získaný přístup na firemní účet mohl mít vysoké autorizační povolení např. na úrovni administrátora, díky čemuž útočníci měli plnou kontrolu na sítí nebo vybraným zařízeními v síti.
4. Poškození: Útočníkům se podařilo získat kontrolu nad průmyslovými řídicími systémy ocelárny a tento přístup využili k fyzickému poškození zařízení. Útočníkům se zejména podařilo poškodit vysokou pec, což vedlo k neplánovanému odstavení.

Dopad Kybernetický útok na ocelárnu v Německu měl významný dopad na cílovou organizaci i na širší prostředí kybernetické bezpečnosti. Zde jsou hlavní dopady útoku:

- Fyzické škody [177]: Útok způsobil fyzické poškození zařízení ocelárny, zejména vysoké pece, což vedlo k neplánovanému odstavení ocelárny. Toto fyzické poškození poukázalo na potenciál kybernetických útoků způsobit fyzické škody a narušení kritické infrastruktury.
- Hospodářský dopad [177]: Útok měl také významné ekonomické dopady, protože neplánované odstavení ocelárny způsobilo narušení dodavatelského řetězce a vedlo k finančním ztrátám společnosti.
- Zvýšené povědomí o rizicích kybernetické bezpečnosti [54]: Útok zvýšil povědomí o potenciálu kybernetických útoků způsobit fyzické škody a narušení kritické infrastruktury, zejména v průmyslových řídicích systémech, které se používají ve výrobě a dalších odvětvích.
- Mezinárodní vztahy [173]: Připsání útoku skupině s podezřením na vazby na Rusko vedlo ke zvýšení napětí mezi Německem a Ruskem a upozornilo na možnost státem sponzorovaných kybernetických útoků na kritickou infrastrukturu.

4.2.6 BlackEnergy

První verze útoku BlackEnergy byla detekována v roce 2007 společností Arbor Networks [97], kde se jednalo o jednoduchého trojského koně se schopností DDoS útoku. Ve druhé verzi byl již útok komplexnější a obsahoval např. instalátor pro jednoduší efektivnější distribuci softwaru. Ve třetí verzi se jedná o mnohem komplexnější útok, který nezahrnuje jen DDoS útok, ale přístup a poškození do cílových zařízení. Třetí verze útoku BlackEnergy se skládá ze dvou hlavních fází, které jsou rozděleny na několik dílčích kroků [162]:

1. Vniknutí: První fází útoku BlackEnergy je analýza napadeného systému a instalace potřebného malwaru pro úspěšné provedení útoku. Fáze se skládá z celkem tří kroků.

(a) Průzkum: Pro úspěšné nasazení malwaru je nutné provést analýzu infrastruktury cílového systému. Průzkum může probíhat řadou technik jako jsou skenování, phising atd.
(b) Infikování: Následuje samotné nasazení malwaru pro vzdálený přístup a sbírání dat s infikovaných stanic.
(c) Dolování: Po infikování následuje samotné sbírání dat, kdy jsou po určitou dobu dolovány informace pro úspěšnou realizaci útoku.

2. Útok: Druhá fáze je již samotný útok, který cílí na poškození OT systému. Fáze se skládá z celkem šesti kroků.
(a) Vývoj: Prvním krokem druhé fáze je proces učení, kdy útočník analyzuje průmyslovou komunikaci a vytváří vzory legitimní provozu. Na základě toho je vyvinut specifický škodlivý kód pro daný systém.
(b) Testování: Následuje krok testování, kde je ověřen vyvinutý kód na vlastním infrastruktuře simulují cílový systém.
(c) Nasazení: Poté je nutné škodlivý kód doručit do vybraných zařízení, k čemuž slouží vybraná forma vzdáleného přístupu do zařízení na administrátorské úrovni, která byla zajištěna v první fázi útoku.
(d) Instalace/Spuštění: Následně jsou spuštěny připravené škodlivé kódy, které způsobí poškození na koncových prvcích systému přes OT PLC/RTU jednotky.
(e) Převzetí: Paralelně s fází Instalace/Spuštění je převzetí kontroly nad pracovními stanice operátorů a tím odepření přístupu a možnosti rychlého zjištění a opravení vzniklé chyby/útoku.
(f) Odepření: Finální část je koordinace útoku s DDoS na návazné systémy pro zamezení dostupnost a koordinace při řešení chyby vzniklé útokem.

Dopad Během útoku na ukrajinský energetický průmysl bylo zasaženo nejméně 27 napájecích stanic ve třech energetických společnostech, což mělo za následek nedostupnost elektrické energie u více než 225 000 odběratelů. Zde jsou hlavní dopady útoku:

- Narušení energetické infrastruktury [98]: Útočníci byli schopni způsobit výpadky elektřiny a narušit provoz několika energetických společností na Ukrajině, což vedlo ke značným hospodářským škodám a rozsáhlému znepokojení veřejnosti.
- Hospodářský dopad [98]: Útok způsobil značné hospodářské škody, zejména v energetickém sektoru na Ukrajině. Náklady na odstranění škod způsobených útokem byly odhadnuty na miliony dolarů.
- Zvýšené povědomí o rizicích kybernetické bezpečnosti [97]: Útok zvýšil povědomí o možnosti státem sponzorovaných kybernetických útoků na kritickou infrastrukturu a zdůraznil potřebu zdokonalit opatření kybernetické bezpečnosti na ochranu před takovými útoky.
- Reakce a obnova [162]: Ukrajinská vláda a energetické společnosti přijaly opatření ke zlepšení svých kyberbezpečnostních opatření a k ochraně před budoucími útoky. To zahrnovalo zavedení nových bezpečnostních opatření a zvýšené sdílení informací o kybernetických hrozbách.
- Přisuzování a mezinárodní vztahy [97]: Útok byl široce připisován skupině s podezřením na vazby na Rusko, což vedlo ke zvýšení napětí mezi Ukrajinou a Ruskem. Útok také podnítil mezinárodní diskuse o potřebě zlepšit spolupráci v oblasti kybernetické bezpečnosti a sdílení informací, aby se podobným útokům v budoucnu zabránilo.

4.2.7 Duqu

Kybernetický útok Duqu [63] byl sérií útoků, které byly zaměřeny na organizace na Blízkém východě a v dalších částech světa. Útoky začaly v roce 2011 a pokračovaly v roce 2012 a byly provedeny pomocí sofistikovaného malwarového nástroje známého jako Duqu. Malware Duqu byl navržen tak, aby z cílových organizací odcizil citlivé údaje, včetně přihlašovacích údajů a dalších citlivých informací. Malware byl také navržen tak, aby byl vysoce skrytý a obtížně odhalitelný. Kybernetický útok Duqu byl velmi sofistikovaný útok, který využíval různé techniky k infikování cílových systémů a krádeži citlivých dat. Zde jsou dílčí kroky [171]:

1. Spear-phishingové e-maily: Útočníci použili spear-phishingové e-maily, aby se zaměřili na zaměstnance cílových organizací. Tyto e-maily byly navrženy tak, aby vypadaly jako legitimní e-maily, a obsahovaly škodlivé přílohy nebo odkazy, které po kliknutí stáhly do cílového systému malware Duqu.
2. Zero-day exploits: Malware Duqu byl navržen tak, aby využíval zranitelnosti nultého dne v operačních systémech Windows a získal přístup do cílového systému. Útočníci tyto exploity použili k získání přístupu k cílovým systémům a k instalaci malwaru Duqu.
3. Šíření: Jakmile byl malware Duqu nainstalován v cílovém systému, vyhledával další zranitelné systémy v síti a pokoušel se šířit. Malware byl vysoce sofistikovaný a používal řadu technik, aby zůstal skrytý a vyhnul se odhalení.
4. Export dat: Malware Duqu byl navržen tak, aby z cílových systémů odcizil citlivá data, včetně přihlašovacích údajů a dalších citlivých informací. Malware pak ukradená data nahrával na vzdálené servery ovládané útočníky.

Dopad Kybernetický útok Duqu měl významný dopad na organizace, které byly jeho cílem, na širší oblast kybernetické bezpečnosti i na geopolitickou situaci na Blízkém východě. Zde jsou některé z dopadů útoku:

- Hospodářský dopad [171]: Útok způsobil cílovým organizacím značné ekonomické škody, zejména pokud jde o ztrátu citlivých dat a náklady na nápravu škod způsobených útokem.
- Špionáž a shromažďování zpravodajských informací [63]: Útočníkům se podařilo z cílových organizací odcizit velké množství citlivých údajů, včetně přihlašovacích údajů, důvěrných dokumentů a dalších citlivých informací. Tyto údaje mohly být použity ke špionáži nebo jiným nekalým účelům.
- Geopolitické napětí [63]: Útok byl široce připisován skupině s podezřením na vazby na Izrael, což vedlo ke zvýšení napětí mezi Izraelem a dalšími zeměmi v regionu. Útok také poukázal na potenciál státem sponzorovaných kybernetických útoků způsobit značné geopolitické napětí a škody.
- Zlepšená opatření v oblasti kybernetické bezpečnosti [171]: Útok zvýšil povědomí o potřebě zlepšit kybernetická bezpečnostní opatření na ochranu před státem sponzorovanými kybernetickými útoky na kritickou infrastrukturu a citlivé údaje. Tento útok podnítil vývoj nových nástrojů a technik kybernetické bezpečnosti, které mají podobné útoky odhalit a zabránit jim v budoucnu.

4.2.8 Industroyer

Útok Industroyer [179] někdy nazývaný také jako CrashOverride byl vysoce sofistikovaný a cílený útok, který se v prosinci 2016 zaměřil na energetické sítě na Ukrajině. Útok byl proveden pomocí malwarového nástroje známého jako Industroyer. Malware byl navržen tak, aby cílil na průmyslové řídicí systémy používané v energetických sítích a další kritické infrastruktuře. Industroyer byl

vysoce sofistikovaný a byl navržen tak, aby způsobil fyzické poškození cílových systémů. Předešlé zmíněné útoky se převážně zaměřovali na inicializační vektor, který jim dovolil infikovat zařízení v cílové infrastruktuře a tím poškodit celý systém. Útok Industroyer se od předešlých liší tím, že nepotřebuje žádné další techniky pro infikování a cílový prvků. Struktura útoku je provedena v několika krocích [190]:

1. Průzkum: Útočníci pravděpodobně provedli rozsáhlý průzkum, aby zjistili zranitelnosti v cílových systémech a vytipovali konkrétní komponenty ICS, na které se mají zaměřit.
2. Spear-phishingové e-maily: Útočníci použili k doručení malwaru Industroyer/CrashOverride do cílových systémů spear-phishingové e-maily. E-maily byly navrženy tak, aby vypadaly jako legitimní e-maily a obsahovaly škodlivé přílohy nebo odkazy, které po kliknutí stáhly malware do cílového systému.
3. Kompromitace systémů ICS: Jakmile byl malware nainstalován do cílového systému, dokázal ohrozit systémy ICS používané ukrajinskou energetickou sítí. Malware byl navržen tak, aby byl velmi skrytý a zůstal co nejdéle neodhalen.
4. Narušení energetické sítě: Útočníci použili kompromitované systémy ICS k narušení ukrajinské energetické sítě, což způsobilo výpadky proudu a další narušení dodávek energie do země.
5. Zahlazování stop: Po provedení útoku podnikli útočníci kroky, aby zahladili stopy a vyhnuli se odhalení. To zahrnovalo vymazání nebo úpravu protokolů a dalších digitálních stop, které by mohly být použity k vystopování útoku až k jeho zdroji.

Samotný útok se skládá z několika dílčích částí, které pracují paralelně ve výše uvedených bodech 3 a 4 [190]:

- MAIN BACKDOOR: Používá se k ovládání všech součástí malwaru. Připojuje se ke svým vzdáleným serverům prostřednictvím protokolu HTTPS, aby přijímal příkazy od útočníků a odesílal informace o infikovaném zařízení.
- ADDITIONAL BACKDOOR: Slouží jako záložní mechanismus v případě odhalení hlavní řídící části MAIN BACKDOOR. Pro ukrytí využívá podvrženou aplikaci Poznámkový blok, který je součástí Microsoft Windows. Pro komunikaci využívá jiné servery než hlavní řídící část.
- LAUCHNER COMPONENT: Komponenta zodpovědná za spuštění dalších částí malwaru v definovaný čas.
- PAYOLAD COMPONENT: Poslední část se zaměřuje na konkrétní protokoly používané v energetickém průmyslu (IEC 60870-5101/104, IEC 61850 a OPC DA). Funkce komponenty je rozdělena dle protokolů. Na počátku je vždy provedeno mapování sítě pro daný protokol, které je následované změnou proměnných na cíleném zařízení. Dále komponenta obsahuje část DATA WRIPER, který přepisuje registry operačního systému zařízení, tím dojde k pádu systému a zamezení jeho opětovného spuštění po restartu.

Dopad Útok způsobil značné škody na ukrajinské energetické síti, což vedlo k výpadkům a narušení dodávek energie do země. Útok také vyvolal obavy z možnosti podobných útoků na kritickou infrastrukturu po celém světě. Při realizaci útoku byl cíl na distribuční elektrickou síť v Kyjevě, kde bylo postiženo přibližně 550 000 odběratelů po dobu jedné hodiny, než byl chyba opravena.

- Hospodářský dopad [190]: Útok způsobil značné hospodářské škody na ukrajinské energetické síti, což vedlo k výpadkům proudu a přerušení dodávek energie do země. Útok rovněž způsobil škody na zařízení a infrastruktuře, které musely být nákladně opraveny nebo nahrazeny.
- Fyzické škody [179]: Útok způsobil fyzické škody na cílových průmyslových řídicích systémech

(ICS), včetně vypínačů a jističů. Toto fyzické poškození poukázalo na potenciál státem sponzorovaných kybernetických útoků způsobit fyzické škody a narušení kritické infrastruktury.

- Zvýšená informovanost [179]: Útok zvýšil povědomí o potřebě zlepšit kyberbezpečnostní opatření na ochranu před státem sponzorovanými kybernetickými útoky na kritickou infrastrukturu. Útok zdůraznil význam monitorování a ochrany průmyslových řídicích systémů, aby se v budoucnu zabránilo podobným útokům.
- Geopolitické napětí [190]: Útok byl obecně připisován skupině s podezřením na vazby na Rusko, což vedlo ke zvýšení napětí mezi Ukrajinou a Ruskem. Útok také vyvolal obavy z možnosti podobných útoků na kritickou infrastrukturu v jiných zemích, což vedlo ke zvýšení globálního napětí.

4.2.9 Triton

Triton [157], také známý jako Trisis, je kybernetický útok, který cílil na bezpečnostní systémy v průmyslových zařízeních, konkrétně na SIS[9]. Útok byl objeven v roce 2017 a jeho cílem bylo manipulovat s těmito bezpečnostními systémy tak, aby došlo k jejich selhání a potenciálnímu ohrožení lidských životů a infrastruktury. V prosinci 2017 bylo hlášeno, že bezpečnostní systémy neidentifikované elektrárny, pravděpodobně v Saúdské Arábii, byly kompromitovány, když byla cílem průmyslová bezpečnostní technologie Triconex od Schneider Electric SE. Útok využil zranitelnosti v počítačích běžících na operačním systému Microsoft Windows.

Stejně jako Industroyer je i Triton samostatně spustitelný malware implementovaný v kompilované verzi jazyka Python, díky čemuž je spustitelný bez nativní instalace Pythonu na většině operačních systémech. Celý útok se skládá ze dvou hlavních fází, které jsou rozděleny na dílčí části [182]:

1. Infikování: První fáze zahrnuje vstup malwaru do cílové sítě, obvykle prostřednictvím kompromitovaných zařízení nebo nedostatečně zabezpečených vstupních bodů. Tento malware je navržen tak, aby se skrýval a nebyl okamžitě detekován, což umožňuje jeho šíření po síti.
2. Průzkum: Po infikování systému malware provádí podrobný průzkum síťového prostředí, identifikuje systémy SIS a hledá zranitelnosti v konkrétních zařízeních, která by mohla být ohrožena. Triton se zaměřuje především na bezpečnostní řídicí systémy od společnosti Schneider Electric, zejména na kontroléry Triconex.
3. Získání kontroly: V této fázi malware přistupuje k zranitelným zařízením a začíná instalovat modifikovaný kód, který umožňuje kontrolu nad bezpečnostními funkcemi SIS. Tento krok může zahrnovat použití "zero-day"zranitelností, které ještě nejsou známé nebo opravené.
4. Manipulace s bezpečnostními systémy: Po získání přístupu se malware pokouší deaktivovat nebo upravit nastavení bezpečnostních kontrolérů, čímž eliminuje ochranné mechanismy. To zahrnuje například záměrné vypnutí nebo změnu parametrů, které by jinak zastavily nebezpečné průmyslové procesy.
5. Maskování: Aby bylo možné útok provádět co nejdéle bez odhalení, Triton využívá techniky maskování, včetně rootkitů, které zajišťují, že všechny změny provedené v systému jsou skryté a že běžné monitorovací systémy neidentifikují škodlivé aktivity.
6. Aktivace a Poškození: Útok může skončit ve fázi, kdy bezpečnostní systémy SIS jsou plně znefunkčněny. Toto by vedlo k potenciálnímu ohrožení lidí a zařízení v případě nebezpečné situace, kterou by normálně bezpečnostní systémy zachytily.

[9]Safety Instrumented Systems jsou systémy navržené k zajištění bezpečnosti v průmyslu

Dopad Útok Triton měl dopad, nejen tím, že ohrozil bezpečnostní systémy v kritických průmyslových zařízeních, ale také tím, že zvýšil povědomí o zranitelnosti průmyslových kontrolních systémů vůči kybernetickým hrozbám.

- Fyzické ohrožení infrastruktury a životů [157]: Kdyby nebyl útok včas odhalen a neutralizován, mohl vést k vážným průmyslovým haváriím, jako jsou výbuchy nebo úniky nebezpečných látek, což by ohrozilo lidské životy a poškodilo zařízení.
- Zvýšená zranitelnost průmyslové infrastruktury [157]: Incident ukázal, jak mohou kybernetické útoky cílit na bezpečnostní systémy v energetickém sektoru, konkrétně na zařízení jako Triconex, která jsou klíčová pro ochranu kritické infrastruktury.
- Globální kybernetické riziko [182]: Triton přitáhl pozornost k otázkám kybernetické války a používání kybernetických zbraní proti civilní a kritické infrastruktuře, naznačujíc, že i systémy určené k ochraně lidí mohou být zneužity k destabilizaci a sabotážím.

4.2.10 TeleBots

TeleBots [59] je hackerská skupina, která je známá svou agresivní politikou kybernetických útoků na kritickou infrastrukturu, zejména na energetickou infrastrukturu. Skupina, která vznikla po rozdělení původní BlackEnergy, je zodpovědná za některé z nejvýznamnějších kybernetických útoků na Ukrajinu, včetně útoků na energetické společnosti a finanční sektor. Její cíle zahrnují průmyslové kontrolní systémy a zařízení SCADA, přičemž její útoky mají nejen špionážní, ale i destruktivní charakter.

TeleBots je známá především díky útokům, které používají malware k narušení a zneškodnění průmyslových kontrolních systémů. Typicky využívají ransomware a disk-wiping malware, jako je NotPetya a KillDisk, k dosažení svých cílů [55]. Jejich útoky mají za cíl destabilizovat a poškodit klíčové části energetických a finančních systémů, což vede k výpadkům elektrické energie a ekonomickým škodám. Malware se šíří skrze různé vektory, včetně phishingu, a zaměřuje se na SCADA systémy, které kontrolují průmyslové procesy, včetně elektrických stanic a transformátorů. Například NotPetya byl šířen pomocí kompromitovaného ukrajinského účetního softwaru, což vedlo k masivnímu šíření po globálních sítích. Útoky nemají pevně danou strukturu, ale dají se identifikovat alespoň určité části [59]:

1. Infikování: Malware se šíří prostřednictvím phishingových e-mailů nebo infikovaných souborů. V některých případech byl NotPetya šířen skrze infikované ukrajinské účetní systémy.
2. Prohledávání a mapování sítě: Po infikování začne malware mapovat síť a vyhledávat ICS systémy, které jsou zodpovědné za správu elektrických stanic a dalších kritických infrastruktur.
3. Vyčištění a šíření: Po zjištění cílů je malware používán k vymazání dat na těchto zařízeních, čímž se stává nefunkčními a poškozuje průmyslové systémy.
4. Zablokování a Sabotáž: Po zasažení zařízení začíná malware blokovat veškerou komunikaci mezi systémy a řídícími centry, což vede k výpadkům a ztrátě dat v reálném čase.
5. Poškození: Konečným krokem je poškození a zničení systémů, což může mít za následek fyzické výpadky a ztrátu kontroly nad kritickými procesy.

Dopad Útoky prováděné skupinou TeleBots měly široký a dlouhodobý dopad na energetickou infrastrukturu a ukázaly, jak mohou kybernetické útoky ohrozit globální energetickou bezpečnost [55]. Způsobily výpadky a destabilizaci provozu v energetických systémech, což vedlo k ekonomickým ztrátám a narušení dodávek energie pro tisíce lidí.

- Fyzické poškození infrastruktury [55]: Útoky měly za cíl přerušit provoz energetických stanic, transformátorů a průmyslových kontrolních systémů, což vedlo k výpadkům elektrické energie a ohrozilo dodávky energie.
- Globální destabilizace [59]: Útoky, jako NotPetya, se rychle šířily po globálních sítích, což ukázalo zranitelnosti v energetických systémech a ve finančních infrastrukturách.
- Mezinárodní reakce [59]: Tyto útoky zdůraznily potřebu lepší ochrany kritických infrastruktur a vedly k většímu mezinárodnímu zaměření na kybernetickou obranu.
- Legislativa a normy [55]: Útoky vyvolaly diskusi o tvorbě mezinárodních bezpečnostních norem pro ochranu energetických a průmyslových systémů před kybernetickými hrozbami.

4.2.11 Shrnutí

Jak se mění dynamika kybernetického prostředí, útoky na OT se stávají sofistikovanějšími a dopady pro organizace jsou stále zvyšují. Útoky, jako byly Stuxnet, Shamoon, Flame, Havex, BlackEnergy, Dugu, Industroyer, Triton, Telebots, ukázaly, jak jsou důležité opatření proti kybernetickým hrozbám. Tyto útoky měly širokou škálu dopadů, od ztráty dat a finančních ztrát přes výpadky výroby až po fyzické poškození zařízení. Útok Stuxnet například zpomalil íránský jaderný program, zatímco útok Shamoon zničil data na 35 000 počítačích. Útoky BlackEnergy a Industroyer/CrashOverride způsobily výpadky proudu na Ukrajině, což mělo značný dopad na tamní energetický průmysl.

Vzhledem k tomu, jaký dopad mohou mít tyto útoky, je zcela zásadní školit zaměstnance v otázkách kybernetické bezpečnosti. Zaměstnanci jsou často první obrannou linií proti kybernetickým útokům a jejich schopnost rozpoznat a správně reagovat na potenciální hrozby může mít zásadní vliv na bezpečnost organizace. Například útoky se často šíří prostřednictvím phishingových emailů, což zdůrazňuje důležitost školení zaměstnanců v rozpoznání a správné reakci na tento typ hrozeb.

Kromě toho jsou důležité také testovací a trénovací prostředí, které simulují reálné systémy. Tyto prostředí umožňují organizacím testovat své bezpečnostní postupy a řešení a připravit se tak na reálné kybernetické útoky. Mohou být také použity k prezentaci účinků různých útoků, což pomáhá zaměstnancům lépe pochopit, jak se tyto útoky provádějí a jak se jim dá předejít. Například útoky, jako byly Stuxnet, Flame nebo BlackEnergy, byly velmi sofistikované a vyžadovaly podrobné technické znalosti, které byly získány právě prostřednictvím testování a tréninku v simulovaných prostředích.

4.3 Riziková analýza datové elektroenergetické infrastruktury

Riziková analýza je jednou z metod pro klasifikaci při návrhu bezpečnostních opatření v kyberfyzických systémech. S rostoucí digitalizací a konvergencí technologií v oblasti Smart Grid roste i množství potenciálních vektorů útoků a zranitelností, které mohou ohrozit dostupnost, integritu a důvěrnost provozu. Kapitola se proto zaměřuje na systematickou identifikaci, klasifikaci a hodnocení rizik, která se týkají vybrané části infrastruktury popsané v předchozí kapitole. Pro účely této analýzy jsou využity kombinované metodiky:

- **STRIDE**: pro formální identifikaci typů hrozeb a jejich pravděpodobnosti a závažnosti,
- **MITRE ATT&CK**: pro mapování fází reálných útoků na energetickou infrastrukturu a jejich logické začlenění do modelu systému,
- **GAP analýza**: pro srovnání identifikovaných rizik s pokrytím ve stávajících bezpečnostních standardech, jako jsou IEC 62443 a IEC 62351.

4.3.1 STRIDE model hrozeb

STRIDE [191] je systematická metodika pro identifikaci bezpečnostních hrozeb, původně navržená v rámci vývojového rámce Microsoft SDL (Security Development Lifecycle). Název modelu je akronymem odvozeným od šesti základních kategorií hrozeb: Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service a Elevation of Privilege. Každá z těchto kategorií reprezentuje odlišný způsob narušení bezpečnostních cílů systému – důvěrnosti, integrity, dostupnosti a odpovědnosti.

Metodika STRIDE umožňuje mapovat hrozby na jednotlivé komponenty systému (např. uživatele, zařízení, procesy nebo komunikační kanály) a tím identifikovat slabiny v návrhu či provozu. Díky této klasifikaci je možné strukturovaně uvažovat o rizicích a plánovat vhodná bezpečnostní opatření. Model STRIDE bývá v některých případech rozšiřován o další dimenze, jako je pravděpodobnost výskytu dané hrozby (Likelihood) a schopnost její mitigace (Mitigability) což je souhrnně označováno jako STRIDE-LM. Toto rozšíření usnadňuje priorizaci identifikovaných hrozeb na základě jejich reálného dopadu a náročnosti obrany. V této práci je však pro účely klasifikace využita původní varianta STRIDE, která poskytuje dostatečný rámec pro základní analýzu. Přehled jednotlivých kategorií hrozeb je uveden v tabulce 4.1.

Tab. 4.1: STRIDE kategorie

	Kategorie hrozby	**Popis**
S	Spoofing	Neautorizované vydávání se za jiný subjekt.
T	Tampering	Neautorizovaná manipulace s daty nebo systémem.
R	Repudiation	Popření akce bez možnosti zpětného doložení odpovědnosti.
I	Information Disclosure	Neautorizované odhalení citlivých informací.
D	Denial of Service	Znepřístupnění služby nebo systému.
E	Elevation of Privilege	Získání vyšších práv, než jaká útočníkovi náleží.

Spoofing – Podvržení identity

Spoofing znamená, že se útočník vydává za jiný subjekt, obvykle za účelem obejití autentizace nebo získání přístupu do systému. V analýze pomocí STRIDE se tento typ hrozby identifikuje zejména u vstupních bodů systému, kde dochází k ověřování identity, typicky o autentizační služby, uživatelská rozhraní (HMI), nebo komunikační rozhraní IED zařízení. Rizikové jsou například nešifrované nebo nedostatečně chráněné přihlašovací kanály, chybějící kontrola integrity zdrojové adresy v síťových protokolech nebo slabé mechanismy autentizace zařízení.

Tampering – Neautorizovaná manipulace

Tampering označuje neautorizovanou změnu dat nebo konfigurace systému. V rámci analýzy se hodnotí rizika manipulace s daty na úrovni přenosu (např. změna GOOSE/MMS zprávy), uložených konfiguračních souborů nebo firmware zařízení. Typickým příznakem je absence kontroly integrity, např. chybějící hashování, podpisy nebo kryptografické ověření. Analytik by měl identifikovat všechny body, kde může být data možné změnit bez detekce, například jde o nezabezpečené přenosy mezi RTU a SCADA.

Repudiation – Popření akce

Repudiation znamená, že uživatel nebo proces může popřít, že provedl určitou akci, bez možnosti zpětného doložení. V analýze se zaměřujeme na existenci auditních záznamů, logovacích mechanismů a jejich integritu. Chybějící nebo snadno upravitelné logy představují významnou slabinu. Analytik sleduje, zda jsou akce zaznamenávány (např. přihlášení, odeslání příkazu), zda je možná korelace s časem a uživatelem, a zda logy nejsou uloženy pouze lokálně bez centrálního sběru.

Information Disclosure – Únik informací

Information Disclosure představuje hrozbu, kdy jsou citlivé informace zpřístupněny neoprávněným subjektům. V analýze se zaměřujeme na otevřená rozhraní, nedefinované přístupové politiky, nešifrovaný přenos dat a přebytečné informace ve výstupech systému. Konkrétní příklady zahrnují např. přenos hesel v prostém textu, diagnostické rozhraní přístupné zvenčí, nebo SCADA webové rozhraní bez autentizace. Hodnotí se i míra odhalení interní topologie systému.

Denial of Service – Odepření služby

Denial of Service (DoS) označuje stavy, kdy systém nebo služba přestane odpovídat v důsledku zahlcení nebo záměrné destabilizace. V rámci analýzy se sledují vstupní body systému (např. otevřené porty), chování při přetížení, a absence ochranných mechanismů jako jsou limitace připojení, timeouty nebo zpomalovací funkce. Typické scénáře zahrnují zahlcení GOOSE nebo MMS zprávami, opakované navazování spojení v IEC 104 nebo vyčerpání paměti v zařízení.

Elevation of Privilege – Zvýšení oprávnění

Elevation of Privilege nastává, když útočník získá vyšší úroveň přístupu, než by měl mít. Při analýze se identifikují body, kde lze eskalovat práva, např. špatně nastavené role, nedostatečně chráněné API, zranitelnosti v autentizačních mechanismech. Důležité je také ověřit, zda aplikace správně kontrolují oprávnění u každého požadavku. V prostředí IED může jít o získání přístupu k diagnostickým nebo konfiguračním funkcím, které by měly být vyhrazeny pouze pro správce.

4.3.2 MITRE ATT&CK

MITRE ATT&CK (Adversarial Tactics, Techniques, and Common Knowledge) je otevřená databáze zaměřená na klasifikaci reálných útoků a technik, které útočníci využívají k dosažení svých cílů v různých typech systémů. Databáze je založen na historických datech o útocích a poskytuje strukturovaný model, jakým způsobem dochází k provedení technik průniku.

Základním prvkem modelu jsou taktiky tedy fáze útoku, jako je počáteční přístup (Initial Access), laterální pohyb (Lateral Movement) nebo dopadu na systém (Impact). Ke každé taktice jsou přiřazeny konkrétní techniky neboli tedy metody, které útočníci v dané fázi používají. Tím vzniká vektor popisující celý útok. Existují varianty tohoto rámce pro různé typy prostředí, včetně ATT&CK for ICS[10], které specificky cílí na průmyslové a energetické systémy. Tabulka 4.2 zobrazuje příklady vybraných taktiky a odpovídající techniky podle rámce MITRE ATT&CK for ICS. Každý řádek představuje krok útočného řetězce, který může být uplatněn proti průmyslovým řídicím systémům (např. RTU, HMI, SCADA).

V rámci bezpečnostní analýzy se rámec MITRE ATT&CK používá ke strukturovanému mapování útoku na jednotlivé fáze a konkrétní techniky. Umožňuje analyzovat, které taktiky byly

[10] https://attack.mitre.org/matrices/ics/

využity, jakými technikami, a jaké byly vstupní vektory i cíle útoku. Jedním z klíčových přínosů je možnost propojení známých útoků s konkrétními technikami v ATT&CK matici, čímž lze vytvořit tzv. útokové vektory, které ukazují slabá místa v infrastruktuře. Například útok na PLC může využít sekvenci:

Initial Access (T0808) → **Execution** (T0853) → **Impair Process Control** (T0831),

kde takový řetězec je v prostředí SCADA/ICS systémů obzvláště nebezpečný, protože míří nejen na IT infrastrukturu, ale na samotný fyzický provoz elektrizační soustavy. Jednotlivé kroky jsou:

1. Initial Access (T0808): Útočník využije zranitelnosti ve veřejně přístupné webové aplikaci nebo portu (např. webové rozhraní PLC či RTU), čímž získá vstup do vnitřní sítě.
2. Execution (T0853): Následně spustí vlastní skript pro ovládnutí zařízení, sběr dat nebo další laterální pohyb.
3. Impact (T0831): Cílem útoku je narušení řízení procesů – například vypnutí jističů, přepsání parametrů ochrany nebo spuštění nebezpečné sekvence.

Tab. 4.2: Ukázka taktik a technik dle MITRE ATT&CK for ICS

Taktika	**Kód**	**Popis**
Initial Access	T0808	Zneužití veřejně přístupného rozhraní k průniku do systému.
Execution	T0853	Využití skriptů ke spuštění škodlivého kódu.
Impact	T0831	Narušení procesního řízení (např. vypnutí ochran, změna logiky).
Collection	T0851	Sběr procesních dat z řídicích zařízení (např. pomocí MMS nebo Modbus).
Command and Control	T0804	Navázání kanálu pro vzdálené ovládání kompromitovaného zařízení.
Persistence	T0886	Zajištění trvalého přístupu do systému (např. skrze upravené konfigurace).
Privilege Escalation	T0842	Získání vyšších oprávnění (např. z inženýrské stanice na root přístup).

4.3.3 STRIDE analýza komunikační infrastruktury

Pro systematické posouzení bezpečnostních rizik jednotlivých protokolů použitých v datové infrastruktuře elektrizační soustavy je v této části práce použita metodika STRIDE. Cílem této analýzy je identifikovat hrozby, kterým mohou být jednotlivé komponenty komunikační architektury vystaveny, a současně zhodnotit míru jejich mitigace pomocí existujících bezpečnostních standardů.

GOOSE

GOOSE protokol dle normy IEC 61850-8-1 slouží pro rychlou a deterministickou výměnu událostí v rámci staniční sítě, typicky mezi ochrannými relé a řídicími jednotkami (IED). Je postaven na multicastových ethernetových rámcích a v běžné praxi není šifrován ani autentizován, což jej činí náchylným k různým typům hrozeb, zejména pokud je útočník přítomen v lokální síti.

GOOSE komunikace je z hlediska STRIDE analýzy zranitelná zejména vůči hrozbám spoofingu, tamperingu a DoS, jak je zobrazeno v tabulce 4.3. Hlavní příčinou je absence kryptografické ochrany a důvěra v bezpečnost fyzické sítě, což neodpovídá aktuálním hrozbám v digitálních rozvodnách. Ačkoli IEC 62351-6 přináší určitou ochranu (např. MAC ověření a kontrolní otisky), implementace v praxi bývá omezená.

Tab. 4.3: STRIDE analýza protokolu GOOSE

	Popis zranitelnosti	**Příklad útoku**	**Pokrytí standardem**
S	GOOSE subscriber neověřuje zdrojovou MAC zpráv	MITM na GOOSE – falešný IED publikuje podvržené zprávy	IEC 62351-6 (HMAC)
T	Není zajištěna integrita dat, útočník může modifikovat zprávy	MITM: změna binární hodnoty při přenosu	IEC 62351-6 (HMAC)
R	Neexistuje záznam ani autentizace původu zpráv	Falešný alarm z podvržené zprávy	Není standardně řešeno
I	GOOSE není šifrovaný, lze jej volně odposlouchávat	Pasivní MITM – mapování stavu zařízení v síti	Není pokryto
D	DDoS GOOSE zpráv k zahlcení linky/ příjemců	DDoS GOOSE zpráv	Částečně: IEC 61850 doporučuje filtry
E	Neexistuje kontrola oprávnění pro publikaci GOOSE zpráv	Podvržené IED publikuje příkazy	Není pokryto

Sampled Values

Sampled Values jsou digitálně přenášená měření fyzikálních veličin (např. napětí, proud), typicky v podobě desítek až tisíců vzorků za sekundu. Jde o časově citlivou komunikaci v rámci staniční LAN, obvykle odesílanou Merging Unit (MU) směrem k IED, která provádějí ochranu nebo řízení. V základním nastavení SV nepoužívá šifrování, autentizaci ani integritu, což z něj činí kritickou zranitelnou složku. SV komunikace je z pohledu STRIDE, jak je zobrazeno v tabulce 4.4, považována za jednu z nejzranitelnějších složek rozvodny, protože:

- není běžně chráněna žádným kryptografickým mechanismem,
- běží ve vrstvě 2 bez možností kontroly nebo validace na úrovni aplikace,
- nese přímo informace, které ovlivňují ochrany, a jejich změna má okamžitý dopad na provoz.

Útoky jako vložení falešných SV rámců nebo pasivní sledování provozu jsou reálně proveditelné a zároveň obtížně detekovatelné, což z této vrstvy dělá ideální kandidát pro pokročilou bezpečnostní detekci a simulaci anomálií v testovacím prostředí.

MMS

MMS je protokol na úrovni aplikace, založený na ISO/OSI modelu a běžně transportovaný přes TCP/IP. Slouží k čtení/zápisu proměnných, řízení IED (např. „operate“ příkaz), přenosu konfigurací nebo registraci událostí. Na rozdíl od GOOSE/SV probíhá MMS typicky jako spojová komunikace, ale její defaultní verze postrádá šifrování i autentizaci (pokud není zavedeno IEC 62351).

Jak je zobrazeno v tabulce 4.5, zranitelnosti MMS plynou zejména z absence bezpečnostních opatření ve výchozím stavu, což jej činí náchylným vůči celé řadě STRIDE hrozeb od spoofingu a manipulace dat až po neoprávněné řízení. Na rozdíl od GOOSE nebo SV nabízí MMS díky vyšší vrstvě protokolu lepší možnosti pro zavedení šifrování, autentizace a role-based přístupu, zejména prostřednictvím IEC 62351-4 a IEC 62351-8.

Tab. 4.4: STRIDE analýza protokolu Sampled Values

	Popis zranitelnosti	**Příklad útoku**	**Pokrytí standardem**
S	SV rámce neobsahují kryptografickou identitu, MU lze napodobit	Vložení falešných SV dat z podvržené zařízení	IEC 62351-9 (volitelné, autentizační rámce)
T	Neexistuje integrita – útočník může upravit hodnoty napětí/proudu	MITM: změna měření, spuštění ochrany	IEC 62351-9 (MAC a časová razítka)
R	Žádná autentizace nebo podpis zpráv, nelze zpětně ověřit původ	Falešný výpadek proudu, chybné řízení	Není pokryto přímo
I	Všechny SV hodnoty jsou přenášeny otevřeně	Pasivní odposlech, profilování zátěže	Není pokryto
D	Možnost zahlcení sítě falešnými SV rámci nebo přerušením MU	Falešný MU generuje tisíce rámců / s	Nepřímo – návrh síťových filtrů
E	Každý uzel může vysílat SV, není kontrola oprávnění	Podvržené MU se vydává za legitimní	Není pokryto

Tab. 4.5: STRIDE analýza protokolu MMS

	Popis zranitelnosti	**Příklad útoku**	**Pokrytí standardem**
S	MMS běží přes TCP/IP, bez zabezpečení je možný IP spoofing klienta	Phishing → získání přístupu → falešné příkazy do IED	IEC 62351-4 (TLS)
T	MMS zprávy lze na úrovni sítě nebo aplikačně upravit	MITM: změna hodnot při přenosu (např. operace)	IEC 62351-4 (TLS)
R	Bez autentizace a logování nelze dokázat, kdo provedl příkaz	Útočník provede „operate“ bez záznamu identity	IEC 62351-4 umožňuje identifikaci a logování
I	Čtení hodnot bez šifrování, lze sledovat stav IED, konfiguraci	Pasivní odposlech MMS: struktura proměnných, přenášená data	IEC 62351-4 (TLS)
D	Opakované „operate“ nebo „select“ požadavky mohou přetížit IED	DDoS nebo flooding příkazů	Nepřímo pokryto (rate-limit, timeouty)
E	Bez řízení přístupů může jakýkoli klient volat operace	Phishing → eskalace práv → operate	IEC 62351-8 (Role-Based Access Control)

IEC 60870-5-104

IEC 104 je protokol pro telemetrii a telecontrol, přestože běží nad TCP, postrádá bezpečnostní mechanismy jako je šifrování, autentizaci nebo kontrolu integrity. Tím se stává velmi zranitelným vůči útokům na otevřených nebo nechráněných spojeních.

IEC 104 představuje kritické rozhraní mezi SCADA a vzdálenými prvky, které v řadě instalací stále běží bez jakékoliv ochrany. Jak je uvedeno v tabulce 4.6, STRIDE hrozby jsou reálně proveditelné a byly také využity nebo simulovány v rámci útoků jako Industroyer (2016), kde útočníci generovali validní IEC 104 rámce pro ovládání výstupních prvků. I když IEC 62351-5 přináší pokročilé bezpečnostní mechanismy (TLS, autentizace handshake, podpisy ASDU), jejich použití v praxi je stále poměrně málo využívané.

Tab. 4.6: STRIDE analýza protokolu IEC 104

	Popis zranitelnosti	**Příklad útoku**	**Pokrytí standardem**
S	Neexistuje autentizace klienta	Exploit na IEC 104 GW: falešné spojení klienta	IEC 62351-5 definuje autentizaci handshake
T	Bez integrity – možné upravit / vytvořit falešné ASDU	MITM nebo exploit → manipulace s binárním stavem	IEC 62351-5 (digitální podpisy ASDU)
R	Žádné podpisy / logy nezajišťují audit, kdo vydal příkaz	Operátor odešle příkaz, který nelze zpětně dohledat	IEC 62351-5 (možné logování a podpisy)
I	Nešifrovaný TCP → viditelnost provozu včetně hodnot, adres, příkazů	Odposlech telemetrie – stav přepínačů, analogové hodnoty	IEC 62351-5 (TLS/IPSec doporučeno)
D	Flooding IEC 104 spojení nebo opakované požadavky mohou přetížit GW/RTU	zahlcení IEC 104 brány upravenými ASDU	IEC 62351-5 doporučuje rate-limiting
E	Chybí řízení oprávnění – jakýkoliv připojený klient může řídit zařízení	Phishing → získání SCADA přístupu → příkaz „operate“	IEC 62351-8 (RBAC pro IEC 104 – nepovinné)

4.3.4 STRIDE analýza zařízení v energetice

Vedle protokolové vrstvy jsou důležité v datové infrastruktuře energetických systémů i samotná zařízení, které zajišťují sběr, zpracování a přenos informací. Každý z těchto prvků představuje potenciální bod selhání nebo vstupní vektor pro útočníka, a to jak na úrovni kybernetické, tak fyzické. Stejně jako v předchozí analýze je i zde cílem identifikovat hrozby a jejich pokrytí standardem.

SCADA

SCADA server je centrálním uzlem sběru a zobrazení dat, odesílání příkazů do systému, historizace a alarmového řízení. V mnoha prostředích funguje také jako komunikační most mezi IT a OT. Často je přístupný přes VPN, RDP[11] nebo přímé webové rozhraní, zároveň propojený s vnitřní sítí. Jeho narušení může vést jak k přímému řízení systému útočníkem, tak k narušení monitoringu a falešnému stavu systému.

[11] Remote Desktop Protocol, protokol pro vzdálené ovládání.

Tabulka 4.7 ukazuje, že SCADA server je ohrožen napříč všemi kategoriemi STRIDE. Nejvýznamnějšími slabinami jsou slabá autentizace a nedostatečné oddělení rolí, které umožňují zneužití identity a eskalaci oprávnění. Rizikem je i manipulace s daty, absence auditních záznamů a nedostatečné šifrování, jež mohou vést k falešnému obrazu systému či úniku citlivých informací. Kritické je také přetížení serveru útoky typu DDoS, které ohrožují dostupnost řízení.

Tab. 4.7: STRIDE analýza prvku SCADA

	Popis zranitelnosti	**Příklad útoku**	**Pokrytí standardem**
S	Slabá autentizace (např. RDP, VPN) umožňuje přístup pod cizí identitou	Phishing – získání přístupu k dispečerské stanici	IEC 62443-3-3 (IAM), NIST 800-82
T	Útočník mění záznamy, hodnoty nebo konfigurační soubory v systému	Phishing → zápis změněných alarmových hodnot	IEC 62443-3-3, RBAC
R	Absence auditních záznamů → nelze určit, kdo provedl operaci	Změna konfigurace bez logu	IEC 62443-3-3 (event logging)
I	Přístup k databázi nebo RAM SCADA umožní čtení struktury systému	Odposlech databázových dotazů, přístup ke schématům	IEC 62443-3-3, TLS/IPSec
D	SCADA server je přetížen např. dotazy, alarmy, chybami	DDoS útok na perimetr (SCADA HMI/API)	IEC 62443-3-3 (resilience), NIST CSF
E	Útočník z běžného účtu získá oprávnění admina systému	Phishing → eskalace na správce → trvalý přístup	IEC 62443-3-3 (least privilege, role separation)

IEC 104 Gateway

IEC 104 gateway zajišťuje překlad mezi vnitřními sítí (např. MMS) a dálkovým přístupem přes IEC 60870-5-104, typicky směrem ke SCADA nebo dispečerským systémům. Nachází se často na perimetru mezi vnitřní a vnější sítí, čímž se stává klíčovým bodem přenosu i bezpečnostní mezí. Gateway představuje hranici mezi SCADA systémem a provozní sítí a právě tento mezistupeň je často opomíjen v bezpečnostních návrzích. Přitom obsahuje kritickou logiku mapování signálů, převody mezi protokoly a směrování příkazů a jakákoliv manipulace nebo výpadek může znamenat narušení řízení celého systému.

Tabulka 4.8 ukazuje, že gateway je kritickým bodem, kde se setkávají vnitřní a vnější sítě. Největší rizika představuje absence ověřování zdroje zpráv a možnost podvržení či manipulace s ASDU, což může vést k přímému narušení logiky řízení. Nešifrovaná komunikace zároveň odhaluje síťovou topologii a hodnoty, zatímco chybějící logy ztěžují zpětnou forenzní analýzu. Významné je i riziko zahlcení gateway nebo zneužití administračního rozhraní bez dostatečného řízení rolí. Přestože IEC 62351-5 a IEC 62443 definují odpovídající ochrany, jejich implementace je v praxi často nedostatečná.

Tab. 4.8: STRIDE analýza prvku IEC 104 gateway

	Popis zranitelnosti	**Příklad útoku**	**Pokrytí standardem**
S	Gateway nedokáže ověřit identitu zdroje IEC 104 zpráv	Exploit na IEC 104 gateway – falešné klientské spojení	IEC 62351-5 (autentizace handshake)
T	Nevalidované zprávy mohou být upraveny nebo podvrženy	Vložení upravených ASDU → změna logiky řízení	IEC 62351-5 (digitální podpisy)
R	Chybí auditní mechanismy k dohledání původu zprávy	Chybějící logy po zneužití spojení	IEC 62351-5, IEC 62443-3-3
I	Nešifrované zprávy odhalují síťovou topologii a hodnoty	Odposlech ASDU mezi SCADA a RTU	IEC 62351-5 (TLS/IPSec)
D	Možné zahlcení parseru nebo TCP spojení (DoS)	syntakticky validní, ale zahlcující zprávy	IEC 62351-5 doporučuje řízení přístupu a throttling
E	Gateway často obsahuje administrační rozhraní bez RBAC	Phishing → přístup k konfiguraci, změna mapování	IEC 62443-3-3 (role-based přístup, hardening)

RTU

RTU slouží jako vzdálený bod komunikace mezi SCADA systémem a provozními zařízeními (např. senzory, ovladače, stykače). Bývá nasazena v místech bez trvalého personálu, často s připojením přes mobilní nebo LAN sítě. Na rozdíl od IED typicky neobsahuje logiku ochrany, ale je důležitá pro přenos informací a výkonných příkazů – její kompromitace může vést k falešným alarmům, manipulaci s měřením nebo přerušení SCADA přehledu.

Tabulka 4.9 ukazuje, že RTU je zranitelné zejména kvůli absenci ověřování a šifrování, což umožňuje podvržení jednotky, manipulaci s daty i odposlech komunikace. Nedostatek auditních logů ztěžuje forenzní analýzu a omezuje dohled nad vykonanými příkazy. Kritické je i riziko přetížení spojení, které může vyřadit telemetrii a omezit dohled SCADA. Bezpečnostní standardy sice nabízejí opatření, jejich implementace v praxi však často chybí.

IED

IED (např. ochranná zařízení) je základní stavební blok moderní rozvodny, který integruje funkce měření, ochrany a řízení v jednom zařízení. Komunikuje pomocí MMS, GOOSE a SV a často přímo ovládá výkonové prvky (např. vypínače, signalizace). IED je typickým příkladem kyber-fyzického prvku, jehož kompromitace má okamžitý dopad na fyzikální stav systému. Ačkoliv samotné protokoly (GOOSE, MMS) už byly zkoumány v předchozí části, zde se STRIDE zaměřuje přímo na vnitřní logiku zařízení, jeho konfiguraci a autentizaci.

Tabulka 4.10 ukazuje, že IED patří mezi nejkritičtější prvky, protože jejich kompromitace má okamžitý dopad na fyzický stav sítě. Nejvýznamnějšími hrozbami jsou podvržení příkazů přes GOOSE/MMS, manipulace logiky ochrany a absence auditních záznamů, které znemožňují zpětnou kontrolu. Neautorizovaný přístup k parametrům nebo DoS útok mohou vyřadit ochranné funkce a ohrozit stabilitu celé soustavy. i když normy IEC 62351 a IEC 62443 definují autentizaci, RBAC či integritu softwaru, jejich implementace bývá v praxi nedostatečná.

Tab. 4.9: STRIDE analýza prvku RTU

	Popis zranitelnosti	**Příklad útoku**	**Pokrytí standardem**
S	SCADA může komunikovat s podvrženou RTU (neověřená IP)	Phishing → přístup k SCADA → změna adresy RTU	IEC 62351-5 (autentizace spojení)
T	Útočník může upravit stavové nebo analogové hodnoty před přenosem	Změna stavových hodnot před SCADA (MITM)	IEC 62351-5 (ASDU podpisy)
R	RTU nevede auditní logy o příkazech a odpovědích	Ztráta záznamu o vykonaném příkazu SCADA	IEC 62443-3-3 (auditní záznamy, syslog)
I	Nešifrované spojení – únik hodnot a topologie	Odposlech komunikace RTU–SCADA (IEC 104)	IEC 62351-5 (TLS/IPSec)
D	Přetížení RTU spojení → ztráta telemetrie a kontroly	Flooding přes IEC 104	IEC 62351-5 doporučuje throttling
E	Přístup ke konfiguraci často bez segmentace nebo RBAC	Phishing → přístup k routeru → změna konfigurace	IEC 62443-4-2 (role-based řízení přístupu)

Tab. 4.10: STRIDE analýza prvku IED

	Popis zranitelnosti	**Příklad útoku**	**Pokrytí standardem**
S	IED často důvěřuje příkazům z neověřených zdrojů (např. GOOSE, MMS)	MITM na GOOSE – falešný IED vydává příkaz	IEC 62351-6 (MAC pro GOOSE), -8 (RBAC)
T	Možnost změny logiky zařízení nebo parametrů ochrany	Manipulace logiky ochrany přes inženýrský přístup	IEC 62443-4-2 (software integrity), 61850 SCL kontrola
R	Bez auditních logů nelze zjistit, kdo změnil konfiguraci	Chybějící záznam o zásahu inženýra	IEC 62443-3-3 (audit), 62351-7 (syslog)
I	Neautorizovaný přístup k parametrům IED nebo hodnotám	Pasivní sledování GOOSE/MMS mezi IED a SCADA	IEC 62351-6/-4 (šifrování, role-based přístup)
D	DoS na IED může vést ke ztrátě ochrany / signalizace	Falešné GOOSE zprávy zahlcující vstupy	IEC 62443-3-3 (resilience), switch-based ochrana
E	Přístup k IED není řízen granularitou → možnost změn logiky	přístup přes servisní port nebo LAN → admin přístup	IEC 62351-8 (RBAC), hardening, fyzická ochrana

Inženýrská stanice

Inženýrská stanice je zařízení používané pro konfiguraci a parametrizaci IED, správu logiky ochran (např. prostřednictvím SCL souborů), firmware update, ladění a síťovou diagnostiku. Bývá připojena přímo k síti (LAN), případně na přechodovém bodě s IT infrastrukturou. Z hlediska útočníka jde o vysoce atraktivní cíl, protože kompromitace znamená přímý přístup ke konfiguraci a chování celého systému.

Tabulka 4.11 potvrzuje, že inženýrská stanice představuje pro útočníka mimořádně atraktivní cíl. Klíčovými hrozbami jsou neautorizovaný přístup přes vzdálená rozhraní, manipulace s konfigurací či firmwarem a únik citlivých SCL souborů obsahujících topologii i přihlašovací údaje. Rizikem je také absence detailního logování a možnost zneužití lokálních účtů bez omezených rolí. Kompromitace stanice má přímý dopad na celý systém, a proto je nutné důsledně aplikovat opatření dle IEC 62443 a IEC 62351, přesto jejich zavedení v praxi často chybí.

Tab. 4.11: STRIDE analýza prvku Inženýrská stanice

	Popis zranitelnosti	**Příklad útoku**	**Pokrytí standardem**
S	Neautorizovaný uživatel získá přístup např. přes RDP, VPN nebo USB	Phishing → přístup ke stanici	IEC 62443-3-3 (IAM, login policy)
T	Úprava konfigurace ochrany, firmware nebo síťové topologie	změna logiky v IED pomocí inženýrské stanice	IEC 62443-4-2 (integrita SW, firmware podpisy)
R	Nedostatečné logování činností – nelze zjistit, kdo provedl změnu	Změna SCL bez logu / rollback konfigurace	IEC 62351-7, 62443-3-3 (logování změn)
I	Nechráněné konfigurační soubory (např. .cid/.scd) obsahují topologii a přístupová hesla	Únik SCL → analýza síťových vazeb, hesla v plaintextu	IEC 62351-8, 62443-3-3
D	Inženýrská stanice zasažen malwarem, šifrováním (např. ransomware), nemožnost zásahu	Ztráta přístupu k systému, nutnost fyzického zásahu	IEC 62443-3-3 (backup, oddělení inženýrské stanice od sítě)
E	Lokální účet s plnými právy bez řízení přístupů, chybí víceúrovňové oprávnění	z běžného účtu změna celé konfigurace rozvodny	IEC 62443-4-2 (RBAC, separation of duties)

Slučovací jednotka

Slučovací jednotka je zařízení sloužící k sběru analogových měření (napětí, proud) z transformátorů a jejich převodu do digitální podoby Sampled Values v souladu s IEC 61850-9-2. MU je považována za první digitální bod ochranného řetězce, a tedy kritický pro správné rozhodování IED. Vzhledem ke své blízkosti k fyzikálním hodnotám a zároveň exponovanosti v síti LAN je vhodná pro STRIDE analýzu. Z hlediska STRIDE se zde jasně uplatňuje hrozba spoofingu, tamperingu a DoS, často obtížně detekovatelná, protože SV rámce jsou vysílány multicastově bez odpovědi.

Tabulka 4.12 ukazuje, že slučovací jednotka je kritickým bodem ochranného řetězce, kde kompromitace přímo ovlivňuje vstupní měření pro IED. Největší hrozbou je spoofing falešných SV

rámců a manipulace s kalibrací či konfigurací, což může vést k nesprávným hodnotám napětí nebo proudu. Závažné je i riziko odposlechu reálných měření a zneužití servisního přístupu bez RBAC. Útoky DoS mohou vyřadit přenos SV a ohrozit funkci ochran. Přestože normy IEC 62351 aIEC 62443 definují autentizaci, integritu i auditní mechanizmy, jejich praktické nasazení v prostředí MU zůstává omezené.

Tab. 4.12: STRIDE analýza prvku Slučovací jednotka

	Popis zranitelnosti	**Příklad útoku**	**Pokrytí standardem**
S	Útočník vydává zařízení za MU a publikuje SV datové rámce	falešné SV hodnoty z podvrženého MU	IEC 62351-9 (MAC a identita zdroje SV)
T	Změna logiky vzorkování, výpočtu, nastavení převodníku	Změna kalibračního koeficientu → chybné napětí	IEC 62443-4-2 (integrita konfigurace)
R	Není auditní záznam, kdo provedl změnu konfigurace	Neznámý operátor změní měřicí rozsah	IEC 62351-7 (audit), 62443-3-3
I	SV přenosy lze pasivně odposlouchávat – obsahují reálné hodnoty	Pasivní MITM → sledování odběrů a zátěže	IEC 62351-9 (šifrování rámců – zatím málo používané)
D	MU zahlcena dotazy, přerušen přenos SV, ztráta měření	DoS: MU nepublikuje SV → IED přechází do ochrany	IEC 62443-3-3 (detekce anomálií, watchdog)
E	Přístup k MU bez RBAC → možnost změnit datové mapování, rozsah	Útočník přes servisní port mění nastavení převodníků	IEC 62443-4-2 (RBAC, policy enforcement)

Shrnutí

Na základě STRIDE analýzy byly identifikovány konkrétní hrozby, které se vztahují k jednotlivým komunikačním vrstvám a systémovým komponentám digitální rozvodny. Tyto hrozby byly porovnány s bezpečnostními požadavky definovanými v příslušných standardech (zejména řadách IEC 62351, IEC 62443 a dílčích rámcích NIST), přičemž bylo vyhodnoceno, zda a do jaké míry jsou jimi řešeny. Takto byla provedena gap analýza, jejímž cílem bylo identifikovat otevřené nedostatky, které nejsou pokryty, jsou pokryty pouze částečně, nebo nejsou v praxi standardně implementovány. Zjednodušený souhrný přehled identifikovaných hrozeb a jejich pokrytí bezpečnostními standardy je uveden v tabulce 4.13.

Bylo zjištěno, že protokoly GOOSE, SV, MMS a IEC 104 vykazují ve výchozím stavu významné bezpečnostní mezery. Ačkoliv jsou v rámci standardů IEC 62351 definována opatření jako je šifrování, autentizace, digitální podpisy nebo zabezpečení přístupu, ve většině případů nebývají tato opatření aktivně nasazována. Tuto skutečnost potvrzují autoři v článku [158], kteří uvádějí, že bezpečnostní mechanismy doporučené v normě IEC 62351 nejsou v průmyslových systémech běžně implementovány, a to zejména kvůli požadavkům na zpětnou kompatibilitu, výkon nebo omezené podpoře ze strany dodavatelů. V dalším článku [205] autoři upozorňují, že zprávy GOOSE a SV jsou v praxi často přenášeny nešifrovaně a bez kontroly integrity, čímž zůstávají otevřené útokům i přes existenci definovaných bezpečnostních funkcí. Ve článku [198] autoři doplňují, že volitelné bezpečnostní části standardu IEC 62351 nejsou implementovány ve většině běžných implementací

protokolů jako je MMS nebo IEC 104, což významně snižuje jejich odolnost vůči reálným útokům. Autoři v článku [89] potvrzují, že Merging Units i IED často postrádají mechanismus pro ověřování integrity SV zpráv, kde v testech bez použití MAC (Message Authentication Code) byly injekční útoky úspěšné a došlo k otevřenému narušení fyzických ochranných mechanismů.

SCADA servery, gatewaye, IED, RTU a MU mají rozdílnou úroveň zranitelnosti a konstrukční složitosti, což ovlivňuje jejich odolnost vůči kybernetickým útokům. U SCADA serveru a inženýrské stanice byly identifikovány nedostatky zejména v oblasti řízení přístupu (absence víceúrovňového oprávnění), slabého logování činností a vysoké náchylnosti na útoky typu phishing nebo neoprávněný vzdálený přístup. Toto zdůrazňuje přehledový článek [202], kde autoři poukazují na rostoucí zranitelnost moderních SCADA systémů v důsledku jejich připojení k internetu a nedostatečného zabezpečení architektury.

Gateway a RTU, umístěné obvykle na rozhraní OT/IT sítí, bývají ohroženy síťovými útoky v důsledku nedostatečné autentizace klientů a slabé ochrany protokolové logiky. Této zranitelnosti se věnuje studie [84], která upozorňuje na nedostatek RBAC mechanismů a potřebu silnější autentizace a integrity zpráv.

U zařízení typu IED a MU byly zaznamenány výrazné nedostatky v oblasti řízení logiky a integrity měřených dat. Bylo zjištěno, že přístup ke konfiguraci je ve většině případů málo omezený, neauditovaný a důvěřuje lokální síti. Komponenty často nedisponují rolově řízeným přístupem (RBAC), ani systémem validace změn či redundantní verifikace hodnot. Přitom jde o prvky s přímým dopadem na ochranné funkce systému. Autoři v článku [89] zjistili, že konfigurace IED bývá ve většině případů málo omezená, bez robustních RBAC mechanismů a bez auditních stop, přičemž systém implicitně důvěřuje lokální síti. Dále zjistili, že při simulaci útoků na IED se standardem IEC 61850 je možné injektovat podrvržená data, což vede k přímému ovlivnění ochranných funkcí elektrických obvodů.

Tab. 4.13: Souhrnná STRIDE analýza protokolů a prvků v energetice

Komponenta	**Zabezpečení ve standardech**	**Identifikované mezery**
GOOSE	IEC 62351-6 (hash, MAC), segmentace, IEC 61850 doporučení	Absence šifrování, běžně neimplementováno; bez autentizace vysílače; zranitelnost vůči MITM a replay
Sampled Values	IEC 62351-9 (nepovinná autentizace), segmentace	Reálná nasazení neobsahují integritu, identitu zdroje; vysoká zranitelnost vůči spoofingu a DoS
MMS	IEC 62351-4 (TLS), -8 (RBAC), podporováno, ale často vypnuto	Absence logování akcí, TLS není v praxi zaveden, přístupové politiky často pouze formální
IEC 104	IEC 62351-5 (TLS, handshake, podpisy), často nepoužito	Významné riziko MITM a spoofingu, útoky typu replay běžně možné, minimum nasazení bezpečnostních prvků
SCADA server	IEC 62443-3-3 (RBAC, audit), NIST 800-82	V praxi často slabé hesla, nedostatečné logování, náchylnost na phishing a RDP přístup
IEC 104 Gateway	IEC 62351-5, 62443-3-3	Slabá validace zpráv, chybějící autentizace klienta, nedostatečná auditovatelnost
IED	IEC 62351-6/-4/-8, 62443-4-2	Chybějící RBAC, otevřený přístup k logice, náchylnost na GOOSE spoofing a přímou manipulaci
RTU	IEC 62351-5, 62443-3-3	Slabé zabezpečení na WAN vrstvě, náchylné na spoofing, málo auditních funkcí, otevřené porty
Inženýrská stanice	IEC 62443-3-3, -4-2	Chybějící segmentace, hesla v plaintextu (v SCL), žádné šifrování dat, vysoké riziko zneužití lokálního přístupu
Slučovací jednotka	IEC 62351-9, 62443-4-2	Minimální bezpečnostní funkce, žádné šifrování SV, žádné logování, zranitelnost vůči spoofingu

4.3.5 MITRE ATT&CK

Na základě předchozí STRIDE analýzy byla provedena mapování jednotlivých kategorií hrozeb na relevantní útočné techniky definované v rámci MITRE ATT&CK for ICS. Cílem tohoto kroku bylo ověřit, které z identifikovaných typových hrozeb odpovídají známým a formálně popsaným útočným scénářům, a tím vytvořit základ pro návrh validovatelných bezpečnostních scénářů v experimentálním prostředí.

U každé komponenty digitální rozvodny, která byla předmětem analýzy (např. GOOSE, SV, MMS, IED, SCADA, MU aj.), byly posouzeny jednotlivé STRIDE hrozby z pohledu dostupnosti odpovídající MITRE techniky. Všechny výsledné tabulky jsou uvedeny příloze A. Zjednodušená souhrnná tabulka 4.14 udává přehled MITRE ATT&CK technik mapovaných na STRIDE analýzu pro jednotlivé prvky elektrizační soustavy.

Z výsledků analýzy vyplynulo, že techniky jako Masquerading (T0853), Unauthorized Command Message (T0851), Sniffing Network Traffic (T0842), Denial of Control (T0804) a Valid Accounts (T0886) se opakovaně objevují napříč celým prostředím a reprezentují reálně proveditelné útoky se závažnými důsledky pro bezpečnost systému.

Zejména protokoly GOOSE a SV byly identifikovány jako vysoce zranitelné vůči útokům typu spoofing (T0854) a manipulace s daty (T0855), přičemž tyto techniky umožňují změnit chování ochran bez fyzického zásahu do zařízení. Zařízení jako IED a RTU jsou náchylná k útokům na ovládací logiku nebo ověření příkazů (T0851), zatímco přístup k SCADA serveru nebo inženýrské stanici umožňuje provádět příkazy na celém systému při zneužití platných přístupových údajů (T0886).

Naopak u některých STRIDE kategorií, zejména repudiace (R), nebyla v rámci ATT&CK for ICS nalezena odpovídající technika. Tyto případy poukazují na přetrvávající nedostatky v oblasti auditu a forenzní dohledatelnosti, které nejsou explicitně modelovány v současném stavu znalostí frameworku MITRE.

Tab. 4.14: Přehledová tabulka STRIDE a MITRE ATT&C

Prvek	**S**	**T**	**R**	**I**	**D**	**E**
GOOSE	T0854	T0858	—	T0842	T0804	—
SV	T0854	T0855	—	T0842	T0804	—
MMS	T0853	T0851	—	T0842	T0804	T0886
IEC 104	T0853	T0851	—	T0842	T0804	T0886
SCADA Server	T0853	T0851	—	T0842	T0804	T0886
IEC 104 Gateway	T0853	T0851	—	T0842	T0804	T0886
RTU	T0853	T0851	—	T0842	T0804	T0886
IED	T0853	T0851	—	T0842	T0804	T0886
Merging Unit (MU)	T0854	T0855	—	T0842	T0804	T0886
Inženýrská stanice	T0853	T0850	—	T0802	T0859	T0886

5 Návrh architektury výzkumného prostředí pro kybernetickou bezpečnost elektroenergetiky

5.1 Požadavky na architekturu testovacího prostředí

V předchozích kapitolách byla provedena analýza technologických řešení využívaných v prostředí kyber-fyzických systémů energetické infrastruktury a byla provedena formální riziková analýza zranitelností, které se v těchto systémech vyskytují. Na základě těchto poznatků je v této kapitole navržen koncept sandbox architektury, která slouží jako výzkumná a experimentální platforma pro testování bezpečnostních scénářů, hodnocení odolnosti, a ověřování mitigačních opatření v realistickém prostředí. Jedná se o systematicky vytvořený rámec, jehož cílem je umožnit simulaci reálných vektorů útoků, provoz vybraných prvků elektrizační soustavy a vyhodnocení dopadů bezpečnostních incidentů na komunikační a řídicí vrstvy systému.

Při návrhu této architektury je kladen důraz na interoperabilitu, škálovatelnost, realističnost a modularitu. Architektura je navržena tak, aby bylo možné její nasazení jak ve fyzickém, tak i ve virtualizovaném prostředí, což umožňuje adaptabilní využití v různých scénářích.

V následujících podkapitolách bude tato architektura podrobně rozebrána z hlediska návrhových principů, komponentního složení, mapování na SGAM model, modelování datových toků a identifikace zranitelných míst.

5.1.1 Požadavky

Architektura testovacího prostředí musí být koncipována jako otevřený a modulární rámec, který bude umožňovat simulaci různých scénářů, snadnou rozšiřitelnost a vysokou míru přizpůsobení.

Interoperabilita Architektura musí zajišťovat interoperabilitu mezi různorodými komunikačními protokoly, zařízeními a standardy. Musí umožňovat integraci zařízení a systémů podporujících odlišné protokoly, například současné použití IEC 61850 a IEC 60870-5-104 prostřednictvím komunikačních bran. Musí být zajištěna schopnost překladu a propojení těchto systémů pro reálné modelování hybridního prostředí typického pro moderní distribuční soustavy.

Škálovatelnost Architektura musí být navržena tak, aby ji bylo možné provozovat v různých měřítkách od malého virtuálního testbedu až po rozsáhlé fyzické nasazení s reálnými zařízeními. Oddělení řídicích, komunikačních a periferních vrstev musí umožňovat nezávislé rozšiřování jednotlivých částí bez zásahu do celkového návrhu.

Realističnost Modelované scénáře, zařízení a síťová struktura musí odpovídat běžné praxi v oblasti automatizace a řízení elektrizační soustavy. Musí být zahrnuty typické prvky, jako jsou PLC, RTU, HMI, gateway, SCADA a přidružené komunikační komponenty. Vzhledem k tomu, že některé kybernetické útoky cílí na specifické protokoly nebo konfigurace, musí architektura umožňovat realistický a detailní popis jednotlivých komponent a jejich interakcí.

Modularita Každý prvek architektury musí být navržen jako samostatná jednotka, kterou lze použít podle daného scénáře. Musí být možné definovat různé typy scénářů – například s výpadkem komponenty, s cíleným útokem na konkrétní rozhraní, nebo se změnou parametrů v síťovém provozu. Modulární přístup musí zároveň usnadňovat opakované použití architektury pro různé výzkumné účely a validace.

5.1.2 Komponenty testovacího prostředí

Výběr a struktura těchto komponent přímo vychází z analytických závěrů předchozích kapitol, kde byly na základě technologické analýz identifikovány klíčové prvky, procesy a komunikační toky relevantní pro distribuovanou elektroenergetickou infrastrukturu.

Struktura architektury respektuje model SGAM, jehož komponentová a zónová vrstva poskytují rámec pro systematické rozdělení zařízení, jejich funkcí a jejich interakcí. Komponenty sandboxu tak reflektují jednotlivé vrstvy a zóny SGAM, přičemž pokrývají jak prvky fyzické infrastruktury (např. RTU, IED), tak řídicí a komunikační technologie (např. SCADA, HMI, gateway).

Cílem návrhu bylo vytvořit realistické a flexibilní prostředí, které umožňuje modelování běžného provozu distribuované energetické sítě i simulaci bezpečnostních incidentů. Zvolená modularita architektury zároveň umožňuje přizpůsobení konkrétním výzkumným scénářům a škálování prostředí podle požadavků experimentální části práce.

- **RTU:** Zajišťují vzdálený sběr dat a přenos řídicích instrukcí mezi koncovými zařízeními a SCADA systémem. Často využívají protokol IEC 60870-5-104.
- **IED:** Zařízení s pokročilou ochranou, řízením a měřicími funkcemi, typicky napojená na komunikační sběrnice dle standardu IEC 61850. Podporují zprávy typu GOOSE, SV i datové služby přes MMS.
- **SCADA:** Slouží pro centrální monitoring, sběr dat a řízení technologických procesů. Umožňuje interakci s operátory a správu událostí v síti.
- **HMI:** Uživatelské rozhraní umožňující vizualizaci stavu systému, ovládání technologických procesů a zadávání příkazů v rámci řízení.
- **Přepínače/směrovače infrastruktura:** Zajišťuje směrování a přepínání dat v rámci sítě, segmentaci jednotlivých částí infrastruktury a implementaci základních bezpečnostních pravidel (např. VLAN, ACL[1]).
- **Gateway:** Slouží k překladu mezi různými komunikačními protokoly (např. IEC 60870-5-104 a IEC 61850) a zajišťuje propojení heterogenních částí sítě.
- **Synchronizační systémy:** Používají se pro zajištění časové přesnosti v prostředí, kde je vyžadována vysoká časová synchronizace (například u GOOSE nebo SV zpráv). Typicky využívají protokoly NTP nebo PTP, jejich nasazení závisí na konkrétním scénáři experimentu.
- **Uživatelské stanice (operátorské/inženýrské/přístupové):** Univerzální počítače připojené do infrastruktury, které slouží k ovládání, správě, konfiguraci i vzdálenému přístupu. Stejné stanice mohou být využity legitimními uživateli (operátor, technik) nebo mohou v experimentálních scénářích reprezentovat útočníka. Funkčně neplní specializovanou roli v řízení infrastruktury, ale tvoří klíčový vstupní bod do systému.

5.1.3 Topologie sandbox architektury

Topologický návrh sandbox architektury vychází ze struktury SGAM, který poskytuje standardizovaný rámec pro systematické členění chytrých energetických sítí z hlediska technologií, komunikace a řízení. Architektura byla navržena tak, aby odpovídala zónám od Procesu po Provoz v souladu s principy SGAM. Cílem návrhu bylo vytvořit realistickou, modulární a bezpečnostně relevantní strukturu, která umožní testování komunikačních vazeb, řízení technologických procesů a simulaci kybernetických útoků. V tabulce 5.1 je uvedeno mapování prvků infrastruktury na SGAM model.

[1] Access Control List, seznam řízení přístupu

Tab. 5.1: Mapování prvků infrastruktury na SGAM model

SGAM zóna	Funkce v rámci architektury	Příklady komponent
Proces	Interakce se senzory a akčními členy	IED (ochrana, řízení), senzory, akční členy
Pole	Přenos měřených a řídicích dat	RTU, GOOSE, SV komunikace
Stanice	Lokální sběr a řízení dat, lidská obsluha	SCADA, HMI, gateway
Provoz	Management, vzdálený přístup, inženýrské stanice	Uživatelské stanice připojené k infrastruktuře
Podnik, Trh	Nejsou součástí sandbox architektury	—

Procesní zóna

Procesní zóna představuje nejnižší vrstvu návrhu sandbox architektury, kde dochází k přímé interakci s fyzickým nebo simulovaným technologickým procesem. Tato zóna je v reálných distribučních soustavách tvořena zařízeními a technologiemi, které přímo ovlivňují stav elektrické sítě, a proto je její správné navržení a zabezpečení klíčové i v rámci výzkumné infrastruktury.

V návrhu sandbox architektury je Procesní zóna implementována jako izolovaný segment, který umožňuje realistickou simulaci vstupů a výstupů technologického procesu, a zároveň poskytuje dostatečnou flexibilitu pro testování různých scénářů řízení, poruchových stavů i kybernetických útoků.

Navržené komponenty a jejich role

- Senzory a akční členy: Ve skutečné infrastruktuře by šlo o proudové a napěťové transformátory, spínače, jističe apod. V návrhu sandboxu budou tyto prvky nahrazeny simulovanými vstupy a výstupy, které budou umožňovat modelování reálných provozních stavů a reakcí systému. Jejich řízení a odezvy budou řízeny z IED.
- IED/MU: Slouží jako hlavní řídicí a ochranné prvky této vrstvy. V návrhu sandboxu budou zajišťovat simulovanou ochranu a řízení technologického procesu včetně zpracování vstupních signálů a generování řídicích výstupů. Součástí návrhu je využití standardu IEC 61850, což umožní realistickou výměnu dat prostřednictvím zpráv typu GOOSE a SV.

Vstupy a výstupy zóny

- Vstupy:
  - Simulovaná měření (hodnoty napětí, proudu, stavové signály),
  - Konfigurační data z vyšších vrstev (Staniční zóna),
  - Příkazy k řízení technologického procesu (vypínání, zapínání).
- Výstupy:
  - Řídicí signály pro akční členy,
  - Stavové informace a alarmy předávané do zóny Pole a Stanice,
  - Data přenášená prostřednictvím GOOSE a SV komunikace.

Možné vstupní body útočníka a rizika

- Kompromitace IED: Například zneužitím slabin v konfiguraci, firmware nebo komunikačním rozhraní.

- Manipulace se vstupními signály: Falsifikace měřených dat, která mohou vést k nesprávnému rozhodování IED.
- Zneužití nedostatečného oddělení zóny: Pokud by sandbox neimplementoval odpovídající segmentaci, mohl by útočník proniknout do této vrstvy z vyšších zón.

Zóna pole

Zóna pole představuje v návrhu sandbox architektury komunikační a přenosovou vrstvu, která zajišťuje propojení mezi zařízeními technologického procesu (zóna procesu) a řídicími a dohledovými systémy (zóna stanice). Tato zóna je kritická z hlediska přenosu dat, řízení technologických procesů a zároveň představuje významný prostor pro modelování bezpečnostních rizik, protože se zde nacházejí přirozené komunikační rozhraní systému. V distribuční infrastruktuře je zóna běžně tvořena fyzickými přenosovými cestami, komunikačními zařízeními a protokoly, které zajišťují spolehlivý a bezpečný přenos dat mezi jednotlivými částmi systému.

Navržené komponenty a jejich role

- RTU: Zajišťuje agregaci dat z technologického procesu a jejich přenos do vyšších vrstev architektury. V návrhu sandboxu RTU plní roli prostředníka mezi IED a SCADA systémem a umožňuje ověřování správnosti přenosu dat, stejně jako testování různých komunikačních scénářů.
- Komunikační infrastruktura: Síťová vrstva zajišťující přenos dat, implementovaná pomocí přepínačů a případně směrovačů, umožňujících segmentaci sítě. V návrhu sandboxu umožňuje testování různých topologií, včetně fyzického oddělení komunikačních cest pro specifické typy přenosu (například separátní VLAN pro GOOSE a SV komunikaci).
- GOOSE a SV komunikace: Využívá se pro přenos stavových a měřicích dat s velmi nízkou latencí mezi IED a RTU. V návrhu sandboxu je možné simulovat realistické scénáře komunikace, včetně testování dopadu různých typů útoků na tuto vrstvu.

Vstupy a výstupy zóny

- Vstupy:
  - Data ze zóny Procesu (stavové a měřicí signály z IED),
  - Konfigurační a řídicí příkazy ze zóny Stanice.
- Výstupy:
  - Agregovaná data do SCADA systému,
  - Stavové informace předávané obsluze přes HMI,
  - Odezvy a potvrzení o správnosti přenosu dat.

Možné vstupní body útočníka a rizika

- Nezabezpečenou RTU: Kompromitace tohoto prvku může umožnit manipulaci s přenášenými daty nebo přerušení komunikace.
- Zranitelnosti v GOOSE/SV komunikaci: Pokud není zajištěna integrita a autentizace těchto zpráv, může dojít ke spoofingu, replay útokům nebo manipulaci s měřenými daty.
- Síťovou infrastrukturu: Pokud není správně nastavena segmentace sítě, může útočník získat neoprávněný přístup k přenosovým cestám a narušit komunikaci mezi jednotlivými částmi systému.

Staniční zóna

Staniční zóna představuje v návrhu sandbox architektury vrstvu lokálního řízení, monitoringu a obsluhy systému. V této části infrastruktury se nachází klíčové komponenty, které zajišťují zpracování dat získaných z nižších vrstev (Proces a Pole) a poskytují operátorům a technikům přímý přístup k řízení distribuované sítě. Staniční zóna je v kontextu návrhu sandboxu rovněž významná z pohledu bezpečnostního modelování, neboť obsahuje přirozené vstupní body, které mohou být zneužity útočníkem.

Navržené komponenty a jejich role

- SCADA: Centrální systém pro monitoring a řízení technologických procesů. V návrhu sandboxu SCADA zajišťuje zobrazení stavu systému, sběr dat z RTU a IED a umožňuje zadávání řídicích příkazů.
- HMI: Uživatelské rozhraní pro obsluhu systému. Poskytuje vizualizaci aktuálního stavu sítě a umožňuje operátorům provádět ovládací zásahy. V rámci návrhu sandboxu je HMI integrováno do architektury tak, aby bylo možné modelovat různé scénáře přístupu a zabezpečení této části systému.
- Gateway: Překladový prvek mezi různými protokoly používanými v distribuované infrastruktuře. V návrhu sandboxu zajišťuje propojení mezi IEC 60870-5-104 a IEC 61850, což umožňuje testování interoperability a zároveň představuje potenciální vektor útoku, pokud by došlo ke kompromitaci této komponenty.

Vstupy a výstupy zóny

- Vstupy:
  - Data a stavové informace z RTU (Polní zóna),
  - Přístupové požadavky a konfigurační data z Provozní zóny (uživatelské stanice).
- Výstupy:
  - Řídicí příkazy do RTU a IED,
  - Vizualizace a alarmy zobrazované operátorům prostřednictvím HMI,
  - Přenesená data směrem k uživatelským stanicím v Provozní zóně.

Možné vstupní body útočníka a rizika

- Slabé zabezpečení HMI nebo SCADA: Pokud nejsou dostatečně chráněny přístupové mechanismy k těmto komponentám, může útočník získat neoprávněný přístup, což umožňuje manipulaci s řízením nebo monitoringem systému.
- Zneužití chyb v konfiguraci nebo implementaci gateway: Překlad mezi protokoly je citlivým místem infrastruktury, jeho kompromitace může vést k narušení integrity nebo dostupnosti komunikace mezi různými částmi sítě.
- Neoprávněný přístup prostřednictvím uživatelských stanic: Pokud jsou stanice v Provozní zóně špatně zabezpečeny, může útočník využít jejich připojení k získání kontroly nad SCADA nebo HMI.

Provozní zóna

Provozní zóna představuje v návrhu sandbox architektury vrstvu, která umožňuje vzdálený i lokální přístup k infrastruktuře distribuované sítě. Zahrnuje zejména uživatelské stanice, které slouží pro správu, konfiguraci a monitoring systému. Z této zóny může probíhat jak legitimní přístup techniků a operátorů, tak je možné tuto část infrastruktury využít pro simulaci neoprávněného přístupu nebo

útoků v rámci testovacích scénářů. Provozní zóna je z hlediska bezpečnosti velmi citlivá, neboť představuje přirozený vstupní bod do systému. V návrhu sandbox architektury je proto tato část navržena tak, aby umožňovala modelování různých variant připojení, autentizace a zabezpečení uživatelských stanic.

Navržené komponenty a jejich role

- Uživatelské stanice: Univerzální pracovní stanice, které mohou být využívány jako inženýrské stanice, operátorské stanice nebo jako útočící stanice v rámci testovacích scénářů. V návrhu sandboxu tyto stanice slouží pro přístup ke SCADA a HMI, konfiguraci zařízení a rovněž pro simulaci útoků na infrastrukturu.
- Přístupová infrastruktura: Součástí návrhu může být volitelně implementace přístupových mechanismů jako jsou VPN brány, vzdálené přístupy (RDP, SSH[2]) nebo autentizační servery, které umožňují modelovat různé varianty bezpečnostního nastavení vzdáleného přístupu.

Vstupy a výstupy zóny

- Vstupy:
  - Oprávněné přístupové požadavky techniků a operátorů,
  - Neoprávněné přístupové pokusy simulované v rámci bezpečnostních scénářů.
- Výstupy:
  - Konfigurační změny v systému,
  - Řídicí zásahy do systému prostřednictvím SCADA a HMI,
  - Generovaný síťový provoz v rámci testovacích scénářů, včetně simulovaných útoků.

Možné vstupní body útočníka a rizika

- Kompromitace uživatelské stanice: Pokud je stanice infikována škodlivým kódem nebo dojde k odcizení přihlašovacích údajů, může útočník získat přístup k řízení a konfiguraci systému.
- Zneužití slabin ve vzdáleném přístupu: Nedostatečně zabezpečené VPN, RDP nebo SSH přístupy mohou být zneužity k neoprávněnému přístupu do systému.
- Sociální inženýrství a phishing: Vzhledem k tomu, že tato zóna zahrnuje uživatelské stanice, může být systém ohrožen i prostřednictvím útoků na samotné uživatele (např. phishing).

5.2 Propojení modelu datových toků s teorií front

Modely datových toků představené v předchozích kapitolách poskytují detailní pohled na strukturu komunikace v návrhu sandbox architektury, včetně identifikace klíčových komponent, typů přenášených dat a hranic důvěry. Tyto modely umožňují analýzu bezpečnostních rizik a struktury infrastruktury, nicméně pro kvantitativní posouzení chování systému za různých provozních podmínek nejsou vhodné. Teorie front představuje vhodný nástroj pro modelování přenosu zpráv v komunikační infrastruktuře, zejména v těch částech systému, kde lze očekávat vznik zpoždění, přetížení nebo ztráty dat v důsledku náhodného charakteru provozu. Kombinace modelu datových toků s teorií front tak umožňuje nejen simulovat běžný provoz distribuované soustavy, ale také kvantitativně popsat chování systému v případě provozní degradace, kybernetického útoku nebo jiného nestandardního stavu. V následující části je provedeno systematické propojení vrstev komunikační infrastruktury s modelováním přenosu zpráv na základě teorie front. Cílem je určit, které části návrhu sandboxu je vhodné kvantitativně analyzovat pomocí frontových modelů a jaké modely jsou pro jednotlivé vrstvy a datové toky relevantní.

[2]Secure Shell, bezpečný komunikační protokol a nástroj pro vzdálený přístup.

5.2.1 Procesní sběrnice a aplikace teorie front

Procesní sběrnice tvoří nejnižší vrstvu návrhu sandbox architektury a zajišťuje výměnu měřených a ochranných dat mezi slučovacími jednotkami (MU) a inteligentními elektronickými zařízeními (IED). Klíčovými přenosy jsou GOOSE zprávy dle IEC 61850-8-1 a Sampled Values (SV) dle IEC 61850-9-2, jejichž generování a přenosové charakteristiky byly detailně popsány v kapitole 3.6. Chování této vrstvy lze z hlediska aplikace teorie front rozdělit do tří provozních režimů: Ideální stav, Reálný provoz a Přetížení.

Ideální stav – optimálně navržená infrastruktura

V případě, že:

- je síťová infrastruktura dimenzována s dostatečnou kapacitou,
- jsou správně nakonfigurovány VLAN pro oddělení SV a GOOSE provozu,
- je zajištěna prioritizace rámců (QoS),

potom probíhá komunikace deterministicky, bez vzniku front. SV zprávy jsou generovány s pevnou periodou dle vztahu:

$$T_{SV} = \frac{1}{f_s} = \frac{1}{N \cdot f_{\text{mains}}} \quad [\text{s}], \tag{5.1}$$

a modelovány deterministickým frontovým modelem **M/D/1**, kde příchody jsou pravidelné s intenzitou $\lambda_{SV} = f_s$.

GOOSE zprávy jsou v klidovém režimu generovány periodicky s nízkou intenzitou, kterou lze vyjádřit jako:

$$\lambda_p = \frac{1}{T_p} \quad [1/\text{s}], \tag{5.2}$$

kde T_p označuje periodu GOOSE zpráv v klidovém režimu. Tento provozní režim je popsán rovněž modelem **M/D/1**.

Reálný provoz – zvýšená zátěž a provozní odchylky

V běžném provozu může docházet k situacím, kdy:

- objem SV provozu dosahuje vysoké hodnoty,
- dočasně nastává burst režim GOOSE komunikace při změnách stavu,
- síťová infrastruktura vykazuje omezenou přepínací kapacitu.

V tomto režimu vznikají krátkodobé fronty v síťových prvcích, zejména na portech přepínačů. Přenos SV zpráv zůstává deterministický (model M/D/1), avšak v případě burst režimu GOOSE je nutné aplikovat **M/M/1** model, který aproximuje Poissonovské příchody zpráv s intenzitou:

$$\lambda_e = \frac{1}{T_{\min}} \quad [1/\text{s}]. \tag{5.3}$$

Současný přenos SV a burst GOOSE může vést ke kumulaci rámců ve vyrovnávacích bufferech, prodloužení latence a zvýšení pravděpodobnosti ztráty zpráv.

Přetížení nebo útokové scénáře

V případě přetížení, ať už v důsledku:

- nasazení příliš mnoha SV proudů bez rezervy kapacity,
- souběhu burst režimu GOOSE s vysokým SV zatížením,
- DoS/DDoS útoku generujícího falešné rámce na druhé vrstvě,

dochází k přetečení vyrovnávacích bufferů a výraznému zhoršení přenosových parametrů. Celkovou intenzitu příchodů zpráv lze v krizovém režimu popsat jako:

$$\lambda_{\text{total}} = \lambda_{SV} + \lambda_{GOOSE} + \lambda_a \quad [1/\text{s}], \tag{5.4}$$

kde λ_a představuje intenzitu rámců generovaných útokem. V tomto stavu je aplikace teorie front (kombinace M/D/1 pro SV, MMPP modelu pro GOOSE a zohlednění útokového provozu) klíčová pro kvantitativní hodnocení dostupnosti komunikace a spolehlivosti ochran.

Kvantitativní vyjádření zatížení a vazba na DFD

Přenos SV zpráv na procesní sběrnici odpovídá datovým tokům mezi slučovacími jednotkami (MU) a inteligentními elektronickými zařízeními (IED), jak jsou zakresleny v DFD modelu v kapitole 3.5. Tyto zprávy přenášejí vzorkované hodnoty proudů a napětí a jejich kmitočet a objem přenosu závisí na konfiguraci systému, zejména na počtu vzorků na periodu síťového kmitočtu.

V praxi se počet vzorků N volí podle požadované přesnosti měření a charakteru chráněného zařízení. Nižší počet vzorků (například 80 vzorků/cyklus) je dostatečný pro standardní aplikace a základní ochrany. Vyšší počet vzorků (128 až 256 vzorků/cyklus) se uplatňuje u přesnějších ochran (například distanční, diferenční) nebo tam, kde je potřeba vyšší rozlišení signálu.

Zvýšení počtu vzorků zlepšuje časové a amplitudové rozlišení měřených signálů, zároveň však výrazně zvyšuje datovou zátěž procesní sběrnice. Výsledný vzorkovací kmitočet se vypočítá dle vztahu:

$$f_s = N \cdot f_{\text{mains}} \quad [\text{Hz}], \tag{5.5}$$

kde f_{mains} je síťový kmitočet, v této práci uvažována standardní hodnota 50 Hz. Při velikosti jednoho rámce $S_{\text{frame}} = 100$ B a přenosové kapacitě linky $C_{\text{link}} = 100$ Mb/s lze kvantitativně odhadnout přenosovou zátěž jednotlivých SV proudů podle tabulky 5.2.

Tab. 5.2: Přenosová zátěž SV proudů v závislosti na vzorkovacím kmitočtu

Vzorky na periodu	**Frekvence rámců f_s**	**Počet rámců za sekundu**	**Zatížení linky**
80	4000 Hz	4000 rámců/s	∼3,2 Mb/s
128	6400 Hz	6400 rámců/s	∼5,12 Mb/s
256	12 800 Hz	12 800 rámců/s	∼10,24 Mb/s

Při typické konfiguraci rozvodny obsahující více Merging Units, kdy každá generuje vlastní SV proudy pro různé fáze a veličiny, může celková zátěž linky rychle narůstat. Uvažujeme-li například:

- jednu rozvodnu s 4 Slučovacími jednotkami,
- každá MU generuje jeden proud SV se 80 vzorky/cyklus,

pak celková zátěž procesní sběrnice je přibližně:

$$Z_{\text{total}} = 4 \cdot 3,2 \text{ Mb/s} = 12,8 \text{ Mb/s}.$$

Při zvýšení počtu vzorků na 256/cyklus narůstá zátěž na:

$$Z_{\text{total}} = 4 \cdot 10,24 \text{ Mb/s} = 40,96 \text{ Mb/s}.$$

Při této konfiguraci je využito již přibližně 41 % kapacity 100 Mb/s linky pouze pro SV provoz, bez započítání GOOSE zpráv a dalšího síťového provozu. To zvyšuje riziko přetížení a prodloužení latence, zejména při souběhu více SV proudů a burst režimu GOOSE.

Kvantitativní příklad přenosové zátěže GOOSE při události

Uvažujme běžný scénář, kdy v důsledku aktivace ochrany dochází ke změně stavu sledované veličiny a IED přechází do burst režimu generování GOOSE zpráv. Pro konfiguraci systému platí:

- Minimální interval mezi GOOSE zprávami $T_{\text{min}} = 2$ ms,
- Velikost jednoho GOOSE rámce $S_{\text{frame}} = 150$ B,
- Trvání burst režimu $t_{\text{burst}} = 100$ ms (typické dle IEC 61850-8-1).

Celkový počet vygenerovaných GOOSE zpráv během burst režimu:

$$N_{\text{GOOSE}} = \frac{t_{\text{burst}}}{T_{\text{min}}} = \frac{100 \text{ ms}}{2 \text{ ms}} = 50 \text{ zpráv}.$$

Celková objemová zátěž na linku během burst režimu:

$$Z_{\text{burst}} = N_{\text{GOOSE}} \cdot S_{\text{frame}} \cdot 8 = 50 \cdot 150 \cdot 8 = 60 \text{ kbit}.$$

Při uvažované kapacitě linky 100 Mb/s představuje celková krátkodobá zátěž GOOSE během burst režimu:

$$P_{\text{burst}} = \frac{Z_{\text{burst}}}{t_{\text{burst}}} = \frac{60 \text{ kbit}}{100 \text{ ms}} = 0,6 \text{ Mb/s}.$$

Tato hodnota sama o sobě nepředstavuje výrazné zatížení linky (cca 0,6 % kapacity). Je však nutné zohlednit situace, kdy může docházet k jejímu krátkodobému nebo trvalému navýšení:

- při souběhu více IED generujících GOOSE zprávy může být krátkodobá burstová zátěž násobně vyšší,
- pokud je linka zatížena jiným síťovým provozem, zejména při nedostatečném nastavení QoS, může dojít ke zvýšení latence GOOSE zpráv,
- v případě cíleného útoku, například generování podvržených GOOSE zpráv s falešným zdrojovým MAC adresováním nebo zahlcení sítě nelegitimními rámci, může být celková přenosová kapacita linky vyčerpána bez ohledu na nastavení priorit.

V případě útoku zaměřeného na zahlcení procesní sběrnice může útočník generovat velké množství podvržených GOOSE zpráv s falešným zdrojovým MAC adresováním. Tyto zprávy se šíří v síti multicastově stejně jako legitimní GOOSE provoz, což komplikuje jejich filtrování na síťové vrstvě.

Při uvažované velikosti jednoho GOOSE rámce $S_{\text{frame}} = 150$ B a přenosové kapacitě procesní sběrnice $C_{\text{link}} = 100$ Mb/s lze odhadnout, jaký počet podvržených zpráv za sekundu (N_{attack}) by vedl k přetížení linky. Celková zátěž způsobená útokem je dána vztahem:

$$Z_{\text{attack}} = N_{\text{attack}} \cdot S_{\text{frame}} \cdot 8 \quad [\text{b/s}].$$

Přetížení nastává, pokud:

$$Z_{\text{total}} = Z_{\text{attack}} + Z_{\text{SV}} + Z_{\text{GOOSE}} > C_{\text{link}}.$$

Jako modelový příklad uvažujme následující parametry:

- Zátěž běžného provozu:

$$Z_{\text{SV}} = 40,96 \text{ Mb/s} \quad (4 \text{ SV proudy při } 256 \text{ vzorcích/cyklus})$$

$$Z_{\text{GOOSE}} \approx 0,6 \text{ Mb/s} \quad (\text{burst režim})$$

- Zbývající kapacita linky:

$$C_{\text{free}} = C_{\text{link}} - (Z_{\text{SV}} + Z_{\text{GOOSE}}) = 100 - 41,56 = 58,44 \text{ Mb/s}.$$

Počet podvržených GOOSE zpráv nutný k přetížení linky:

$$N_{\text{attack}} = \frac{C_{\text{free}}}{S_{\text{frame}} \cdot 8} = \frac{58,44 \cdot 10^6}{150 \cdot 8} \approx 48\,700 \text{ zpráv/s}.$$

Tedy přibližně 48 700 falešných GOOSE zpráv za sekundu by zcela vyčerpalo zbývající kapacitu procesní sběrnice a vedlo k přetížení linky. V takovém případě selhává doručování i prioritizovaných legitimních GOOSE zpráv, což ohrožuje ochranné a řídicí funkce systému.

5.2.2 Staniční sběrnice a aplikace teorie front

Staniční sběrnice tvoří střední komunikační vrstvu návrhu sandbox architektury a zajišťuje výměnu informací mezi IED, HMI, SCADA a dalšími zařízeními v rámci elektrické stanice. Přenos probíhá na základě protokolu MMS dle IEC 61850-8-1, případně GOOSE zpráv pro logické propojení ochranných funkcí mezi jednotlivými poli. Přenosové charakteristiky a vztah k modelům teorie front jsou detailně popsány v kapitole 3.6. Chování této vrstvy lze z hlediska aplikace teorie front rozdělit do tří provozních režimů: Ideální stav, Reálný provoz a Přetížení.

Ideální stav – optimálně navržená infrastruktura

V případě, že:

- je síťová infrastruktura dostatečně kapacitní (typicky 100 Mb/s až 1 Gb/s),
- je oddělen provoz jednotlivých komunikačních protokolů (např. VLAN pro MMS, případně oddělení GOOSE),
- je správně nakonfigurována prioritizace kritických zpráv (QoS),

probíhá komunikace bez výrazných zpoždění a vzniku front. Přenosové požadavky odpovídají běžnému provozu:

- MMS zprávy pro vizualizaci a dohled mezi IED a SCADA/HMI mají nízkou frekvenci,
- Spontánní hlášení (reporting, SOE[3]) se vyskytují nepravidelně dle událostí v systému,
- Případné GOOSE zprávy na staniční úrovni (například blokovací nebo logické signály mezi IED) jsou generovány pouze při změně stavu.

V tomto režimu je možné aplikovat základní modely teorie front jako **M/D/1** pro cyklický provoz nebo **M/M/1** pro spontánní hlášení, avšak riziko přetížení je minimální.

[3]Sequence of Events, mechanismus, kdy IED posílá spontánní hlášení do SCADA

Reálný provoz – zvýšená zátěž a provozní odchylky

V běžném provozu může dojít k:

- zvýšené četnosti MMS komunikace při aktivním ovládání, diagnostice či konfiguraci ze SCADA/HMI,
- nárůstu počtu spontánních hlášení generovaných IED při poruchových stavech,
- aktivaci ochranných funkcí generujících GOOSE zprávy mezi jednotlivými IED na staniční sběrnici.

V těchto situacích může vznikat kumulace zpráv ve vyrovnávacích bufferech přepínačů a staniční sběrnice se stává citlivější na zpoždění a ztráty. Z hlediska teorie front lze v této fázi uvažovat:

- **M/M/1** model pro nepravidelné příchody MMS zpráv a SOE,
- **M/D/1** model při cyklickém dotazování dat,
- **MMPP** model při kombinaci klidového a událostního režimu GOOSE zpráv.

Správné nastavení QoS pomáhá minimalizovat zpoždění kritických zpráv, avšak při vyšší zátěži již dochází k prodlužování latence.

Přetížení nebo útokové scénáře

Při cíleném útoku nebo extrémní zátěži může dojít k:

- zahlcení staniční sběrnice falešnými MMS zprávami (například podvrženými reportingy),
- přetížení vyrovnávacích bufferů v přepínačích,
- ztrátě důležitých zpráv nebo zvýšení latence hlášení SOE a GOOSE zpráv.

Celkovou intenzitu příchodů lze analogicky popsat jako:

$$\lambda_{\text{total}} = \lambda_{\text{MMS}} + \lambda_{\text{SOE}} + \lambda_{\text{GOOSE}} + \lambda_{\text{attack}} \quad [1/\text{s}]. \tag{5.6}$$

Při překročení kapacity obsluhy μ vznikají fronty a ztráty zpráv, což ohrožuje spolehlivost řízení a dohledu v rámci stanice.

Kvantitativní vyjádření zatížení a vazba na DFD

Přenos MMS zpráv mezi IED a SCADA/HMI, řídící hlášení z IED a případné GOOSE zprávy mezi IED na staniční sběrnici. Objem přenášených dat závisí na četnosti vizualizace, konfigurace a počtu událostí. Uvažujme typickou středně velkou distribuční rozvodnu, která obsahuje přibližně 20 IED. Toto číslo odpovídá následující struktuře:

- 6 polí (VN, VVN) s dvojicí IED pro ochrany a měření na každém poli,
- 4 IED pro přípojnicové, nadřazené nebo záložní funkce.

V případě poruchového stavu, například aktivace ochranných funkcí, může každé IED generovat v krátkém časovém okně sérii řídících hlášení, která zaznamenávají:

- překročení limitů měřených veličin,
- aktivaci ochrany,
- blokovací signály,
- potvrzení příkazů.

Pro účely zátěžového scénáře uvažujeme intenzitu generování SOE zpráv 10 událostí za sekundu na jedno IED, což odpovídá intenzivní událostní situaci při rozsáhlejší poruše nebo testování systému.

Dále uvažujme:

- velikost jednoho SOE hlášení 200 B,
- běžnou velikost MMS datového rámce pro vizualizaci 300 B,

- GOOSE zprávy na staniční sběrnici jsou generovány pouze při změnách logických stavů mezi jednotlivými IED.

Výpočet objemu SOE provozu při této poruchové situaci:

$$Z_{\text{SOE}} = 20 \cdot 10 \cdot 200 \cdot 8 = 320 \text{ kb/s}.$$

Zátěž běžného MMS provozu pro vizualizaci mezi SCADA/HMI a IED:

$$Z_{\text{MMS}} \approx 300 \text{ B} \cdot 10 \text{ zpráv/s} \cdot 8 = 24 \text{ kb/s}.$$

Při útoku generujícím například 5000 falešných MMS zpráv za sekundu o velikosti 300 B lze očekávat:

$$Z_{\text{attack}} = 5000 \cdot 300 \cdot 8 = 12 \text{ Mb/s}.$$

Na staniční sběrnici s kapacitou 100 Mb/s představuje útok zátěž na úrovni 12 %, což při souběhu s běžným provozem a SOE zprávami výrazně zvyšuje riziko přetížení.

5.2.3 Přístupová a WAN vrstva a aplikace teorie front

Přístupová a WAN vrstva tvoří nejvyšší komunikační úroveň návrhu sandbox architektury. Zajišťuje propojení elektrické stanice s nadřazenými dispečerskými systémy SCADA/DMS prostřednictvím směrovačů, firewallů a WAN technologií. Klíčovým komunikačním protokolem je IEC 60870-5-104, který realizuje přenos stavových informací, měření a řídicích příkazů mezi stanicí a dispečerským systémem. Tato vrstva je zároveň nejvíce vystavena externím hrozbám z veřejných a sdílených sítí. Kapacita přenosové trasy v této vrstvě se výrazně liší v závislosti na použité technologii připojení a fyzickém umístění objektu. V praxi lze rozlišit následující scénáře:

- **V průmyslových objektech nebo rozvodnách v terénu**:
  - Mobilní připojení (LTE/5G): typicky jednotky až desítky Mb/s,
  - Bezdrátové spoje (mikrovlnné, rádiové): řádově 10–100 Mb/s,
  - Metalické WAN připojení (starší technologie): obvykle 10/100 Mb/s.
- **V moderních rozvodnách nebo při přímém optickém propojení**:
  - Optické připojení: běžně 100 Mb/s, 1 Gb/s nebo i více.

Chování této vrstvy lze z hlediska aplikace teorie front rozdělit do tří provozních režimů: Ideální stav, Reálný provoz a Přetížení.

Ideální stav – optimálně navržená infrastruktura

V případě, že:

- je přenosová trasa dostatečně kapacitní vzhledem k typu použité technologie,
- je komunikace šifrována a zabezpečena (VPN, IPsec),
- je zajištěna prioritizace kritických zpráv (QoS na WAN rozhraní),

probíhá přenos dat deterministicky, s minimálním zpožděním a bez ztrát. V tomto režimu lze modelovat přenos zpráv pomocí **M/D/1** modelu pro periodické přenosy a **M/M/1** modelu pro spontánní hlášení a příkazy.

Reálný provoz – zvýšená zátěž a provozní odchylky

V běžném provozu mohou ovlivnit kvalitu přenosu následující faktory:

- sdílené využívání WAN infrastruktury s jinými systémy,

- zvýšený objem přenosu při aktualizacích nebo konfiguracích,
- kolísání kapacity u bezdrátových nebo mobilních WAN technologií,
- dočasné zhoršení kvality přenosu (jitter, latence, ztrátovost).

V těchto situacích může vznikat kumulace zpráv ve vyrovnávacích bufferech na WAN rozhraní a zvýšení latence. Z hlediska teorie front je vhodné modelovat systém kombinací **M/M/1** a **M/D/1** modelů dle charakteru provozu.

Přetížení nebo útokové scénáře

Největší riziko na této vrstvě představují:

- DoS/DDoS útoky zahlcující WAN rozhraní (např. SYN flooding, UDP flooding),
- útoky na VPN nebo šifrovací protokoly vedoucí ke zpomalení přenosu,
- zahlcení linky nelegitimním provozem (např. velké objemy dat přicházejících z veřejné sítě).

Celkovou intenzitu příchodů lze popsat jako:

$$\lambda_{\text{total}} = \lambda_{\text{IEC104}} + \lambda_{\text{background}} + \lambda_{\text{attack}} \quad [1/\text{s}],$$

kde:

- λ_{IEC104} představuje intenzitu kritického provozu přenášeného protokolem IEC 60870-5-104,
- $\lambda_{\text{background}}$ zahrnuje ostatní běžný síťový provoz, například administrativní data, diagnostiku nebo aktualizace zařízení,
- λ_{attack} odpovídá intenzitě nelegitimního provozu generovaného v rámci kybernetického útoku.

Při překročení kapacity WAN rozhraní μ dochází ke ztrátám zpráv, zvýšení latence nebo úplnému výpadku komunikace mezi stanicí a dispečerským systémem.

Kvantitativní vyjádření zatížení a vazba na DFD

Přenos dat přes přístupovou/WAN vrstvu odpovídá toku mezi stanicí (IEC 104 gateway) a dispečerským systémem SCADA/DMS, jak je zachyceno v DFD modelu kapitoly 3.5. Objem přenášených dat a celková zátěž této vrstvy závisí na použité technologii připojení a její kapacitě.

Pro účely zátěžového výpočtu uvažujme následující vstupní parametry:

- velikost jedné IEC 104 zprávy 200 B,
- frekvence přenosu 20 zpráv za sekundu,
- útok generující 5000 nelegitimních paketů za sekundu o velikosti 500 B.

Běžná zátěž kritického provozu:

$$Z_{\text{IEC104}} = 200 \text{ B} \cdot 20 \text{ zpráv/s} \cdot 8 = 32 \text{ kb/s}.$$

Zátěž útoku:

$$Z_{\text{attack}} = 5000 \cdot 500 \cdot 8 = 20 \text{ Mb/s}.$$

Celkové využití přenosové kapacity v závislosti na typu WAN připojení je shrnuto v tabulce 5.3. Z výpočtu je zřejmé, že při nízkokapacitním připojení (například 10 Mb/s) i relativně nízkoobjemový útok zcela vyčerpá kapacitu a znemožní komunikaci. Při standardním optickém připojení (100 Mb/s) je stále nutné počítat se zvýšenou latencí a rizikem degradace služeb, zejména pokud není správně nastaveno QoS nebo filtrování. Vysoce kapacitní připojení (1 Gb/s) výrazně zvyšuje odolnost vůči zátěžovým stavům a útokům, přičemž běžný i nelegitimní provoz představuje zanedbatelné zatížení.

Tab. 5.3: Využití přenosové kapacity WAN vrstvy při různé kapacitě připojení

Přenosová kapacita	IEC 104 provoz	Zátěž útoku	Celkové využití
10 Mb/s	0,32 %	200 %	Přetížení
100 Mb/s	0,032 %	20 %	Zvýšené riziko, ale funkční
1 Gb/s	0,0032 %	2 %	Zanedbatelné

5.3 Analýza existujících testovacích prostředí

Cílem této kapitoly je systematicky zmapovat a analyzovat aktuálně existující přístupy k testovacím prostředím v oblasti elektroenergetiky se zaměřením na jejich schopnosti, limity a využitelnost z hlediska kyberbezpečnosti a testování komunikačních protokolů. Na základě této analýzy budou identifikovány klíčové nedostatky těchto řešení, které motivují návrh vlastní škálovatelné sandbox architektury představené v této práci.

Článek [35] poskytuje podrobný přehled a metodiku pro vytváření testbedů, které jsou klíčové pro vývoj a testování bezpečnostních řešení v průmyslových řídicích systémech. Vytváření testovacích prostředí lze rozdělit do několika kategorií, z nichž každá má své specifické výhody a omezení. Fyzické testbedy, které využívají reálné hardwarové komponenty k napodobení skutečného průmyslového prostředí, poskytují nejvyšší úroveň věrnosti. Tyto testbedy jsou schopny přesně simulovat reálné provozní podmínky, což umožňuje detailní analýzu a testování bezpečnostních opatření. Nicméně, jejich vytvoření a údržba jsou nákladné a časově náročné.

Alternativou k fyzickým testbedům jsou simulované testbedy, které využívají softwarové simulace k replikaci chování průmyslových zařízení. Tyto simulace jsou nákladově efektivnější a snadněji škálovatelné než fyzické testbedy. Simulované testbedy umožňují flexibilní konfiguraci různých scénářů a podmínek, což je ideální pro testování různých typů kybernetických útoků. Na druhou stranu, simulace mají nižší úroveň věrnosti ve srovnání s fyzickými testbedy, což může omezit přesnost výsledků.

Virtuální testbedy představují kombinaci simulací a virtuálních zařízení, která běží na společném hardwaru. Tento přístup nabízí kompromis mezi náklady a věrností, což z něj činí praktické řešení pro mnoho aplikací. Virtuální testbedy jsou také flexibilní a umožňují snadnou úpravu a rozšíření dle potřeby. Hybridní testbedy pak kombinují prvky fyzických, simulovaných a virtuálních testbedů, čímž poskytují vyvážený přístup s výhodami všech tří metod. Tento přístup umožňuje detailní simulaci reálného prostředí s nižšími náklady než u čistě fyzických testbedů a zároveň nabízí vyšší věrnost než čistě simulované prostředí.

Vytváření a hodnocení testbedů v rámci této metodiky zahrnuje několik klíčových parametrů. Věrnost, tedy jak věrně testbed napodobuje skutečné prostředí, je jedním z nejdůležitějších aspektů. Fyzické testbedy obvykle získávají nejvyšší skóre v této oblasti, zatímco simulace, ačkoli nákladově efektivnější, poskytují nižší úroveň věrnosti.

5.3.1 Kritéria hodnocení a jejich odůvodnění

Pro objektivní srovnání jednotlivých testovacích prostředí byla zvolena následující kritéria, která reflektují požadavky na moderní kyber-fyzickou výzkumnou platformu v oblasti elektroenergetiky. Kritéria vycházejí z praktických požadavků, které definují, jak realisticky dané prostředí odráží skutečné provozní podmínky, jak komplexní je jeho zaměření a jaké možnosti nabízí pro testování komunikace a kybernetické bezpečnosti.

- Realizace testovacího prostředí: Úroveň realismu je pro validaci výzkumu zcela zásadní. Simulace nabízí flexibilitu a snadnou modifikovatelnost, emulace přidává přesnost reakce zařízení a fyzické prvky jsou nutné pro testování skutečných scénářů včetně kybernetických útoků na reálný hardware. Bez této kombinace nelze dosáhnout dostatečně věrného testovacího prostředí.
- Podporované komunikační protokoly: Energetická infrastruktura je extrémně heterogenní z pohledu používaných protokolů. Pro realistické testování bezpečnosti a interoperability je nezbytné, aby prostředí podporovalo široké spektrum běžně nasazovaných protokolů, a to jak na úrovni stanic, tak v řídicích centrech.
- Zastoupení klíčových prvků infrastruktury: Bez replikace základních komponent elektroenergetické sítě nelze validně testovat jak provozní scénáře, tak útoky nebo poruchové stavy. Klíčové je zastoupení řídicích systémů (SCADA), prvků na úrovni pole (IED, RTU) a vizualizačních rozhraní (HMI).
- Účel a zaměření prostředí: Různá prostředí cílí na odlišné výzkumné oblasti. Pro vývoj a validaci CPS je však nezbytné, aby prostředí umožňovalo nejen simulaci provozu, ale i testování bezpečnosti a realistických útoků.

5.3.2 Výsledky z testovací prostředí

V níže uvedené tabulce 5.4, jsou uvedena relativní testovací prostředí vybraná podle kritérií[4], Vyhledávání bylo provedeno v IEEE, kde byl stanoven rok mezi 2015 až 2022. Hledání podle roku bylo omezeno, protože v článku [61] jsou shrnuty nejvhodnější starší testovací prostředí do tohoto roku. Celkem bylo vráceno 130 výsledků, z nichž byly vybrány testovací prostředí zaměřené na energetiku. Popis každého z analyzovaných prostředí je uveden v příloze B.

Tabulka je rozdělena do sedmi částí, přičemž většina sloupců je vyjádřena pomocí symbolů ✓nebo ✗, které označují, zda je daný prvek v testovacím prostředí přítomen, či nikoliv. První sloupec tabulky (Reference) slouží jako identifikátor testovacího prostředí a je vyjádřen citací článku, ze kterého byly informace o daném prostředí získány. Druhý sloupec (Rok) uvádí rok publikace článku.

Sloupce souhrnně označené jako **Realizace** vyjadřují, zda testovací prostředí obsahuje virtualizované/simulované, emulované či fyzické komponenty. Virtualizovaný či simulační systém nebo prvek je softwarový program, který umožňuje virtualizaci jednotlivých prvků či celých systémů. Tento přístup není vázán na konkrétní hardware nebo operační systém. Typickým příkladem může být například OPNET Modeler nebo NS-3.

Emulovaný prvek či systém je sada softwarových nástrojů, která na hardwaru vytváří stejné vstupy a výstupy jako reálný fyzický prvek či systém. Emulovaný systém však není závislý na konkrétním hardwaru, jeho funkčnost spočívá v replikaci fyzických vstupů a výstupů, které odpovídají skutečnému fyzickému prvku či systému. Konkrétním příkladem může být implementace knihoven pro standard IEC 61850 na zařízení Raspberry Pi s moduly pro snímání elektrických veličin, které jsou následně převedeny do datové komunikace, čímž je například emulováno zařízení typu ochranné jednotky.

Fyzický systém či prvek představuje reálné zařízení běžně používané v praxi pro reálné aplikace. Případně se za fyzický systém či prvek považuje zařízení, které sice replikuje vstupy a výstupy reálných zařízení, ale je proprietární z hlediska hardwaru, softwaru, nebo obojího, a nelze jej přenést

[4](ics OR scada OR ied OR substation) AND (testbed OR test bed OR cyber range OR cyber-range) AND (virtual* OR simulat* OR emulat* OR virtual machine OR physic*) AND (electric* OR energy OR 61850 OR 60870 OR DNP3)

Tab. 5.4: Testovací prostředí energetických sítí

Reference	Rok	Realizace			Protokoly						Prvky					Účel			Ostatní
		Virt./Simul.	Emulovane	Fyzické	IEC61850	IEC60870	DNP3	OPC UA	ModBusTCP	C37.118	SCADA	HMI	(M/R)TU	IED	Útočník	Gen./Simul.	Edukační	Bezpečnost	
[64]	2015	✓	✗	✗	✗	✗	✗	✓	✗	✗	✓	✓	✗	✓	✗	✗	✗	✗	IEEE 39-bus
[203]	2015	✗	✗	✓	✓	✗	✗	✗	✗	✗	✗	✗	✓	✗	✓	✗	✗	✓	RTDS, Fuzzitng
[189]	2022	✓	✗	✗	✓	✗	✓	✗	✓	✗	✗	✗	✗	✓	✗	✗	✗	✓	-
[187]	2020	✗	✓	✓	✓	✗	✓	✗	✓	✗	✓	✗	✗	✓	✗	✓	✓	✓	RTDS, OpenADR 2.0, IEEE 13-bus, IEEE 39-bus
[204]	2019	✗	✓	✓	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	RTDS
[67]	2018	✓	✗	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗	✓	✓	✗	✗	✓	libiec61850, GNS3, Matlab/Simulink
a [180]	2019	✗	✓	✓	✓	✓	✓	✓	✓	✗	✓	✓	✓	✓	✓	✗	✗	✓	IRIG-B, EthernetIP, NTP
[91]	2021	✓	✗	✓	✗	✗	✓	✗	✗	✓	✗	✗	✓	✓	✗	✗	✗	✓	PowerWorld DS, RTAC
[200]	2016	✓	✗	✓	✗	✗	✗	✗	✓	✗	✓	✗	✗	✗	✗	✓	✗	✗	RDTS, Matlab
[201]	2021	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	✗	✓	RDTS
[87]	2021	✗	✓	✗	✓	✗	✗	✗	✗	✗	✓	✗	✗	✓	✗	✓	✗	✗	Microgrid, emulated IED
[93]	2020	✓	✗	✗	✗	✗	✓	✗	✗	✗	✓	✗	✓	✓	✗	✗	✓	✗	PowerWorld DS, DTS
[52]	2022	✓	✓	✓	✗	✗	✗	✗	✗	✗	✓	✓	✗	✓	✗	✗	✗	✓	GNS3
[192]	2015	✓	✗	✗	✗	✓	✓	✗	✗	✗	✗	✓	✓	✓	✓	✗	✗	✓	PSAT
[208]	2020	✓	✗	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗	✓	✓	✗	✗	✓	IEEE 39-bus
[207]	2021	✓	✗	✓	✓	✗	✗	✗	✗	✗	✗	✗	✗	✓	✗	✗	✗	✓	-
[185]	2019	✗	✓	✓	✓	✗	✓	✗	✗	✓	✓	✓	✓	✓	✓	✗	✓	✓	RTDS, RTAC
[92]	2022	✓	✗	✗	✗	✗	✓	✗	✗	✗	✗	✗	✓	✓	✓	✗	✗	✓	PWDS, CORE, RTAC
[66]	2016	✓	✓	✓	✓	✗	✗	✗	✗	✗	✗	✗	✓	✓	✗	✗	✗	✗	-
[90]	2018	✓	✗	✓	✓	✗	✗	✗	✗	✗	✗	✗	✗	✓	✓	✗	✗	✓	RTDS
[164]	2018	✗	✓	✓	✗	✗	✗	✗	✗	✓	✗	✗	✗	✓	✗	✓	✗	✓	RTDS, RIAPS, IEEE 14-bus
[166]	2020	✓	✓	✓	✓	✗	✗	✗	✗	✗	✗	✓	✗	✓	✗	✗	✓	✗	-
[159]	2016	✓	✗	✓	✓	✗	✗	✗	✗	✗	✗	✓	✗	✓	✓	✓	✗	✓	-
[184]	2020	✓	✗	✓	✓	✗	✓	✗	✗	✗	✓	✗	✓	✓	✗	✓	✗	✓	IEEE 14-bus, OPAL-RT
[48]	2022	✓	✓	✓	✓	✗	✗	✗	✓	✗	✗	✗	✗	✓	✓	✗	✗	✗	OPAL-RT, MATLAB/Simulink, Kali
[88]	2016	✓	✗	✓	✗	✗	✗	✗	✗	✓	✗	✗	✗	✓	✓	✓	✗	✓	NS-3, Riverbed Modeler, SITL, WAMC
[199]	2015	✓	✗	✓	✓	✗	✓	✗	✗	✓	✗	✓	✗	✓	✓	✓	✗	✗	RTDS, IEEE 14, NS-3
[47]	2015	✓	✗	✓	✗	✗	✓	✗	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗	Opal-RT, Mat-lab/Simulink, RTDS
[46]	2016	✓	✓	✓	✓	✗	✓	✗	✓	✓	✓	✗	✗	✓	✗	✓	✗	✓	matlab, python, HIL, SIL, RTDS, openPDC,
[45]	2018	✗	✗	✓	✓	✗	✗	✗	✗	✗	✓	✗	✓	✓	✓	✓	✗	✓	-
[156]	2015	✓	✗	✓	✓	✓	✗	✗	✗	✗	✓	✗	✓	✓	✓	✗	✗	✓	SNORT, BRO
[172]	2018	✓	✗	✗	✗	✓	✗	✓	✗	✗	✗	✓	✓	✗	✗	✓	✗	✗	-
[53]	2016	✗	✓	✓	✓	✗	✓	✗	✗	✓	✓	✗	✓	✓	✓	✗	✓	✓	-
[51]	2018	✓	✗	✗	✗	✓	✗	✗	✗	✗	✓	✓	✓	✗	✗	✗	✓	✓	CRATE, OTS Power Grid
[197]	2013	✓	✗	✗	✗	✓	✓	✗	✓	✗	✓	✓	✓	✓	✗	✓	✓	✗	-
[168]	2018	✓	✓	✗	✓	✓	✓	✗	✗	✗	✓	✓	✓	✓	✗	✗	✗	✓	Snort, ICCP/TASE.2
[85]	2016	✓	✓	✗	✓	✗	✗	✗	✗	✗	✗	✗	✓	✓	✗	✓	✗	✗	libiec61850, IEDscout
[196]	2016	✓	✗	✗	✓	✗	✗	✗	✗	✗	✗	✓	✓	✓	✓	✗	✗	✓	Matlab/simulink, libiec61850

na jiný hardware či software. Příkladem takového zařízení je RTDS, které umožňuje simulaci rozsáhlých sítí, emulaci zařízení včetně fyzických výstupů a zároveň obsahuje proprietární hardware. V tomto případě je RTDS klasifikováno jako fyzický prvek, protože stejně jako reálná zařízení je tvořeno specializovaným hardwarem a softwarem, přestože z hlediska funkcí splňuje parametry virtualizace nebo simulace.

Z testovaných prostředí vyplývá, že nejvíce projektů je realizováno formou virtuálních nebo simulačních prostředí, která tvoří cca 76 %. Fyzické prvky se objevují v přibližně 61 % a emulace v cca 37 % případů. Kombinace všech tří typů realizace (virtuální/simulační, emulované i fyzické prvky) je pro věrné hodnocení kyber-fyzických vlastností zásadní. V analýze prostředí ji však splňuje jen 5 [52, 66, 166, 48, 46] z 38 (cca 13 %). Zbylé jsou zaměřené jen na jeden nebo dva typy realizace, což zhoršuje jejich použitelnost a realičnost.

V oblasti komunikačních protokolů má nejvyšší zastoupení IEC 61850 (cca 63 %), což odráží jeho roli jako současného standardu pro staniční a procesní automatizaci i ochranné funkce. Druhým nejčastějším protokolem je DNP3 (cca 40 %). Protokoly IEC 60870-5-104 a Modbus/TCP se vyskytují shodně přibližně v 18 % testovacích prostředí, což ukazuje na jejich spíše doplňkovou roli. OPC UA má minimální zastoupení (cca 8 %), a C37.118, určený pro přenos synchrofázorů, je přítomen asi ve 21 % případů.

Protokoly IEC 61850 a IEC 60870-5-104 představují stěžejní komunikační standardy pokrývající celé spektrum přenosu dat od procesní a staniční úrovně v elektrické rozvodně (IEC 61850) až po komunikaci mezi řídicím systémem a dispečinkem (IEC 60870-5-104). Pro zajištění plnohodnotné funkčnosti a ověřitelnosti scénářů je nezbytné, aby byla obě rozhraní v testovacím prostředí zastoupena současně. Z analyzovaných prostředí tuto podmínku splňují pouze [180], [156] a [168]. Absence jednoho z těchto protokolů významně snižuje využitelnost testovací platformy, zejména při ověřování kyber-fyzických interakcí v rámci celé komunikační vertikály. Alternativou k IEC 60870-5-104 může být protokol DNP3, ten je však relevantní především pro americké prostředí. V evropském, a tedy i českém kontextu, kde je tato práce primárně situována se nevyužívá.

Protokoly DNP3, OPC UA, C37.118 a Modbus/TCP sice nejsou v této disertační práci detailně rozebírány, ale patří mezi relevantní technologie používané v energetickém sektoru. DNP3 má své hlavní uplatnění v USA a dalších mimoevropských regionech, kde nahrazuje IEC 60870-5-104, zatímco v Evropě se IEC 104 používá pro přímé řízení v elektroenergetice. OPC UA a Modbus/TCP se uplatňují spíše v podpůrných systémech a nadřazených řídicích aplikacích, nikoli jako hlavní protokoly pro kritické procesní řízení.

V rámci hodnocených testovacích prostředí jsou nejčastěji zastoupeny IED, a to přibližně v 82 % případů, což odráží důraz na modelování zařízení pole a ochran. Na druhém místě se nacházejí jednotky (M/R)TU s podílem okolo 47 %, které slouží pro sběr a předávání dat mezi poli a staniční úrovní. Systémy SCADA jsou implementovány zhruba ve 42 % prostředí a rozhraní HMI pouze ve 34 %. Tato distribuce ukazuje, že zatímco prvky procesní vrstvy jsou poměrně dobře zastoupeny, nadřazené řídicí systémy a operátorská rozhraní se vyskytují méně často. Plnohodnotná replikace vertikály SCADA–HMI–IED je proto spíše výjimečná, což snižuje možnosti provádět komplexní testování celého řetězce „měření–ochrana–řízení–operátor“. Nedostatek HMI a SCADA zároveň omezuje prověřování operačních aspektů kybernetické bezpečnosti, jako je práce s alarmy nebo reakční časy obsluhy při mimořádných událostech.

Analýza účelu hodnocených testovacích prostředí ukazuje, že přibližně 68 % z nich je primárně zaměřeno na oblast kybernetické bezpečnosti. Explicitní model útočníka, tedy scénáře, které definují schopnosti, záměry a postupy protivníka, se objevuje přibližně ve 42 % případů. Generování či simulace provozních dat je zahrnuto u zhruba 37 % prostředí a edukační scénáře, zaměřené na výuku a trénink obsluhy, tvoří přibližně 18 %. Z toho pouze jediné prostředí [187] je zaměřeno na

všechny tři účely - edukaci, simulaci/generování a kybernetickou bezpečnost.

Z výsledků analýzy vyplývá, že žádné z hodnocených testovacích prostředí nepokrývá plně všechna stanovená kritéria napříč skupinami Realizace, Protokoly, Prvky a Účel. Nejvhodnějším kandidátem z hlediska šíře pokrytí je prostředí popsané v [180], které dosahuje nejvyššího celkového počtu splněných kritérií (13 z 17) a zároveň zahrnuje oba klíčové standardy — IEC 61850 a IEC60870. Má kompletní zastoupení všech prvků a vysoké pokrytí protokolů, chybí mu pouze C37.118. Jeho slabinou je však oblast účelu, kde se zaměřuje výhradně na bezpečnostní scénáře, bez podpory simulačních a edukačních aktivit a v oblasti realizace, kde umožňuje emulaci zařízení, používá i fyzická zařízení, ale neumožňuje jejich virtualizaci.

Dalšími relevantními kandidáty jsou [168] a [156], které rovněž zahrnují oba zásadní komunikační standardy, avšak s nižším celkovým pokrytím kritérií (10/17, resp. 9/17). Celkově lze konstatovat, že neexistuje žádné prostředí, které by pokrývalo celé spektrum od úrovně realizace až po účel využití. Tento nedostatek odráží současný stav testovacích prostředí v energetickém sektoru a podtrhuje potřebu vývoje komplexní platformy, která by tato omezení překonala, což je i jedním z hlavních cílů této disertační práce.

6 Implementace testovací prostředí a validace

Cílem této kapitoly je představit realizaci a validaci testovacího prostředí, které bylo vytvořeno pro simulaci komunikačních a řídicích procesů v prostředí elektrických stanic. Na základě analytických modelů datových toků a architektonických vrstev byla vytvořena funkční topologie odpovídající reálným podmínkám v přenosové a distribuční soustavě. Kapitola se soustředí jak na strukturu testbedu založeného na DFD modelech, tak na implementaci jednotlivých vrstev komunikace, tak i celého systému včetně ověření.

6.1 Využití DFD modelů pro návrh struktury testovacího prostředí

Při návrhu topologie testovacího prostředí byly jako vstupní analytické podklady využity DFD modely popsané v kapitole 3.5. Modely zachycují klíčové datové toky mezi jednotlivými funkčními entitami. Jejich hlavním přínosem pro implementaci je popis komunikačních vazeb a logických rozhraní, které následně slouží jako základ pro segmentaci sítě a realizaci komponentového uspořádání testbedu.

Segmentace sítě na základě DFD modelu vzdálené komunikace

První model popisuje komunikaci mezi dispečerským centrem, SCADA systémem a elektrickou stanicí. Slouží jako podklad pro komunikační vrstvu mezi SCADA a RTU na hranici elektrické stanice. V tabulce 6.1 je uvedena realizace pomocí fyzických a softwarových prvků, použité protokoly a role pro daný segment sítě.

Tab. 6.1: Síťové segmenty na základě DFD modelu vzdálené komunikace

Segment sítě	**Role v systému**	**Realizace**	**Protokoly**
Dispečerská síť	operátor	VM, PC, HMI	IEC 60870-5-104
SCADA	správa, řízení	VM, server	IEC 104, MMS
WAN	SCADA ↔ Stanice	směrovače	TCP/IP
Stanice	Přijímající zařízení	VM, PC	IEC 104

Segmentace na základě DFD modelu vnitřní komunikace stanice

Druhý model se zaměřuje na vnitřní provoz v rámci elektrické stanice. Popisuje interakci mezi měřicími zařízeními, IED, řídicími jednotkami a systémy pro vizualizaci či historizaci dat. Tento model sloužil jako výchozí podklad pro návrh vnitřní topologie stanice. V tabulce 6.2 je uvedena realizace pomocí fyzických a softwarových prvků, použité protokoly a role pro daný segment sítě.

Tab. 6.2: Síťové segmenty na základě DFD modelu vnitřní komunikace

Vrstva testbedu	**Role v systému**	**Realizace**	**Protokoly**
Procesní vrstva	MU, čidla, měření	VM, PC	SV
Polní vrstva	Ochrana	VM, PC	GOOSE, MMS
Staniční vrstva	SCADA v rozvodně	VM, server, HMI	MMS

6.2 Emulační jednotka

V předchozí části byly na základě DFD modelů definovány klíčové funkční vrstvy systému a síťová segmentace testbedu. V této struktuře hrají zásadní roli jednotlivé funkční uzly, které zajišťují generování, přenos a zpracování datových toků – typicky odpovídajících komunikaci v rámci standardu IEC 61850 nebo IEC 60870-5-104. Pro realizaci těchto uzlů byly zvoleny počítače Raspberry Pi, které díky své flexibilitě umožňují věrně emulovat zařízení jako jsou měřicí jednotky (MU), ochrany (IED), SCADA stanice či brány RTU. Každá emulační jednotka byla přiřazena konkrétní roli v rámci segmentu vymezeného DFD modelem a přenáší odpovídající datové toky prostřednictvím vybraných protokolů (GOOSE, MMS, SV, IEC 104).

Raspberry Pi jsou malé jednodeskové počítače, které jsou snadno přenosné a mohou být umístěny téměř kdekoli. Jejich kompaktní velikost umožňuje integraci do různých fyzických struktur a zařízení. Oba modely poskytují dostatečný výpočetní výkon pro emulaci, díky čtyřjádrovým procesoru a 1 až 8 GB RAM dle konfigurace. To je více než dostačující pro zařízení, které se vyskytují v elektrických stanicích a slouží pro řízení a ochranu elektrických zařízení.

Díky rozhraním jako jsou GPIO piny, ethernetové a USB porty, lze Raspberry Pi snadno rozšířit o další fyzické prvky, jako jsou senzory, akční členy, další ethernetové rozhraní a nebo jiné periferie. To umožňuje vytvářet komplexní a realistické emulační scénáře. Raspberry Pi běží na operačním systému Linux (Raspbian), který je flexibilní a podporuje širokou škálu softwaru. To umožnuje schopnost komunikovat přes různé protokoly a rozhraní běžné v průmyslových aplikacích. Jednotky jsou cenově a široce dostupné, což je činí ideálními pro použití v emulačních stanicích, kde je potřeba více jednotek pro simulaci různých zařízení. Raspberry Pi má rozsáhlou uživatelskou komunitu a mnoho dostupných zdrojů podpory. To zahrnuje návody, knihovny a softwarové balíčky, které mohou usnadnit vývoj a implementaci emulačních aplikací.

Díky otevřenému Linuxovému prostředí (Raspbian) lze na Raspberry použit různé jazyky (C, Python, Java apod.), snadno instalovat knihovny, aktualizovat software a rozšiřovat hardware. Pro realizaci protokolů ze standardu IEC 61850 byla vybrána knihovna libiec61850[1], která je napsaná v jazyce C pod licencí open-source (GPLv3) a je přenosná na mnoho platforem včetně ARM Linuxu.

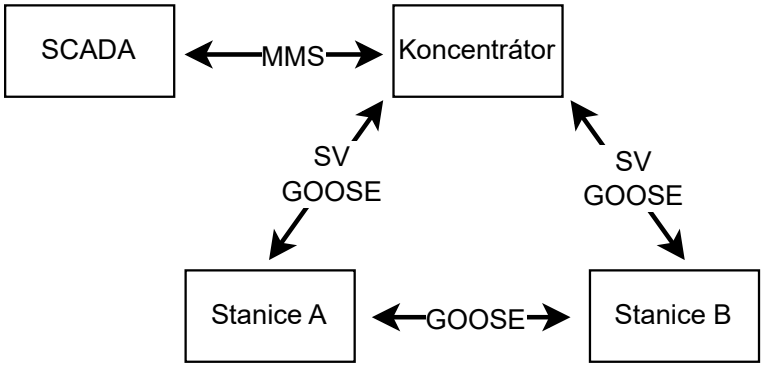
V článku [5] je uvedeno zátěžové testování Raspberry Pi 3B+ jako hlavní hardware platformy pro generování síťového provozu protokolů MMS, GOOSE a SV v rámci standardu IEC 61850. Struktura testovací prostředí se skládala ze tří Raspberry Pi jednotek a jednoho desktopového počítače. Zjednodušené schéma je uvedeno na obrázku 6.1 a skládá se z následujících stanic:

- Koncentrator: Raspberry Pi fungující jako ekvivalent RTU, který sbírá data z Stanice a a Stanice B zařízení a posílá je pomocí MMS protokolu na SCADA.
- Stanice: Dvě Raspberry Pi fungující jako simulovaná OT zařízení, která komunikují přímo pomocí protokolů MMS, GOOSE a SV.
- SCADA: Funguje jako SCADA kontrolní a zpracovatelský blok, který zpracovává data získaná z Koncentratoru.

Pro protokol MMS komunikace probíhala mezi Koncentrátor a HMI, kde Koncentrátor fungoval jako server a HMI jako klient. Testování ukázalo, že Raspberry Pi dokáže zpracovat až 87 236 MMS paketů za sekundu při průměrné rychlosti přenosu téměř 160 Mbit/s a využití CPU kolem 80 %. Toto ukazuje, že Raspberry Pi je schopno efektivně zvládnout vysoký objem datového provozu v reálných podmínkách ICS sítí.

GOOSE zprávy byly generovány z obou Stanice A a B a přijímány Koncentrátorem. Každé Stanice vysílalo GOOSE zprávy obsahující 195 bajtů dat, zatímco zprávy generované z Koncent-

[1] https://libiec61850.com/



Obr. 6.1: Schéma zapojení emulačních jednotek při zátěžovém testování

rátor obsahovaly 422 bajtů dat, protože zahrnovaly data z obou Stanic. Během testování dosáhla přenosová rychlost ze stanici kolem 185 Mbit/s s využitím CPU na Stanice a a B přes 80 %. Pro Koncentrátor byla přenosová rychlost přibližně poloviční, ale využití CPU pouze 15 %. Tato čísla potvrzují schopnost Raspberry Pi efektivně zvládat komunikaci pomocí GOOSE protokolu.

SV zprávy byly generovány ze Stanice a a B a přijímány Koncentrátor. Běžně jeden kanál generuje 4800 vzorků za vteřinu. Během testování SV protokolu byla dosažena přenosová rychlost přes 200 Mbit/s při obdobném využití CPU jako u GOOSE. Konkrétně, Stanice a a B generovaly zprávy o velikosti 203 bajtů (1,624 bitů), což odpovídá běžné velikosti SV zpráv v reálných podmínkách. Pokud předpokládáme, že každá SV zpráva obsahuje vzorky z jednoho kanálu a běžný kanál generuje 4800 vzorků za sekundu, pak Raspberry Pi je schopno zpracovat přibližně $((200 * 10^6)/1,624)/4800)$ 25 SV kanálů.

Výsledky testování ukazují, že Raspberry Pi je více než dostatečné pro simulaci reálných podmínek v energetických sítích a je schopné zpracovat vysoký objem datového provozu. To z něj činí ideální volbu pro testování a vývoj v oblasti kybernetické bezpečnosti.

6.2.1 Vyhodnocení komunikační kapacity testovacího prostředí s využitím teorie front pro DFD modelu vnitřní komunikace stanice

Na základě provedeného zátěžového testování emulačních jednotek byly získány datové hodnoty charakterizující přenosovou kapacitu jednotlivých protokolů (MMS, GOOSE, SV). Cílem této kapitoly je využít dříve zavedené modely teorie front (viz kapitola 3.7, 3.8 a 3.9) k analytickému vyhodnocení těchto výsledků a odvození limitních parametrů testovacího prostředí. Tato analýza slouží k posouzení schopnosti prostředí obsluhovat vícenásobné komunikační toky a dimenzovat architekturu pro scénáře s vyššími nároky na přenos dat. Výsledky zároveň poskytují vstupní informace pro návrh simulací a bezpečnostních experimentů realizovaných v dalších fázích dizertace.

GOOSE – aplikace modelu MMPP

GOOSE zprávy jsou charakteristické nepravidelným tokem řízeným událostmi. Jak bylo popsáno v kapitole 3.7, GOOSE zprávy vykazují událostně řízený, nepravidelný tok, který je možné modelovat pomocí Markovem modulovaného Poissonova procesu (MMPP). Z testovacího prostředí vychází tyto klíčové hodnoty pro Stanice jednotky:

- CPU vytížení: 82,8% a 88,9%,

- přenosová rychlost: 184,7 a 185,7 Mbit/s,
- počet paketů: 122 072 a 122 112 paketů/s.

Tyto hodnoty představují celkový datový tok 244 184 paketů/s při 185 Mbit/s a 85 % využití CPU. Nicméně tato data sama o sobě neposkytují dostatečný vhled do toho, kolik paralelních GOOSE kanálů testbed dokáže spolehlivě emulovat. Proto je potřeba znát charakteristiky jednotlivých kanálů během klidového i burst režimu. K tomuto účelu byl vybrán článek [169], kde jsou uvedeny hodnoty:

- klidový režim $\lambda_1 = 2\ zpráv/s$,
- burst režim $\lambda_2 = 500\ zpráv/s$,
- s průměrnou délkou burstu 60 ms,

které odpovídají horní hranici generování GOOSE zprav. Tyto parametry jsou použity v modelu MMPP, který umožňuje rozdělit celkový datový tok na kanály a zjistit, kolik z nich testbed skutečně simuluje během burstu:

$$\frac{244\,184 \text{ paketů/s}}{500 \text{ zpráv/s na kanál}} \approx 488 \text{ kanálů.}$$

Na základě naměřeného vytížení CPU, hlavně při 185 Mbit/s, a s ohledem na požadavky IEC 61850 (latence GOOSE < 3 ms), je vhodné emulační jednotku dimenzovat na maximálně 500 paralelních kanálů.

Sampled Values – aplikace modelu M/D/1

Přenos SV zpráv je typicky deterministický, generuje pevný objem dat ve fixních intervalech. V kapitole 3.8 byl zaveden model M/D/1, který tuto pravidelnost vystihuje přesněji než stochastické přístupy. Z naměřených hodnot z výše uvedeného testování vyšli následující hodnoty pro stanice Stanice a a Stanice B:

- CPU vytížení: 79,45 a 85,69 %,
- přenosová rychlost: 206,42 a 208,33 Mbit/s,
- počet paketů: 129 889 a 129 889 paketů/s.

Celkový počet SV paketů dosahuje hodnoty $129\,889 + 130\,456 = 260\,345$ paketů/s, při průměrné přenosové rychlosti 207 Mbit/s a průměrném zatížení CPU 83 %. Každý SV kanál standardně generuje 4800 vzorků/s (tj. 50 Hz × 96 vzorků/cyklus). Z tohoto vyplývá:

$$\frac{260\,345}{4\,800} \approx 54,2 \text{ paralelních SV kanálů.}$$

Model M/D/1 potvrzuje, že do této úrovně jsou fronty zanedbatelné, latence minimální a provoz stabilní díky deterministické povaze a nízké varianci přenosu. Dle výpočtu výsledku Emulační stanice s Raspberry Pi a libiec61850.

Dle výsledků z testování Emulační stanice s Raspberry Pi a libiec61850 dokáže simulovat maximálně 25 paralelních SV kanálů, což je významně méně než modelované maximum cca 54 kanálů, ale plně postačuje pro většinu aplikací typických zařízení v elektroenergetice. Rozdíl mezi teoretickou a reálnou hodnotu může být způsoben neefektivní implementací pomocí výše zmíněné knihovny pro standart IEC 61850 na jednotce Raspberry Pi.

MMS – aplikace modelu M/M/1

Zpracování MMS zpráv mezi jednotkami Koncentrátor a HMI odpovídá režimu klient–server, jak bylo uvedeno v kapitole 3.9. Komunikaci lze efektivně modelovat pomocí fronty M/M/1, kde příchody požadavků (MMS požadavků) i doba obsluhy mají exponenciální charakter. Z výsledku

testová emulační jednotky postavenou na Raspberry Pi, které je uvedeno výše, vyplývají tyto klíčové hodnoty:

- příchozí MMS požadavky: $\lambda \approx 87\ 236$ paketů/s,
- přenosová rychlost: 159,24 Mbit/s,
- CPU zatížení přijímače : 80,9 %.

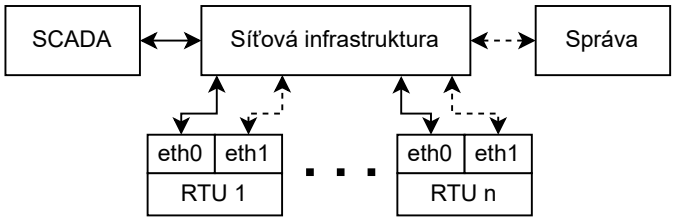
Co se týče obslužné kapacity μ, můžeme vycházet z toho, že server je pod hranicí nasycení – zatížení systému (utilizace) je tedy:

$$\rho = \frac{\lambda}{\mu} \approx 0{,}8 \quad \Longrightarrow \quad \mu \approx \frac{\lambda}{0{,}8} \approx 109\,045 \text{ paketů/s}.$$

Hodnota potvrzuje, že Raspberry Pi s libiec61850 funguje v režimu M/M/1 se zatížením menším než 1 a tedy v oblasti stabilního provozu (platí pro M/M/1 $\rho < 1$). To znamená, že za provozních podmínek může systém bezpečně zvládnout výrazně větší počet požadavků nebo více současných MMS spojení, aniž by došlo k rapidnímu nárůstu latencí. Díky výsledkům je možné konstatovat, že Raspberry Pi s použitou implementací MMS má dostatečnou kapacitu i pro zvýšený počet klientů.

6.2.2 Analýza DFD modelu vzdálené komunikace na základě IEC 104

Kapitola obsahuje měření a analýzu komunikace mezi SCADA a RTU na základě definovaného DFD modelu pro vzdálenou komunikaci. Komunikace probíhá pomocí IEC 60870-5-104 a to v nezabezpečené verzi, tak i s TLS 1.1, dle IEC 62351. Zjednodušení testovacím prostředí je zobrazeném na obrázku 6.2. Jak již bylo zmíněno, tak testovacím prostředí byla implementována zabezpečená i nezabezpečená varianta komunikace, kde samotný způsob přenosu dat je prakticky totožný. Jediným rozdílem je úvodní fáze navazování zabezpečeného spojení pomocí TLS handshake, během kterého dochází k výměně certifikátů a nastavení parametrů zabezpečení. Po navázání spojení může být zahájen vlastní přenos dat.



Obr. 6.2: Testovací prostředí pro analýzu IEC 104

Režie způsobené přidáním TLS jsou zobrazeny v tabulce 6.3, kde lze vidět, že až na velikost řídicího paketu má TLS varianta minimální dopad. Řídicí data v tabulce představují zprávy protokolu sloužící k navázání nebo udržení spojení a mají nepravidelný výskyt. Naproti tomu aplikační data přenášejí samotné užitečné informace, například hodnoty monitorovaných veličin. Druhým sledovaným parametrem bylo zpozdění způsobená zpracováním zprávy. Tato latence odpovídá časovému rozdílu mezi okamžikem vzniku události a přijetím zprávy dohledovým centrem. Konkrétně byla vypočtena jako rozdíl mezi časovou značkou zprávy generované emulovanou stanicí a časem, kdy byla tato zpráva zaznamenána v logovacím systému centrály. i zde je patrné, že dopad IEC 104 v zabezpečené verzi je minimální.

V rámci testování byla provedena série měření zaměřených na maximální propustnost mezi jednotlivými prvky testovacího prostředí. Konkrétně šlo o propojení mezi dohledovým centrem

Tab. 6.3: Dopad režií při přidání TLS k IEC 104.

	IEC 608750-5-104		**TLS 1.1**	
Data	Velikost paketu [B]	Zpoždění [ms]	Velikost paketu [B]	Zpoždění [ms]
Řídicí	493	110	1 948	810
Aplikační	1 225	1,28	1 164	1,48

(OpenMUC), řídicí aplikací (Správa) a testovacími stanicemi (RTU). K měření datové propustnosti byl použit nástroj **iperf**, který slouží ke zjištění síťového výkonu bez výrazného zatížení samotného zařízení.

Výsledky těchto měření poskytují užitečné informace o efektivitě komunikace v rámci infrastruktury testbedu. Pro každé měření byla provedena sada tří desetiminutových testů, a to jak s využitím TCP, tak i UDP přenosu. Výsledky těchto testů jsou uvedeny v tabulce 6.4.

Tab. 6.4: Propustnost mezi prvky testovacího prostředí

	Typ komunikace	**OpenMUC RTU**	**Správa RTU**	**RTU RTU**
UDP	**Přenos dat** [GB]	$18,7 - 18,8$	$16,3 - 16,8$	$18,5 - 18,7$
	Šířka pásma [Mb/s]	269	$233 - 241$	$264 - 268$
	Přenos datagramů [-]	$13,7 \cdot 10^6$	$11,8 - 12,2 \cdot 10^6$	$13,4 \check{} 13,6 \cdot 10^6$
	Ztracené datagramy [-]	$0 \check{} 4$	$51 \check{} 339$	$41 - 127$
	Míra ztráty [%]	$0 - 0,0003$	$0,004 - 0,028$	$0,003 - 0,009$
	Zpoždění [ms]	$0,632$	$0,255$	$1,140$
	Kolísání [ms]	$0,121 - 0,132$	$0,058 \check{} 0,151$	$0,049 \check{} 0,122$
TCP	**Přenos dat** [GB]	$19,2 \check{} 19,3$	$14,8 \check{} 15,5$	$18,3 \check{} 18,4$
	Šířka pásma [Mb/s]	275	$212 \check{} 221$	$262 \check{} 263$

Při každém testu bylo přeneseno přibližně 18 GB testovacích dat mezi jednotlivými stanicemi, a to jak v režimu TCP, tak UDP. Průměrná přenosová rychlost se pohybovala kolem 260 Mb/s, což je v kontextu průmyslových aplikací nadstandardní hodnota. V běžném průmyslovém prostředí jsou zařízení od výrobců jako ABB nebo Siemens vybavena převážně 100Mb/s rozhraními, takže dosažené přenosové rychlosti jsou více než dostatečné pro optimální provoz průmyslových systémů. Z měření vyplynulo, že spojení typu „Správa – RTU“ vykazuje přibližně o 20 % nižší rychlosti než ostatní testované kombinace. Tento rozdíl však není kritický, neboť se jedná o vedlejší komunikační kanál určený pro správu testbedu a nemá vliv na hlavní provozní funkce systému.

Součástí měření bylo také sledování míry ztrátovosti paketů. Tato hodnota se pohybovala v řádu tisícin procent přenesených dat, což se dá považovat za zanedbatelné. Nejhorších výsledků opět dosáhlo spojení „Správa – RTU“, nicméně i zde byla ztrátovost zanedbatelná a nijak neovlivnila funkčnost jednotlivých částí testbedu.

Neméně důležitým parametrem testovacího prostředí je také komunikační zpoždění mezi stanicemi. Jedná se o dobu, která uplyne od odeslání požadavku jedním zařízením po přijetí odpovědi druhým zařízením. Tento proces zahrnuje přenos dat napříč různými síťovými protokoly a médii (např. kabelové či bezdrátové připojení). Zpoždění může být ovlivněno mnoha faktory, jako je vzdálenost mezi zařízeními, propustnost sítě nebo množství přenášených dat. Je důležité sledovat a minimalizovat zpoždění, protože ovlivňuje kvalitu služeb a aplikací přenášených po síti. Z výsledků měření vyplývá, že největší zpoždění nastává při vzájemné komunikaci mezi stanicemi.

To může být způsobeno vyšším zatížením okrajového přepínače, který obsluhuje více než dvacet zařízení současně. Přesto však naměřené hodnoty zůstaly v bezpečných mezích a nepřekročily maximální mez pro optimální provoz stanovenou na 3 ms, tedy nejnižší mez podle typu zpráv dle normy IEC 61850-5 [127]. V rámci testu byla sledována také proměnlivost zpoždění, tzv. jitter, jehož hodnoty se pohybovaly mezi 0,05 a 0,15 ms. Tyto výsledky lze považovat za dostatečné a nepředstavují žádné omezení pro provoz testbedu.

Vyhodnocení komunikační kapacity testovacího prostředí s využitím teorie front pro DFD model vzdálené komunikace

V této části je analyzována kapacita testovacího prostředí pro přenosové scénáře založené na vzdálené komunikaci mezi SCADA a RTU, která využívá protokol IEC 60870-5-104. Tato komunikace probíhá na bázi klient–server v režimu, kdy přicházejí jednotlivé požadavky ze SCADA systému a jsou následně zpracovávány vzdálenou RTU. Tento přenosový model lze formálně vyjádřit jako systém M/M/1, kde jak příchod požadavků, tak doba jejich obsluhy mají exponenciální rozdělení.

Z pohledu DFD odpovídá tento přenos spojení mezi centrálním dohledovým systémem a emulovanou RTU jednotkou, implementovanou na platformě Raspberry Pi 3B+. Tato jednotka má vzhledem ke své konstrukci (LAN připojené přes USB 2.0 sběrnici) reálnou maximální propustnost přibližně 300 Mbit/s, což představuje přirozené omezení přenosového výkonu.

Na základě výsledků testování (viz tabulky 6.3 a 6.4) lze odhadnout příchozí datový tok jako $\lambda \approx 30\,000$ paketů za sekundu. Tato hodnota zohledňuje velikost aplikačních paketů (1200 B), skutečnou přenosovou rychlost kolem 260 Mb/s a datovou režii na transportní vrstvě.

Obslužnou dobu jednoho požadavku nelze stanovit pouze ze zpoždění celé zprávy, neboť to zahrnuje i přenosové a síťové zdržení. Proto byla zvolena konzervativní hodnota 3 ms dle normy IEC 61850-5 jako horní hranice latence pro časově kritické zprávy (např. GOOSE). Tuto hodnotu použijeme jako realistický odhad doby zpracování jednoho požadavku na straně zařízení:

$$\mu = \frac{1}{3 \times 10^{-3}} = \frac{1}{0{,}003} = 333\,333 \text{ paketů/s}.$$

Z toho vyplývá míra využití systému:

$$\rho = \frac{\lambda}{\mu} = \frac{30\,000}{333\,333} \approx 0{,}09.$$

Výpočet podle modelu M/M/1 ukazuje, že emulovaná jednotka je z hlediska zpracování požadavků zatížena pouze z 9 %, což potvrzuje stabilní provoz bez zahlcení parseru nebo komunikační knihovny. Je však důležité rozlišovat mezi výpočetní kapacitou systému a fyzickou propustností síťového rozhraní. i když je využití CPU a obsluhy nízké, dosažená přenosová rychlost kolem 260 Mbit/s odpovídá téměř maximální reálné kapacitě síťového rozhraní Raspberry Pi 3B+ (kvůli omezení danému USB 2.0 sběrnicí). Další nárůst provozu by tak vedl primárně k zahlcení přenosové vrstvy, nikoli výpočetní části systému.

Z hlediska modelu DFD lze tuto část infrastruktury považovat za dimenzovanou s rezervou z hlediska výpočetní kapacity, avšak limitovanou fyzickými možnostmi použité platformy. Výsledky dále potvrzují, že i při implementaci TLS dle IEC 62351 zůstává dopad na přenosovou kapacitu minimální, přičemž kritické parametry jako latence a jitter se pohybují hluboko pod mezními hodnotami stanovenými normami.

6.3 Komplexní testovací prostředí

V této části je navázáno na předchozí návrhové a implementační kroky a představeno komplexní testovací prostředí, které pokrývá obě definované komunikační vrstvy (vzdálenou i vnitřní) a integruje je do ucelené architektury. Toto prostředí, označované jako **BUTENET**, které je podrobně popsané v článku [4], rozšiřuje předchozí koncepci o fyzické komponenty, virtualizované systémy a realistické scénáře provozu i kybernetických incidentů. V následujících částech jsou podrobně popsány jeho architektura, realizované scénáře, nasazení fyzických zařízení i způsob propojení s existujícími emulačními prvky.

BUTENET je navržen jako hybridní prostředí kombinující fyzické, emulované a virtualizované prvky, které dohromady umožňují realistickou simulaci provozu v elektrizační soustavě. Architektura tohoto testbedu vychází z dvouvrstvého návrhu definovaného pomocí DFD modelů – tedy jak z pohledu horizontální komunikace uvnitř elektrické stanice (procesní, staniční a řídicí vrstva), tak z pohledu vertikální komunikace mezi dispečerským centrem, SCADA systémem a vzdálenými zařízeními (RTU, IED).

Základními stavebními prvky prostředí jsou jednodeskové počítače Raspberry Pi, které zajišťují emulaci jednotlivých zařízení stanice, dále virtualizované servery pro běh SCADA/HMI a integrační uzly, a konečně reálné fyzické prvky (např. IED od ABB či Siemens), které rozšiřují prostředí o autentické chování skutečných zařízení. Všechny komponenty jsou propojeny do jednotné infrastruktury, která umožňuje testování běžných provozních stavů, řízených přechodů, poruchových stavů i kybernetických útoků na úrovni datové i řídicí vrstvy.

V následujících podkapitolách je detailně popsána architektura testbedu BUTENET, přehled použitých zařízení a softwaru, způsob propojení jednotlivých vrstev a realizované scénáře provozu a incidentů.

6.3.1 Využití testbedu BUTENET

Testovací prostředí BUTENET bylo navrženo jako multifunkční platforma podporující široké spektrum aktivit v oblasti výzkumu, vývoje a vzdělávání zaměřeného na kyber-fyzické systémy elektroenergetiky. Jeho architektura umožňuje jak realistickou emulaci standardního provozu, tak experimentální simulaci poruchových a bezpečnostních stavů, a to v prostředí, které je kontrolované a plně replikovatelné. Využití testbedu lze rozdělit do čtyř hlavních oblastí: vzdělávání, bezpečnostní analýzy, generování provozních dat a aplikovaný výzkum.

1. Vzdělávání a odborná příprava BUTENET poskytuje technicky detailní prostředí pro výuku a školení odborníků v oblasti chytrých sítí a jejich zabezpečení. Díky kombinaci reálných zařízení, emulovaných komponent a virtualizovaných prvků je možné realizovat komplexní výukové scénáře pokrývající celé spektrum činností – od konfigurace síťových segmentů a zařízení (např. IED, RTU, SCADA), přes analýzu přenosových protokolů (např. MMS, GOOSE, SV, IEC 104) až po reakci na provozní události či kybernetické incidenty. Praktická interakce s komponentami systému podporuje hlubší porozumění strukturám, závislostem a provozním specifikům elektroenergetické infrastruktury.

2. Analýza bezpečnostních scénářů Architektura testbedu umožňuje definici a spuštění simulačních scénářů zaměřených na bezpečnost komunikační infrastruktury a řídicích prvků. Lze simulovat útoky typu DDoS, spoofing, replay nebo manipulaci s GOOSE/MMS zprávami a hodnotit jejich dopad na provozní chování systému. BUTENET umožňuje sběr a vyhodnocení technických metrik

(latence, ztrátovost, zatížení CPU, chybovost) i funkčních dopadů (např. aktivace ochran, nesprávné reakce SCADA) v závislosti na typu a rozsahu incidentu. Tyto scénáře mohou být využity i pro testování robustnosti a efektivity bezpečnostních opatření, jako jsou šifrování, autentizace, redundantní přenosy nebo detekční systémy.

3. Generování provozních dat a ověřování hypotéz Díky možnosti řízeného ovládání vstupních veličin (napětí, proud, výkon, kmitočet, stavové proměnné) a jejich reprezentace v komunikačních protokolech je možné na BUTENETu generovat realistická datová streamy včetně typických i nestandardních provozních stavů. Tato data slouží jak pro trénink a testování algoritmů strojového učení (např. detekce anomálií, predikce selhání), tak pro validaci matematických modelů (např. modely teorie front, řízení stability či toků výkonu). Oproti zcela simulovaným systémům poskytuje BUTENET vyšší míru věrohodnosti dat díky kombinaci reálných zařízení, emulace a řízené deterministické manipulace s parametry.

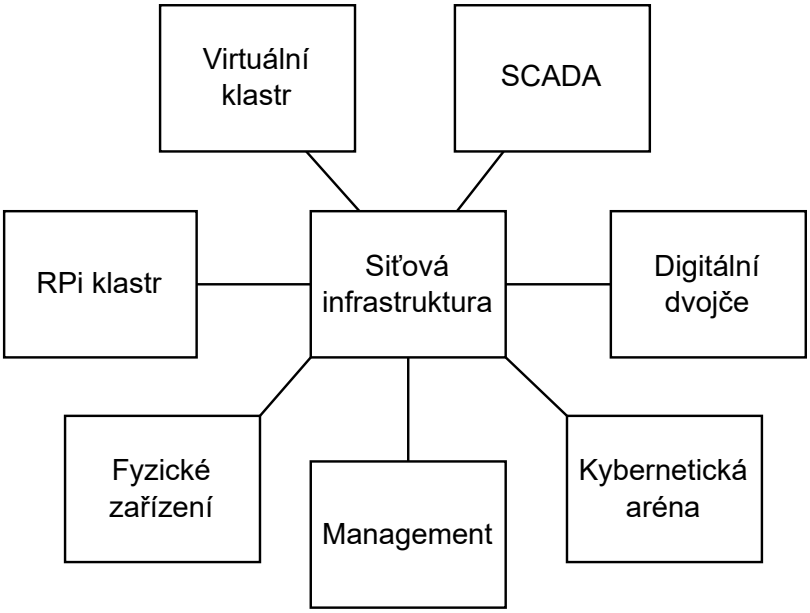
4. Výzkum a vývoj v oblasti chytrých sítí BUTENET představuje platformu pro vývoj, testování a validaci nových konceptů v oblasti řízení, komunikace a zabezpečení v elektroenergetických sítích. V rámci prostředí je možné implementovat nové protokolové zásahy, nasazovat alternativní řídicí logiky, testovat decentralizované algoritmy řízení nebo ověřovat interoperabilitu komponent různých výrobců. Díky možnosti připojení na kybernetickou arénu lze testbed využít také pro výzkum odolnosti systémů vůči komplexním útokům včetně koordinovaných vícestupňových scénářů. Z hlediska metodiky výzkumu nabízí BUTENET možnost opakovatelných experimentů s kontrolovanými vstupními podmínkami a přesně měřit výstupní charakteristiky systému.

6.3.2 Architektura testovacího prostředí BUTENET

Architektura testbedu BUTENET je navržena jako modulární, škálovatelné prostředí, které tvoří základní páteř pro realizaci kyber-fyzických scénářů v oblasti elektroenergetiky. Jeho jádrem je síťová infrastruktura, která propojuje fyzické, emulované i virtualizované komponenty a umožňuje jejich koordinaci při simulaci běžných i poruchových stavů. Základní architektura prostředí je znázorněna na obrázku 6.3.

Testovací prostředí BUTENET zahrnuje následující základní komponenty:

- **RPi klastr**: tvořen 50 jednodeskovými počítači Raspberry Pi, které jsou navzájem propojeny pomocí přepínačů a směrovačů. Tento klastr slouží pro realizaci emulačních jednotek popsaných v předchozí kapitole. Jednotlivé RPi emulují zařízení typu MU, IED, RTU a jsou schopny generovat síťový provoz v souladu se standardy IEC 61850 a IEC 60870-5-104.
- **Virtuální klastr**: sestává ze serverů s nainstalovanými virtualizačním nástroje Vmware, který umožňuje provozovat inženýrské stanice, HMI rozhraní, útočící uzly nebo síťových sond. Virtuální klastr zajišťuje flexibilitu při nasazování scénářů, změně topologie a přidávání nových komponent.
- **SCADA systém**: představuje dohledové centrum založené na open-source platformě OpenMUC. Tento systém zajišťuje sběr, zobrazení a historizaci dat z emulovaných i fyzických zařízení, podporuje protokoly MMS a IEC 104 a umožňuje definovat odezvy na události v systému.
- **Management**: centrální komponenta určená pro správu a orchestraci prostředí. Zahrnuje správu síťových konfigurací, monitoring zátěže jednotlivých uzlů, vzdálený přístup k zařízení.



Obr. 6.3: Základní architektura prostředí BUTENET

- **Fyzická zařízení**: do prostředí jsou integrovány i reálné průmyslové komponenty jako jsou slučovací jednotky (např. ABB SMU615), RTU a další ochranné prvky (např. ABB REF615). Tato zařízení slouží k validaci výsledků emulace a zvyšují věrohodnost simulovaných scénářů.

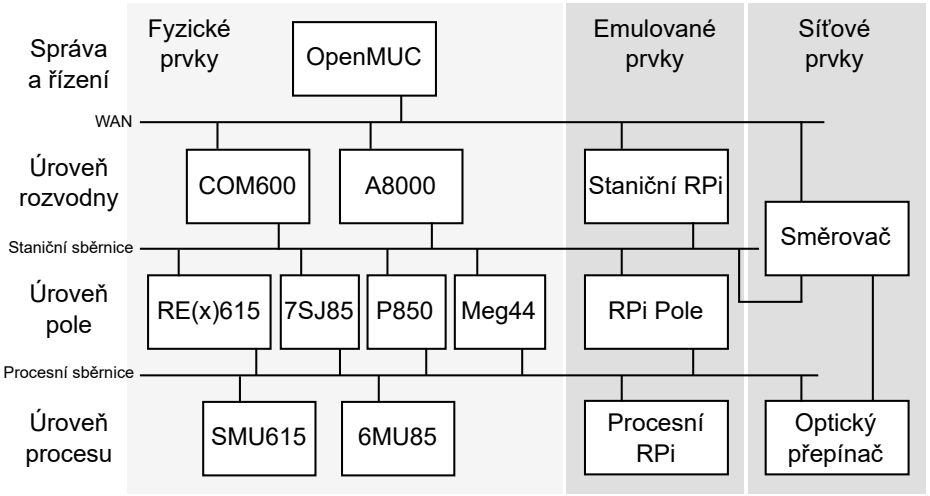
Nad rámec této základní infrastruktury je možné na prostředí BUTENET napojit další systémy:

- **Kybernetická aréna BUTCA**[2] – samostatné platforma pro trénování v oblasti kybernetické bezpečnosti. BUTENET je prostřednictvím síťové infrastruktury propojen na do BUTCA, díky čemuž je možné realizovat věrohodnější a reálnější scénáře pro edukaci.
- **Digitální dvojče** [41] [1] – dynamický model systému, který umožňuje simulovat provoz a chování elektroenergetických komponent propojených s BUTENETem. Při propojení s testbedem je možné validovat vliv změn, incidentů nebo stavových odchylek na systém jako celek, případně vytvářet prediktivní scénáře.

6.3.3 Implementace elektrické stanice

Elektrická stanice představuje klíčový prvek přenosové a distribuční soustavy, který zajišťuje transformaci mezi napěťovými hladinami, kompenzaci jalového výkonu a přepojování vedení. V souladu se standardem IEC 61850 je její architektura členěna do tří hierarchických úrovní: procesu, pole a rozvodny, jak je uvedeno na obrázku 6.4. Implementace elektrické stanice se skládá ze dvou částí a to fyzická s reálnými průmyslovými zařízeními a emulovaná stanice používá dříve popsanou Emulační jednotku.

[2] https://www.utko.fekt.vut.cz/butca-kyberneticka-arena



Obr. 6.4: Struktura implementace elektrické stanice

Fyzická část elekrické stanice

Úroveň procesu Tato úroveň představuje nejnižší vrstvu elektrické stanice, ve které dochází ke kontaktu s napěťovými a proudovými veličinami. Fyzická varianta využívá slučovací jednotky ABB SMU615 a Siemens SIPROTEC 6MU85, které přenášejí měřená data ve formátu Sampled Values a zároveň vysílají kritické zprávy pomocí GOOSE protokolu. Konfigurace a dohled nad zařízeními je realizován pomocí MMS.

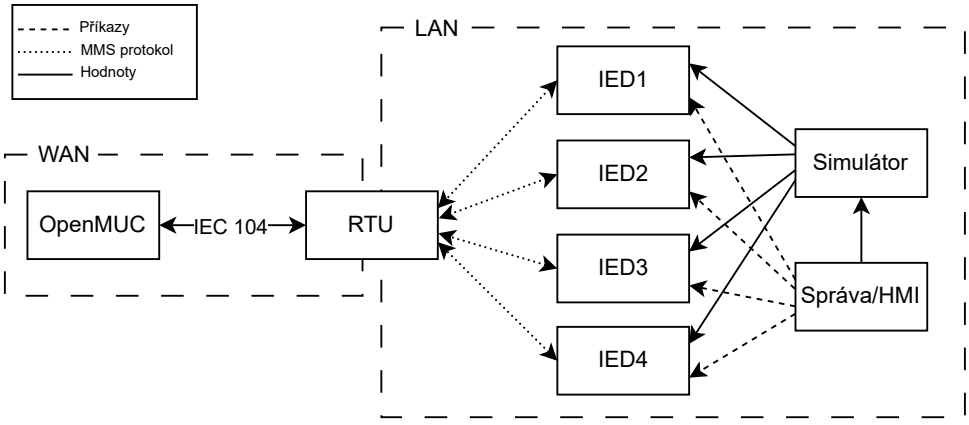
Úroveň pole Tato úroveň zajišťuje první úroveň zpracování a interpretace dat z procesní vrstvy. Fyzická část zahrnuje nasazení ochranných relé ABB RE(X) - REF615, REC615, RER615 a Siemens SIPROTEC 7SJ85. Kromě IEC 61850 podporují i další protokol IEC 104, což umožňuje flexibilní konfiguraci a adaptaci na různá prostředí. Pro potřeby monitorování kvality elektrické energie jsou dále nasazeny analyzátory PQ monitor MEg44PAN a Siemens SICAM P850, které poskytují detailní měření parametrů napětí, proudu a výkonu a podporují integraci do nadřazených systémů prostřednictvím standardizovaných komunikačních protokolů jako je IEC 61850 a IEC 60870-5-104.

Úroveň rozvodny Tato úroveň zajišťuje centrální sběr, vizualizaci a předávání dat. Ve fyzické variantě jsou využita zařízení ABB COM600 a Siemens SICAM A8000, která přijímají data z IED a zajišťují jejich další přenos do nadřazeného řídicího centra.

Emulovaná část elektrické stanice

Architektura je rozdělena do dvou částí LAN a WAN, jak je zobrazeno na obrázku 6.5. Část WAN je spojení mezi RTU jednotkou a SCADA OpenMUC. Komunikace probíhá pomocí protokolu IEC 60870-5-104. LAN část je komplexnější a zahrnuje několik prvků, které spolu komunikují pomocí protokolů MMS, GOOSE a SV. IED zařízení v navrženém systému jednotlivé uzly rozvodny, které vykonávají ochranné a řídicí funkce na základě vstupních dat simulátoru. Každé IED běží jako samostatná emulační jednotka, která simuluje buď zařízení na úrovní pole nebo na procesní úrovni, dle obrázku 6.4. RTU na pomezí LAN a WAN sítě potom představuje zařízení na úrovni

rozvodny. Všechny části jsou propojeny pomocí metalických směrovačů. Bližší popis jednotlivých prvků emulované části elektrické stanice jsou popsány níže.



Obr. 6.5: Architektura emulované části elektrické stanice

Simulátor Simulátor tvoří nejnižší součást systému určenou pro generování fyzikálních veličin. Jeho hlavním úkolem je vytvářet realistické třífázové napěťové a proudové signály a následně je distribuovat k jednotlivým IED zařízení. V rámci obrázku je distribuce těchto signálů zobrazena plnou čarou a legendě označena jako "Hodnoty".

Simulátor také emuluje stavy spínačů a poruchové situace, což umožňuje testování různých provozních scénářů bez nutnosti zásahu do reálné infrastruktury. Tato funkcionalita je realizována pomocí knihovny PySpice[3], která umožňuje definovat elektrický obvod, simulovat jeho chování a exportovat vypočtené hodnoty v čase.

Samotná komunikace mezi simulátorem a ostatními komponentami probíhá prostřednictvím proprietárního aplikačního protokolu a slouží čistě výměny hodnot generovaných veličin. Tato komunikace však nepředstavuje skutečný přenos po síti (neimituje žádný energetický protokol), nýbrž pouze výměnu dat v rámci fyzického segmentu, která by za běžného provozu byla realizována prostřednictvím měřicích transformátorů a svorek.

Správa/HMI Správa/HMI slouží jako uživatelské rozhraní pro řízení a vizualizaci stavu simulovaného systému. V roli lokálního ovládacího panelu, umožňuje operátorovi provádět základní operace jako zapnutí, vypnutí, reset nebo změnu režimu jednotlivých spínacích prvků, případně úpravu vstupních parametrů simulátoru.

HMI je implementováno jako webová aplikace přístupná z běžného prohlížeče, zajišťující obousměrnou komunikaci mezi uživatelem, simulátorem a jednotlivými IED zařízeními. Příkazy generované uživatelem jsou předávány simulátoru, který je následně distribuuje příslušným IED podle logických vazeb a synchronizačních mechanismů definovaných v konfiguraci (např. prostřednictvím SCL souborů).

IED 1 Zařízení IED 1 reprezentuje řídicí logiku pro ovládání výkonových spínacích prvků a dle obrázku 6.4 představuje Procesní RPi. IED simuluje následující logické uzly, které jsou četně jejich

[3]https://pypi.org/project/PySpice/

označení dle standardu IEC 61850 a použitého datového typu, podrobně popsány v příloze C v tabulce C.1 a C.2:

- **XCBR (Circuit Breaker)** simuluje výkonový vypínač, který na základě přijatých příkazů mění svůj stav a následně hlásí polohu kontaktů.
- **CSWI (Switch Controller 1 a 2)** zajišťuje ovládání spínačů; přijímá rozkazy z HMI či SCADA a řídí odpovídající XCBR uzly.
- **CILO (Interlocking)** realizuje bezpečnostní blokace mezi prvky, aby se zabránilo nebezpečnému nebo nevhodnému sepnutí vypínače při nevyhovující topologii.
- **LLN0 (Logical Device)** obsahuje základní konfigurační údaje a stavové proměnné celého zařízení.
- **LPHD (Physical Device)** popisuje fyzickou vrstvu zařízení, včetně napájení a diagnostických informací.
-

IED 2 Zařízení IED 2 (dle obrázku 6.4 se jedná o RPi pole) plní v modelu rozvodny ochrannou funkci, konkrétně simulaci nadproudové ochrany. Simuluje následující logické uzly, které jsou včetně jejich označení dle standardu IEC 61850 a použitých datových typů podrobně popsány v příloze C v tabulce C.3 a C.4:

- **PTOC (Time Overcurrent Protection)** zajišťuje detekci nadproudových stavů na základě vstupních proudových hodnot; při překročení nastavených mezí generuje výstražné nebo vypínací signály.
- **PTRC (Protection Trip Conditioning)** vyhodnocuje výsledky ochranných funkcí a vytváří binární signál pro vypnutí zařízení.
- **GGIO (Generic Process I/O)** slouží pro přímé mapování binárních vstupů a výstupů; zajišťuje interakci se simulovaným systémem bez nutnosti specifických logických vazeb.
- **LLN0 (Logical Node Zero)** obsahuje základní konfigurační informace a řídicí proměnné specifické pro dané IED.
- **LPHD (Logical Physical Device)** reprezentuje fyzickou instanci zařízení včetně jeho diagnostiky, napájení a hardwarového stavu.

IED 3 a 4 Zařízení IED 3 a IED 4 (dle obrázku 6.4 se jedná o Procesní RPi) představují měřicí úroveň systému. Obě zařízení sdílejí téměř identickou architekturu a jejich hlavním účelem je poskytování vstupních vzorkovaných hodnot Sampled Values. Napojení na systém je realizováno prostřednictvím následujících logických uzlů, které včetně označení dle IEC 61850 a použitých datových typů jsou podrobně popsány v příloze C v tabulce C.5 a C.5:

- **MMXU (Measurement Unit)** provádí výpočet efektivních hodnot napětí a proudu (RMS), přepočítává statistiky a připravuje data pro publikaci.
- **TCTR (Current Transformer) a TVTR (Voltage Transformer)** emulují chování proudových a napěťových transformátorů, které mění velikost signálů na úrovni vhodnou pro měření a následnou distribuci v systému.
- **LLN0 (Logical Node Zero)** koordinuje interní funkce zařízení, zajišťuje synchronizaci měření a zpracování dat před jejich odesláním.

RTU Zařízení RTU v navržené architektuře funguje jako klíčový komunikační prvek, kde dle obrázku 6.4 se jedná o Staniční RPi. RTU zajišťující propojení mezi LAN rozvodny a WAN, která obsahuje SCADA OpenMUC. V této roli plní RTU funkci brány s důrazem na kybernetickou bezpečnost a hlediskem kontroly datových toků mezi zónami s odlišnou úrovní důvěry.

Z hlediska funkčnosti zastává RTU obousměrný protokolový překladač pro zprávy GOOSE, SV a MMS, které překládá na protokol IEC 60870-5-104. Specificky RTU sbírá data z IED (GOOSE, MMS, SV), převádí je do formátu vhodného pro IEC 104 a odešle je do dispečerského systému. Naopak přijímá řídicí příkazy z nadřazeného systému, mapuje je na MMS/GOOSE a distribuuje zpět do příslušných IED.

Realizace je založena na mapovacím mechanismu, který překládá datové body definované ve standardu IEC 61850-80-1 do adresního prostoru a typových formátů protokolu IEC 104. V tabulce C.6 v příloze C jsou uvedeny klíčové proměnné (včetně datových typů, IOA adres a přenášených významů), vybrané kvůli svému významu pro řízení a monitorování. Tato sada je dostačující pro správnou funkčnosti převodu, aniž by bylo nutné mapovat celý datový model.

U IED 1 a IED 2, které obsahují binární ovladatelné prvky (např. pozice vypínače), byly hodnoty mapovány jako double-point commands (DPC). Pro přenos byly využity odpovídající typy zpráv dle IEC 104:

- Odpověď na požadavek: M_DP_NA_1 (typ 3)
- Spontánní zasílání: M_DP_TB_1 (typ 31)
- Jednoduchý požadavek: C_DC_NA_1 (typ 46)
- Požadavek s časovou značkou: C_DC_TA_1 (typ 59)

Pro zařízení IED 3 a IED 4, která přenášejí měřené analogové hodnoty (např. proudy a napětí z MMXU, TCTR nebo TVTR), byly hodnoty mapovány jako měřené analogové hodnoty s využitím těchto typů:

- Odpověď na požadavek: M_ME_NC_1 (typ 13)
- Spontánní zasílání: M_ME_TF_1 (typ 36)

6.3.4 SCADA/HMI - OpenMUC

Po centrální řízení, monitoring a vizualizaci provozu celého testbedu bylo zvoleno řešení OpenMUC[4], což je otevřený a modulární SCADA rámec vyvinutý na Institutu Fraunhofer ISE. OpenMUC je založen na jazyce Java a architektuře OSGi, což umožňuje jednoduché rozšiřování a úpravy podle konkrétních scénářů (např. protokoly, logování, HMI). Výhodou OpenMUC je jeho open-source kód, modulární návrh a flexibilita přizpůsobení specifickým potřebám. Platforma umožňuje:

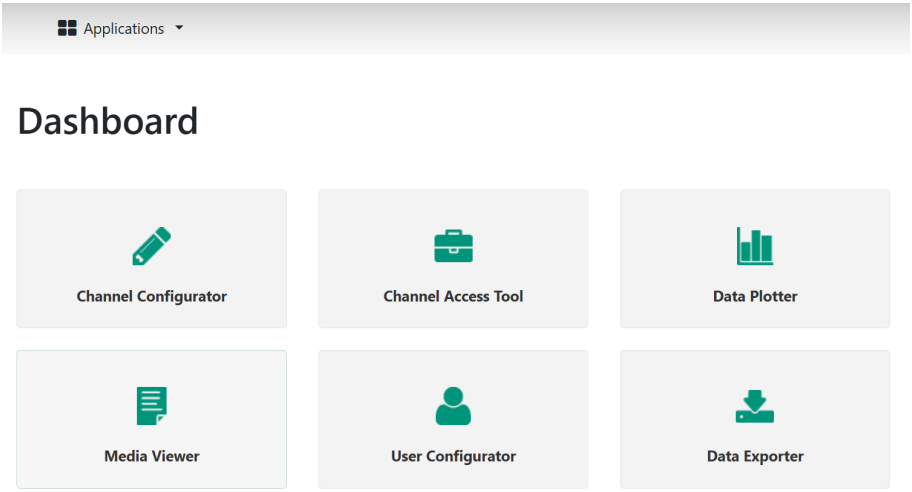
- sledovat a ovládat zařízení v reálném čase,
- sbírat data a generovat přehledy pro řízení energetických a průmyslových systémů,
- přijímat a zpracovávat data ze všech komponent testovacího prostředí.

Uživatelské rozhraní

OpenMUC poskytuje WebUI, což je modulární webové rozhraní, kde se po přihlášení objeví rozhraní pro konfiguraci, vizualizaci a ověřování datových kanálům, jak je zobrazeno na obrázku 6.6.

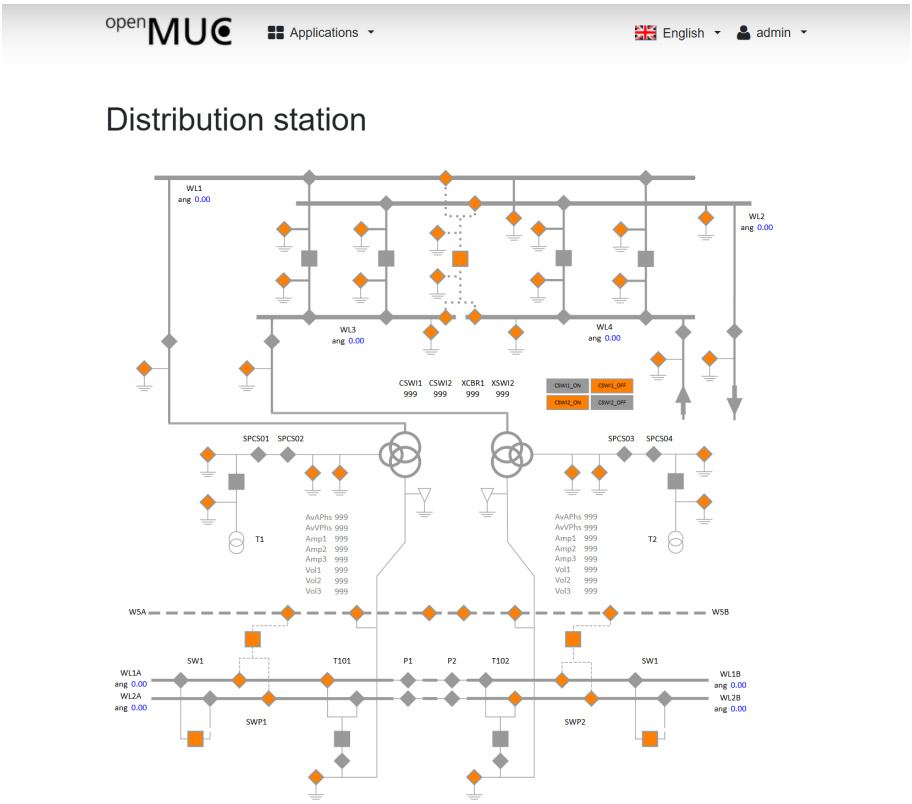
- **Channel Configurator**: Konfigurace a správa zařízení a jejich hodnot (kanálů).
- **Channel Access Tool**: Umožňuje v reálném čase zobrazit aktuální hodnoty kanálů a zadávat řídicí příkazy (např. ovládání XCBR) pro testování odezvy systémů.
- **Data Plotter**: Grafická vizualizace časových řad dat z kanálů.
- **Media Viewer**: Zobrazení multimediální podpory jako schémata a obrázky rozvodny v kontextu zařízení či kanálů.
- **User Configurator**: Správa uživatelských účtů a přístupových práv.
- **Data Exporter**: Export historických dat či PCAP záznamů.

[4] https://www.openmuc.org/



Obr. 6.6: Zakládaní prvky rozhraní OpenMUC po přihlášení

Díky modulární OSGi architektuře je možné vytvářet a přidávat další pluginy dle potřeby, což umožňuje flexibilně rozšiřovat platformu například o nové vizualizační panely či analytické nástroje, které je možné připojit do hlavní nabídky a tak k tomu jednoduše přistupovat. Příkladem může být HMI panel zobrazený na obrázku 6.7, kde je vidět vizualizace prvků emulované elektrické stanice popsané výše.



Obr. 6.7: HMI panel emulované elektrické stanice

6.3.5 Scénáře elektrizační soustavy

Součástí navržené architektury testbedu je i možnost simulace provozu přenosové nebo distribuční elektrizační soustavy pomocí zařízení typu RTU ve spojení s dohledovým centrem postaveným na platformě OpenMUC. Každé RTU zde vystupuje jako samostatná elektrická stanice (například rozvodna či transformační uzel) a zajišťuje generování stavových a měřených hodnot v souladu s protokolem IEC 60870-5-104, který slouží pro komunikaci se SCADA systémem.

Zásadní výhodou tohoto přístupu je, že není nutné detailně modelovat vnitřní strukturu rozvodny (např. procesní nebo staniční úroveň) – scénáře jsou generovány přímo na úrovni RTU, čímž lze efektivně simulovat rozsáhlou topologii elektrizační soustavy s minimálním počtem zařízení. RTU umožňuje provoz čistě v režimu IEC 104 serveru, přičemž simulované stavy a měřené veličiny jsou přímo přenášeny do systému OpenMUC, kde jsou dále zpracovávány a vizualizovány.

V rámci testovacích scénářů je však možné některé vybrané stanice nahradit reálnou (fyzickou nebo emulovanou) implementací elektrické stanice dle modelu IEC 61850. Tím lze docílit komplexnější interakce – například vygenerování poruchového stavu na procesní úrovni jedné stanice (např. zkrat na výstupu) může vyvolat reakci jiné stanice reprezentované pouze RTU modelem (např. aktivaci ochran nebo změnu provozního režimu).

Díky tomuto flexibilnímu přístupu lze snadno sestavit simulace pokrývající různé typy provozních i mimořádných událostí v rámci elektrizační soustavy České republiky, a to s vysokou mírou realismu a při současném zachování technické jednoduchosti.

V testovaném prostředí je definovano pět základních scénářů, které pokrývají nejčastější provozní stavy v přenosových a distribučních rozvodnách: standardní provoz, nestabilita napětí (podpětí nebo přepětí), přetížení (nadproud), zkrat (s obnovou a výpadkem) a běžné manipulační zásahy (servisní). První čtyři scénáře simulují nejpravděpodobnější situace, jaké mohou v reálném provozu nastat, zatímco pátý slouží pro základní servisní postupy. Všechny scénáře jsou realizovány přímo na emulované stanici s možností interakce přes management server nebo lokální konfigurační soubory.

Standardní provoz

Standardní provoz simuluje chování transformátoru, přičemž jsou emulovány měřené fyzikální veličiny a jejich následná komunikace směrem k řídicímu centru. V tomto režimu stanice generuje vstupní a výstupní napěťové hodnoty (U_a, U_b, U_c) v rozsahu 380–420 kV pro napěťovou úroveň 400 kV, 209–231 kV pro 220 kV a 99–121 kV pro 110 kV. Současně jsou emulovány hodnoty vstupních a výstupních proudů (I_a, I_b, I_c), které se pohybují od desítek ampér až po jednotky kilo ampér v závislosti na denní době a průběhu zatížení uvedeném výše. Dále hraje roli i typ samotné stanice, tedy zda simuluje provoz hraničního transformátoru elektrárny nebo jiné stanice přenosové soustavy.

Pro dosažení realistické simulace stanice rovněž počítá činný výkon (P) a jalový výkon (Q), které poskytují detailní informace o energetických tocích v síti. Dynamická změna fázového posunu (φ) v průběhu simulace umožňuje modelovat různé provozní stavy a docílit co nejvěrnějšího obrazu skutečné situace. Dále byly implementovány funkce generující hodnoty kmitočtu v rozsahu 49,5–50,5 Hz, přičemž jmenovitý kmitočet činí 50 Hz. Teplota transformátoru byla modelována v rozmezí 100–140 °C, zatímco okolní teplota byla nastavena v intervalu 15–25 °C, což odpovídá běžným podmínkám okolního prostředí.

Z hlediska komunikace s řídicím centrem jsou v tomto režimu odesílány výhradně PM (periodické zprávy). Interval odesílání těchto zpráv je nastaven na 10 sekund a každá zpráva obsahuje

informace o měřených (v tomto případě simulovaných) veličinách. Tyto zprávy se nacházejí v rozsahu IOA adres 1000 až 5013 dle tabulky 6.5. Kromě měřených hodnot jsou přenášeny také stavy jednotlivých ochranných prvků, konkrétně CB (vypínač), DC (odpojovač) a ES (uzemňovač).

Tab. 6.5: Simulovaná data generovaná elektrickou stanicí v polygonu

Počet	**IOA rozsah**	**Význam dat**
12	1000–1011	Data představují vstupní hodnoty fyzikálních veličin – napětí (U), proud (I), činný (P) a jalový (Q) výkon pro všechny tři měřené fáze.
12	2000–2011	Data představují výstupní hodnoty fyzikálních veličin – napětí (U), proud (I), činný (P) a jalový (Q) výkon pro všechny tři měřené fáze.
5	3000–3002	Data představují teplotu transformátoru (TT), okolní teplotu (AT) a frekvenci (f).
5	4000–4003	Data představují stavy ochranných prvků – vypínač, odpojovač a uzemňovač.
5	5000–5013	Data představují stavy definovaných událostí (např. vypnutí vypínače nebo vyvolání alarmu). Zároveň přenášejí informace o stavech alarmu: přepětí/podpětí, nadproud, zkrat.

V rámci scénáře standardního provozu existuje možnost aktivace definovaných pod-scénářů, jejichž zjednodušené časové průběhy jsou znázorněny na obrázku 6.8, kde část (a) znázorňuje napěťové charakteristiky pro standardní provoz (zeleně), podpětí (modře) a přepětí (červeně). Dále jsou uvedeny definované prahové hodnoty pro odeslání informací o možném pod/přepětí (světle modře) a hodnoty pro výstražné zprávy v případě výrazného odchýlení od nominálu (oranžově). Část (b) zachycuje časové průběhy proudu pro scénář standardního provozu (zeleně), nadproud (červeně), výpadek s obnovou (modře) a zkrat bez obnovy (fialově).

Hodnoty napětí a proudu na ose y jsou v grafu reprezentovány jako „pu“ (poměrná jednotka), což představuje normalizovaný koeficient vztažený k jmenovité hodnotě, umožňující vyjádřit veličinu jako poměr k jejímu jmenovitému stavu. Osa x zobrazuje časový vývoj v sekundách, který znázorňuje změnu v rámci pod-scénáře vůči výchozímu stavu. Nejedná se tedy o celkový časový průběh daného scénáře.

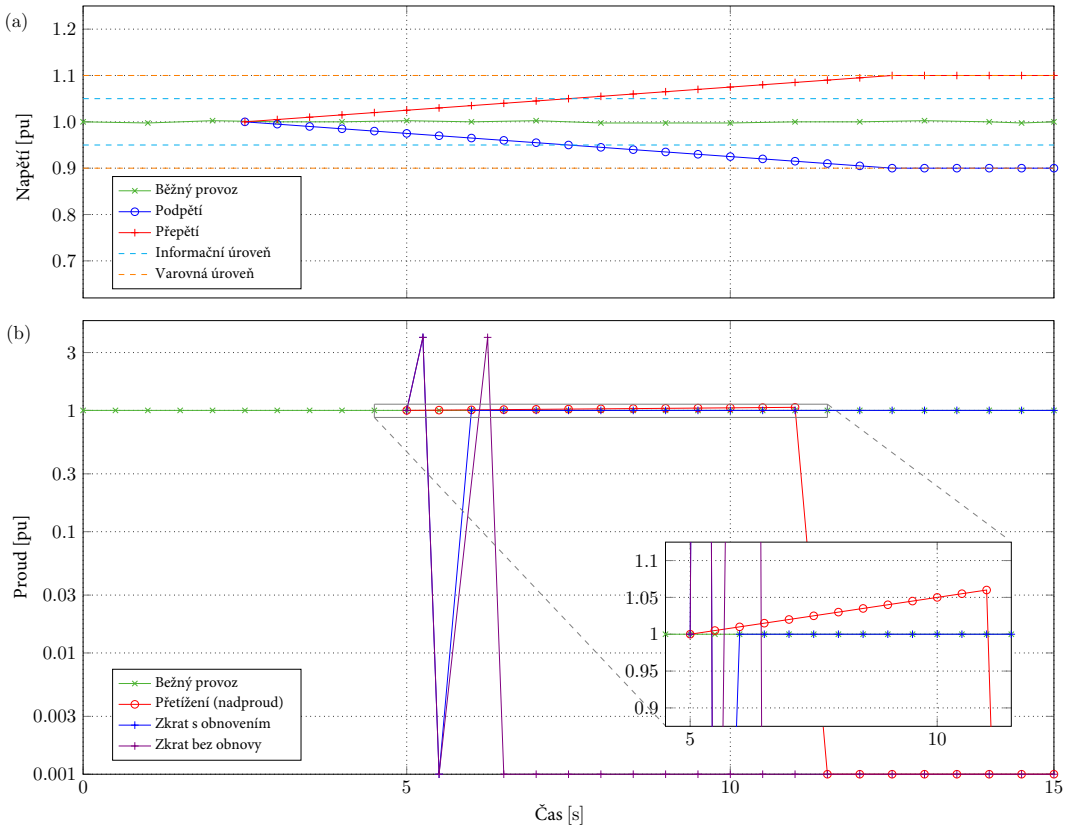
Standardní manipulace „Servisní“

Servisní zásahy v rozvodnách jsou běžnou a nezbytnou součástí provozu elektrických rozvoden, které zajišťují optimální údržbu a bezproblémový chod energetických systémů. Scénář „Servis“ představuje simulaci nezbytných oprav a údržby elektrické rozvodny. Tento scénář má tři varianty a zohledňuje různé bezpečnostní prvky stanice (vypínač, odpojovač, uzemňovač). Scénář je spuštěn odesláním příkazu k odpojení (nebo připojení) příslušného prvku. Tato akce způsobí, že stanice odpoví odesláním NPM zprávy o změně stavu daného prvku.

Následně je daný prvek uveden do logické mezipozice, kde vyčkává na provedení změny. Dispečerské centrum je poté informováno o odpojení (nebo připojení) daného prvku další NPM zprávou. Tento proces je shodný pro všechny výše uvedené prvky.

Podpětí / Přepětí

Scénář napěťové nestability představuje situaci, kdy transformované napětí vybočuje ze své jmenovité hodnoty. V tomto případě mohou nastat pouze dvě odchylky: podpětí (snížení úrovně napětí)



Obr. 6.8: (a) Průběh napětí ve scénáři standardního provozu, podpětí a přepětí; (b) Průběh proudu ve scénáři standardního provozu, nadproud, zkrat s obnovou a bez obnovy

a přepětí (zvýšení úrovně napětí). Oba tyto stavy se přitom mohou dále stupňovat do dvou úrovní: informační (nekrizová odchylka), a výstražná (kritická odchylka od jmenovitého napětí).

V takových případech jsou kromě periodických zpráv (PM) odesílány také neperiodické zprávy (NPM) směrem k řídicímu centru. V rámci těchto NPM jsou zasílány buď výstražné informace při výskytu nekrizové události, nebo zprávy indikující kritický stav – spuštění alarmu a konkrétní typ události (kritické podpětí či přepětí).

Nadproud

Ukládání elektrické energie představuje náročnou a časově nákladnou operaci. Výrobny elektrické energie nemohou produkovat libovolné množství energie – celý systém musí být udržován ve stavu takzvané rovnováhy, kdy množství vyrobené energie odpovídá spotřebě. Pokud je tato rovnováha narušena, může v systému nastat přepětí (při nadprodukci) nebo podpětí (při nadspotřebě). Pokud řídicí centrum nedokáže tyto odchylky dostatečně kompenzovat, může dojít k selhání části systému nebo celého systému.

Scénář nadproudu simuluje situaci, kdy v elektrickém systému dojde k překročení proudové zátěže, což vede k bezpečnostnímu odstavení stanice. Tento scénář simuluje postupné zvyšování proudu, které začíná v čase $t = 5\,s$ (viz obrázek 6.8 (b)). V čase $t = 12\,s$ dojde k reakci ochranných prvků a následně k bezpečnostnímu odpojení. V rámci odezvy ochranných prvků jsou odesílány neperiodické zprávy obsahující stav těchto prvků (odpojovač a vypínač) a informace o změně jejich stavu. Zároveň jsou zasílány zprávy o aktivaci alarmu a výskytu kritické nadproudové události. Po vyřešení problému a návratu ochranných prvků do původního stavu je řídicí centrum informováno novými NPM a systém se přepíná zpět do scénáře standardního provozu.

Zkrat

Ke zkratu v elektrickém systému dochází v okamžiku, kdy dojde k nežádoucímu spojení elektrických vodičů s rozdílným potenciálem, což má za následek náhlý a nekontrolovaný přetok elektrického proudu. Simulace zkratu je důležitá, protože umožňuje otestovat reakci elektrického systému na tento kritický jev. Identifikace a pochopení chování systému během zkratu je klíčové pro návrh bezpečnostních opatření, ochran a strategií s cílem minimalizovat riziko poškození zařízení a zajistit rychlé a spolehlivé odstavení v případě závažného problému.

Scénář zkratu je navržen ve dvou variantách: se zotavením provozu a bez následného obnovení provozu. Tento scénář lze rozdělit do dvou hlavních fází: simulovaný výpadek a následná reakce stanice. Celá situace je zobrazena na obrázku 6.8. V první fázi je simulovaný výpadek vyvolán v čase $t = 5{,}5\,s$. Dochází k náhlému skokovému nárůstu proudu, který vyvolá téměř okamžitou reakci ochranných prvků. Během této události jsou odesílány NPM zprávy týkající se stavu ochrany proti zkratu, přepnutí ochrany proti zkratu, výstražné zprávy a informace o stavech a změnách prvků odpojovač a vypínač.

Ve druhé fázi, tedy při reakci stanice, přicházejí dvě možné varianty. První představuje reakci s následným obnovením provozu (zobrazeno modře na obrázku). V tomto případě se stanice pokusí úspěšně obnovit provoz. Při této akci jsou odesílány NPM o změně stavu vypínače a o změnových událostech. Následně je znovu spuštěn scénář standardního provozu.

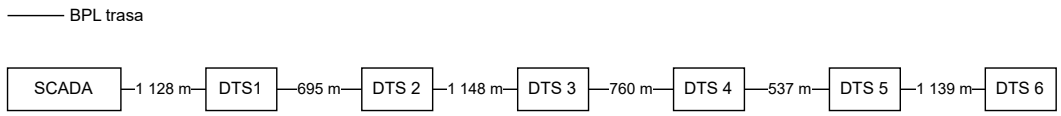
Druhou možností je reakce stanice bez následného obnovení provozu (zobrazeno fialově). Při neúspěšném pokusu o obnovení provozu v čase $t = 6\,s$ jsou postupně odesílány NPM zprávy obdobné jako v první fázi, tedy o stavu ochrany proti zkratu, o přepnutí ochrany proti zkratu, výstražné zprávy a informace o stavech a změnách prvků odpojovač a vypínač.

6.4 Aplikace testovacího prostředí

V této podkapitole jsou uvedeny příklady použití testovacího prostředí BUTENET. Podkapitola je rozdělena na tři části, kde v první je uveden použití emulační jednotku pro ověří možnosti BLP komunikace v reálných podmínkách distribučních trafostanic. Dále je uvedeno použití části sítě BUTENET s fyzickými zařízeními pro generování datové komunikace protokolů IEC 60870-5-104, MMS, GOOSE, SV a ModBusTCP. Poslední příkladem je použití BUTENET pro ověření zabezpečení testovaných zařízení dle metodiky [11].

6.4.1 Testování BPL komunikace pomocí Emulační jednotky

Testovací prostředí bylo vybudováno na reálné komunikační infrastruktuře BPL (broadband over powerline) v městské části Brno-střed. Bylo zapojeno 6 distribučních trafostanic (DTS) v linii mezi centrálním uzlem a nejvzdálenější stanicí. Centrální uzel (SCADA) fungoval jako sběrný bod, kde agregoval veškerá data ze sítě a představoval nadřazený systém komunikující s podřízenými stanicemi. BPL síť byla na obou koncích odpojena od dalších uzlů tak, aby vznikla izolovaná linie pouze s testovanými stanicemi. Celková délka trasy mezi centrálou SCADA a poslední stanicí (DTS 6) byla 5,4 km a signál procházel přes 19 BPL opakovačů Na obrázku 6.9 v dokumentu je zobrazena topologie se vzdálenosti mezi stanicemi.



Obr. 6.9: Topologie testovacího prostředí

Každá trafostanice v linii byla vybavena Emulačními jednotkami nebo reálnými prvky, které reprezentovali zařízení a služby chytré stanice. V každé DTS byly nasazeny:

- VN pole (vysoké napětí): emulace řídicí jednotky pole VN (spínače, odpojovače apod.), komunikující protokolem IEC 104.
- NN rozvaděč (nízké napětí): emulace řídicí jednotky rozvaděče NN (odběrové pole NN), taktéž komunikující protokolem 104.
- Univerzální monitor: měřicí zařízení pro energetické veličiny (tzv. PQ monitor) MEg44PAN schopné jedním dotazem poskytnout desítky měřených hodnot. Komunikace probíhala protokolem 104 stejně jako u VN/NN.

Všechny výše uvedené služby běžely paralelně a sdílely společnou komunikační infrastrukturu BPL. Na straně SCADA běžela odpovídající aplikace, která vůči stanicím vystupovala jako nadřazený systém. BPL modemy v jednotlivých stanicích zajišťovaly přenos dat po silovém vedení. V rámci topologie byly v některých stanicích instalovány také síťové prvky (např. ethernetové switche) pro propojení více zařízení v DTS.

Metodika testování a cíle měření

Testování bylo navrženo tak, aby prověřilo komunikační schopnosti BPL sítě pro současný provoz více služeb, určilo limity přenosové kapacity a ověřilo spolehlivost přenosu za zátěže. Bylo definováno několik hlavních cílů (KPI), které měření postupně ověřovala:

1. Schopnost základní komunikace: Ověřit, zda je vůbec možné navázat a udržet spojení protokolem IEC 104 mezi centrálou a libovolnou trafostanicí v dané topologii. Nejprve bez zátěže a následně i při zátěži linky. Kritériem bylo prosté ANO/NE, zda spojení funguje.
2. Přenos všech služeb současně: Otestovat, zda BPL linka zvládne současný provoz všech definovaných služeb při daném počtu stanic, a to bezchybně. Emulovaným datovým provozem se simulovaly reálné odečty dle požadavků (konkrétní měřené hodnoty jako napětí, proudy atd.). Bezchybným provozem se rozumí, že centrála správně obdrží všechny požadované hodnoty z každé služby (i když případně se zpožděním).
3. Zatížení linky protokolem IEC 61850: Prověřit komunikaci protokolem 104 (odečty VN/NN) v případě, že paralelně probíhá zátěžový provoz dle standardu IEC 61850. Cílem bylo najít hraniční míru zatížení, při níž ještě 104 komunikace funguje bezchybně a při níž již začne docházet k výpadkům.
4. Reálný odečet dat reálným zařízením: Do testů bylo zahrnuto také skutečné měřicí zařízení (Univerzální monitor MEg44) komunikující protokolem 104. Ověřovalo se, zda reálný odečtový proces (např. jednorázový dotaz na konkrétní hodnoty, hromadný dotaz na všechny hodnoty nebo odečet dat formou file transferu) proběhne korektně a jakou má režii a zpoždění. Zde se měřila i odezva systému, např. doba mezi dotazem a odpovědí při různých typech dotazů (jednotlivý vs. hromadný) a chování file transfer mechanismu.
5. Dostupnost a stabilita linky: Dlouhodobým testováním (24 h a více dní) zjistit spolehlivost BPL kanálu, vyjádřenou např. procentem dostupnosti (SLA). Pro tento účel byly nasazeny trvalé ping testy, případně udržovací spojení protokolu 104 či monitorování přes SNMP, aby se sledovala ztrátovost paketů a kolísání odezvy v čase.
6. Maximální počet paralelních služeb: Experimentálně určit, kolik paralelních datových přenosů (služeb 104) je BPL linka schopna současně unést při zachování bezchybného odečtu dat. V testech se postupně navyšoval počet souběžných komunikací 104 (všechny se stejným objemem dat) až do bodu, kdy některé odečty začaly selhávat. Tím byl stanoven maximální teoretický počet odečtů, které lze po dané lince provozovat současně.

Přehled testovacích scénářů a jejich zaměření

V testování probíhaly čtyři typy komunikace, které reprezentují klíčové služby trafostanice:

- Scénář VN pole: Pravidelný odečet stavu a měřených hodnot ve VN poli (např. stav vypínače, odpojovače, měřené proudy/napětí). Využívá protokol IEC 104. Tento scénář simuluje komunikaci mezi terminálem VN pole a nadřazeným systémem.
- Scénář NN rozvaděč: Podobně pravidelný odečet v NN rozvaděči (stav jističů, odpojovačů NN, případně měřené hodnoty na odchodech). Také protokol 104. Simuluje komunikaci řídicí jednotky rozvaděče s centrálou.
- Scénář Univerzální monitor (UM): Průběžný sběr měřených energetických veličin (napětí, proudy, výkon, kmitočet apod.) z PQ monitoru v trafostanici. Realizováno protokolem 104. V testech byl nasazen reálný měřič MEg44PAN, který poskytuje přes 80 různých hodnot v jednom odečtu.
- Scénář Ostatní (zatěžovací): Doplňkový scénář představující další zatížení sítě mimo výše uvedené běžné služby. Zahrnuje jednak komunikaci dle IEC 61850 (GOOSE, Sampled Values), a dále souborový přenos (File Transfer) v protokolu 104. Tyto přenosy představují extrémní zátěž, která v reálném provozu není trvalá, ale mohla by nastat.

Každý z výše uvedených scénářů má definován seznam datových bodů k odečtu. Například pro VN pole byly stanoven seznam monitorovaných stavů zařízení v poli, která je uvedena v příloze D v tabulce D.1, kde se jedná jednotlivé signály typu SP – single point (jednobitová indikace), DP – double point (dvoubodová indikace s dvěma bity), případně měřené analogové veličiny ME (measured value). Tabulka D.1 uvádí konkrétní H-kódy položek VN pole (např. stav vypínače zapnut/vypnut, stav odpojovačů, ztráta napětí, atd.). Obdobně pro NN rozvaděč byla stanovena sada stavových signálů (stav jističů, dveří, uzemnění, atd.), jak je uvedeno v příloze D v tabulce D.2. Scénář Univerzální monitor zahrnuje desítky analogových měřených hodnot (typ 13 – měřené hodnoty) a několik binárních vstupů (typ 1 a 3). V testu se vždy dotazovaly všechny dostupné objekty monitoru MEg44PAN.

Popis komunikačních protokolů v testování

IEC60870-5-104 Protokol byl páteří většiny scénářů (VN, NN, UM) a byl využit i pro speciální testy. V testu centrála navazovala TCP spojení ke každé stanici a periodicky zasílala dotazy (ASDU) na definované datové objekty, na které stanice odpovídala přenosem hodnot. Komunikace probíhala buď cyklicky (centrála se každou minutu dotázala na všechny hodnoty daného scénáře) nebo spontánně (v režimu spontaneous mohla stanice posílat změny sama, to však bylo využito jen okrajově u UM). Emulační stanice s 104 implementovaná v testbedu podporovala logování všech odeslaných i přijatých telegramů pro vyhodnocení (včetně detekce ztracených či duplikovaných segmentů). Protokol 104 byl rovněž použit pro file transfer scénář, který generoval výrazné jednorázové zatížení linky (simulace hromadného výpisu dat ze stanice).

MMS Generátor umožnil simulovat obdobu dotazů/odpovědí jako u IEC 104, ale v prostředí MMS. V měření byl spuštěn paralelní provoz dotaz-odpověď přes MMS s podobnou sadou objektů, jaké byly v scénářích VN a NN (7 polí VN a 12 rozvaděčů NN na stanici). Výsledkem byly údaje o ztrátovosti při MMS komunikaci mezi různě vzdálenými stanicemi.

GOOSE V testu byly GOOSE simulovány spíše jako součást celkové zátěže, např. V rámci scénáře "Ostatní" byl generován ruch odpovídající burst režimu GOOSE.

Sampled Values V první fázi testování bylo generování SV rámců nastaveno s periodou 10 ms, při kterém ještě probíhala komunikace 104. Následně se interval zkracoval, při periodě 3 ms už došlo k zahlcení kanálu, které se projevilo tím, že nebylo možné navázat žádnou jinou komunikaci s žádnou stanicí. Tím se experimentálně určil hraniční bod, kdy datový tok dle 61850 prakticky zahltí kapacitu BPL.

Výsledky testování

Ve všech kombinacích běžných služeb (VN, NN, UM) prokázala BPL síť schopnost přenosu, kde ve scénářích 1–4 bylo možné provozovat všechny odečty současně i na nejvzdálenější stanici. Při zatížení ve scénáři 5 (Ostatní) v DTS 4, 5 a 6 došlo k rozpadu komunikace. Komunikace se zátěží tak mohla být realizována až k DTS 3.

Měření ztrátovosti na transportní vrstvě ukázala, že chybovost přenosu narůstá se vzdáleností stanice od centrály, a to zhruba exponenciálně. V měření byly nejbližší stanice téměř bez chyb, zatímco nejvzdálenější vykazovaly významné ztráty. Tabulka 6.6 uvádí ztrátovost paketů (protokolu 104) pro scénář VN a NN v jednotlivých stanicích. Z tabulky jde vidět, že pro DTS 1 až DTS 3 (do cca 1,8 km) zůstává ztrátovost velmi nízká (méně než 1 %).

U DTS 4 již dochází k citelným ztrátám v jednotkách až desítkách procent. Nejvzdálenější dvě stanice (DTS 5 - cca 4,5 km, DTS 6 - cca 5,4 km) měly ztrátovost okolo 50 %, což je již kritická hodnota, kdy se ztratilo okolo poloviny paketů 104.

Tab. 6.6: Ztrátovost paketů 104 v závislosti na vzdálenosti stanice

Stanice	**Ztrátovost VN [%]**	**Ztrátovost NN [%]**
DTS 1	0,213 %	0,730 %
DTS 2	0,430 %	0,384 %
DTS 3	1,869 %	1,369 %
DTS 4	12,830 %	7,958 %
DTS 5	49,087 %	22,662 %
DTS 6	46,794 %	54,421 %

Podobného průběhu dosahuje i doba odezvy na DTS 1 až DTS 6. Během všech testů bylo prováděno tetování na dostupnost jednotlivých stanic pomocí nástroje PING, který se z centrální SCADA stanice dotazoval na jednotlivé DTS. Dotazy probíhaly během všech testů s frekvencí jednoho dotazu za dvě sekundy. Z těchto hodnot se potom počítaly celkové průměrné hodnoty, kde tabulka 6.7 shrnuje výsledky pro průměrnou ztrátovost ping paketů a min/průměr/max odezvu pro jednotlivé stanice.

Z tabulky jde vidět obdobný exponenciální průběh jako v případě ztrátovosti paketů pro IEC 104. Prvních čtyři stanic mají průměrnou ztrátu do cca 1 % a odezvu mezi 30 až 120 ms, zatímco u DTS 5 ztrátovost narostla na přibližně trojnásobek, tak u nejvzdálenější stanice jeto už více než desítinásobek oproti prvním čtyřem stanicím. Z výsledků obousměrného zpoždění (RTT) je patrné, že průměrná odezva RTT roste s každou další stanicí. Do DTS 3 (včetně) se RTT zvyšovalo rovnoměrně a ztrátovost zůstávala pod 1,1 %, což znamená stále stabilní přenos. Ke změně dochází u DTS 4, kde se RTT dostává přes 110 ms a začíná výrazně kolísat. Největší problémy jsou u nejvzdálenější DTS 6, kde průměrné RTT překračuje 150 ms, maximální hodnota dosahuje přes 1 s. Tato kombinace vysokého zpoždění a ztrát znamená, že spojení zde již není spolehlivé pro časově citlivé služby.

Tab. 6.7: Průměrná odezva a ztrátovost pro DTS

Stanice	**Ztrátovost [%]**	**Průměr RTT [ms]**	**Min RTT [ms]**	**Max RTT [ms]**
DTS 1	0,69 %	27,39	10,46	234,19
DTS 2	0,78 %	56,34	24,93	322,44
DTS 3	1,08 %	91,00	44,44	417,18
DTS 4	1,39 %	112,41	59,79	464,93
DTS 5	3,30 %	125,35	68,02	586,02
DTS 6	13,04 %	156,92	80,56	1069,78

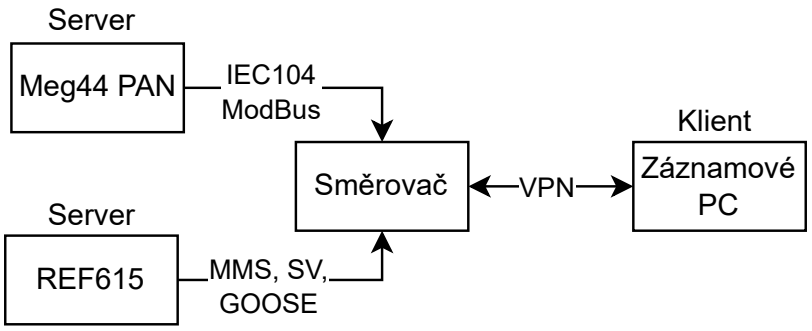
6.4.2 Generování dat pro neuronové sítě

Článek [23] se zabývá problematikou rozpoznávání průmyslových protokolů pomocí hlubokého učení, konkrétně konvolučních neuronových sítí (CNN). Hlavním cílem studie bylo klasifikovat nešifrovaný a šifrovaný provoz průmyslových protokolů. Článek se zaměřují na pět průmyslových protokolů: IEC 60870-5-104, MMS, GOOSE, SV a Modbus/TCP. Studie zkoumá, zda lze tyto

protokoly rozpoznat i v jejich šifrované verzi, a zda je možné rozpoznat šifrovaný provoz pomocí technologie VPN.

Hlavním přínosem generovaných dat na testovacím prostředí bylo, že většina dostupných článku zabývajících se neuronovými sítěmi a VPN komunikací vychází ze stejných datových sad, přičemž většina těchto datových sad neobsahuje energetické protokoly, jako jsou IEC 60870-5-104, MMS, GOOSE, SV. Z tohoto důvodu bylo využito testovacího prostředí, jak je zobrazeno na obrázku 6.10. Specificky zařízení PQ Monitor MEg44PAN, který simuloval komunikaci protokoly IEC 104 a Modbus, a ochranné a řídící relé ABB REF615, které bylo využito pro simulaci protokolů MMS, GOOSE a SV. Router zajišťoval přenos dat mezi těmito zařízeními a počítačem, kde byla data zaznamenávána pomocí nástroje Wireshark. Tento záznam byl poté rozdělen na kategorie na základě typu protokolu a toho, zda byla data šifrovaná nebo ne. Aby byla simulována šifrovaná komunikace, bylo do testovacího prostředí zahrnuto VPN spojení mezi routerem a počítačem, které umožnilo šifrovat komunikaci bez nutnosti zásahu do samotných koncových zařízení.

Výsledné datové sady zahrnovaly celkem 11 kategorií, z nichž pět obsahovalo nešifrovaná data, pět šifrovaná data a jedna kategorie obsahovala šifrovaný provoz, který se skládat z běžné komunikace uživatele na internetu. Tyto datové sady byly následně použity k trénování modelů CNN. Díky testovacímu prostředí, které umožnilo generování realistických a reprezentativních dat, dosáhly modely CNN vysoké přesnosti při rozpoznávání průmyslových protokolů.



Obr. 6.10: Testovací prostředí pro simulaci dat - IEC 104, MMS, GOOSE, SV, ModbusTCP

V článku jsou představeny tři modely CNN, které byly trénovány na rozpoznávání těchto průmyslových protokolů. Autoři použili tři různé scénáře: 1D, 2D a PKT (zaměřený na jednotlivé pakety), přičemž každý scénář byl ověřen pomocí trénovacích, testovacích a validačních dat. Modely dosáhly vysoké přesnosti v rozmezí 96-97% při klasifikaci jak nešifrovaných, tak šifrovaných průmyslových protokolů. Zejména 2D model byl rychlejší než modely 1D a PKT, což naznačuje jeho potenciální využití v specifických sítích. PKT model se ukázal jako užitečný v sítích, kde se vyskytuje více průmyslových protokolů, protože dokáže analyzovat síťový provoz na úrovni jednotlivých paketů. Výsledky ukazují, že CNN mohou být velmi efektivním nástrojem pro rozpoznávání průmyslových protokolů, což má významný dopad na zabezpečení průmyslových sítí.

6.4.3 Metodika testování bezpečnostních parametrů RTU

Jednou z aplikací BUTENETu je i možnost využití při testování odolnosti zařízení z energetického sektoru. Mezi takové případy spadá i Metodika testování bezpečnostních parametrů RTU jednotek [11]. Tato metodika je navržena pro hodnocení RTU zařízení používaných v distribučních sítích

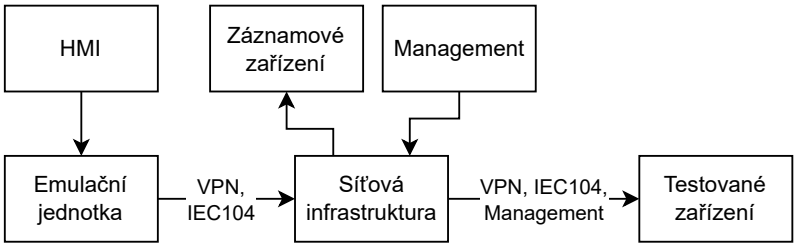
komunikujících pomocí protokolu IEC 60870-5-104 s nadřazeným dohledovým centrem. Metodika se skládá ze sedmi hlavních kategorií, pod kterou spadají samotné testy.

1. Udržitelný design (UDR): Zaměřuje se na to, aby zařízení RTU mělo dostatečné hardwarové rezervy pro budoucí rozšíření, např. pro podporu nových bezpečnostních požadavků či delších kryptografických klíčů. Testy ověřují, zda výkonové parametry (CPU, RAM, FLASH) zůstávají nad stanovenou hranicí i při běžném i zatíženém provozu.
2. Kryptografie (KRY): Tato kapitola hodnotí, zda RTU používá bezpečné kryptografické algoritmy a klíčové délky v souladu s doporučeními (např. dle NIST). Zahrnuje testy integrity, autentizace, důvěrnosti a ochrany proti replay útokům právě v kontextu spojení IEC 104 přes VPN/IPsec.
3. Komunikační bezpečnost (KOM): Zde je posuzována robustnost protokolové implementace, zejména schopnost přístroje správně zpracovat validní zprávy a bezpečně odmítat chybná či fuzzed data. Cílem je, aby jakékoli nevalidní vstupy vedly k žádnému nežádoucímu nebo neznámému stavu zařízení.
4. Záloha, spuštění a aktualizace (ZSA): Sleduje, jak RTU reaguje na výpadky během provozu, aktualizace či bootování. Testy zahrnují simulaci ztráty sítě nebo napájení během aktivní IEC 104 komunikace a ověřují, zda zařízení dokáže obnovit spojení a funkčnost bez manuálního zásahu.
5. Podpora bezpečnostních operací (OPE): Tato část se zabývá schopností RTU poskytovat auditní stopy, logování bezpečnostních událostí, správu přístupových práv a monitorování kritických operací. Důraz je kladen na transparentnost a sledovatelnost chování zařízení.
6. Systémový hardening (HAR): Cílem je ověřit, že RTU obsahuje pouze nejnutnější software a služby, pravidelně se aktualizuje a odděluje kritické funkce (bezpečnost, komunikace, procesní). Sleduje se také ochrana paměti a prevence zneužití běhového prostředí.
7. Záruka dodavatele (DOD): Zaměřuje se na kvalitu dodavatelského procesu, zajištění dlouhodobé podpory, dostupnost firmware aktualizací, záplat a dokumentace. Kontroluje se, zda dodavatel garantuje bezpečnostní aktualizace a podporuje životní cyklus produktu.

Testování probíhá formou simulovaných scénářů přizpůsobených konkrétnímu zařízení, přičemž každý testovací proces je individuální, protože i zařízení stejného typu se mohou lišit z hlediska operačního systému, firmware či vstupně výstupních rozhraní.Testované zařízení je připojeno do infrastruktury BUTENET, které je zobrazeno na obrázku 6.11 a jednotlivé části jsou:

- Emulační jednotka: v této části běží simulace prostřednictvím protokolu IEC 60870-5-104, která napodobuje chování reálného RTU. Jednotka přijímá příkazy a generuje datové toky dle scénářů (včetně chybových stavů, výpadků, aktualizací apod.).
- Ovládání přes HMI: Operátor prostřednictvím HMI provádín scénáře testu – mění parametry komunikace, spouští emulaci chyb, sleduje stavové ukazatele RTU či spouští výpadky. HMI slouží jako přímý nástroj interakce s emulační jednotkou.
- Síťová infrastruktura: Zajišťuje komunikace mezi všemi prvky infrastruktury, ale nejdůležitější je mezi emulační jednotkou a testovaným zařízením (RTU). Do provozu jsou zapojeny protokoly VPN/IPsec a IEC 104, které umožňují testovat bezpečnostní aspekty spojení.
- Testované zařízení (RTU): RTU je připojeno do stejné síťové infrastruktury. Emulační jednotka s ním komunikuje přes IEC 104 s použitím VPN/IPsec. Testované scénáře zahrnují standardní i chybovou komunikaci, výpadky, aktualizace či bezpečnostní útoky. Management přístupu slouží k vzdálenému řízení, konfiguraci nebo obnově provozu při výpadcích.
- Management: Management reprezentuje nástroje pro správu RTU – vzdálený přístup, nastavování IP, firmware, aktualizace, případně restart, aktualizace konfigurace, nebo vytažení diagnostických logů přímo z testovaného zařízení.

- Záznamové zařízení (logging/pcap): v síti je zároveň nasazen záznamový systém pro ukládání logů, pcapů i systémových událostí. Tyto záznamy slouží k pozdější analýze komunikace, detekci chyb nebo prověření dodržení testovacích scénářů (např. nevalidní zprávy, latence, obnovy spojení).



Obr. 6.11: Zjednodušené prostředí BUTENET pro testování RTU

Příklad testů

UDR.01 – Dostatečné rezervy v hardwarových prostředcích V rámci testu UDR.01 je emulační stanice BUTENETu využita pro odeslání náhodného IEC 60870-5-104 datagramu přes VPN/IPsec a změřena doba odezvy. Současně je sledováno zatížení CPU, RAM a flash paměti, aby nebylo v průběhu testu překročeno 70 %. Takto se ověřuje, že testbed s reálnou komunikací IEC 104 nedosahuje kritického využití prostředků a poskytuje dostatečnou rezervu pro spolehlivý provoz.

KRY.01 – Bezpečné kryptografické algoritmy Pro test KRY.01 je BUTENET konfigurace emulační stanice nastavená na provoz IEC 104 přes VPN/IPsec. Testuje se, zda jsou implementovány doporučené kryptografické algoritmy a délky klíčů a současně se provádí kontroly ochrany integrity, autenticity a důvěrnosti přenášených zpráv. BUTENET tak simuluje autentizaci, modifikaci i odposlech, aby bylo možné vyhodnotit bezpečnostní kvality komunikace IEC 104.

KOM.01 – Validace protokolové sady Test KOM.01 kontroluje schopnost RTU pracovat pouze s platnými IEC 104 zprávami. BUTENET emuluje validní i nevalidní komunikaci (chybný formát, zlomkové zprávy, chybné CRC) včetně režimu fuzzingu. RTU je testováno, zda tyto vstupy správně odmítne a nevyvolá ani neočekávané stavy. Test se opakuje i při zatížení sítě, což potvrzuje robustnost protokolu při reálném provozu.

ZSA.02 – Ochrana systému proti chybám při spuštění, aktualizaci a provozu Při testu je BUTENET použit tak, že v průběhu aktivní IEC 104 komunikace přes VPN/IPsec dochází k simulovanému výpadku datové sítě i napájení na minutu. Test se opakuje během běhu, bootování i aktualizace firmware. Emulační stanice pak ověřuje, že RTU zvládne obnovit spojení a vrátit se do normálního provozu bez zásahu obsluhy, čímž se testuje jeho odolnost a fail-safe mechanismy.

Závěr

Předložená disertační práce se zaměřila na aktuální a stále naléhavější problém zajištění kybernetické bezpečnosti v oblasti elektroenergetiky, která prochází rozsáhlou digitalizací a integrací provozních technologií. Vzhledem k narůstajícímu riziku cílených útoků na kritickou infrastrukturu bylo nezbytné vytvořit nástroje a prostředí, které umožní bezpečný výzkum, školení a testování bezpečnostních opatření bez ohrožení reálných systémů.

Hlavní výzkumné otázky se soustředily na tři klíčové problémy: nedostatečnou připravenost personálu v oblasti OT kybernetické bezpečnosti, absenci bezpečného a realistického testovacího prostředí a omezenou dostupnost autentických provozních dat. Cílem práce proto bylo navrhnout a realizovat škálovatelnou sandbox architekturu, která umožní realistickou emulaci provozu elektroenergetických sítí, testování zranitelností i mitigací a současně poskytne platformu pro školení v multitechnologickém prostředí.

V rámci práce byl vytvořen referenční model energetické datové infrastruktury na základě konceptu SGAM, zahrnující klíčová zařízení (MU, IED, RTU, HMI, SCADA a další) a komunikační protokoly MMS, GOOSE, SV a IEC60870-5-104. Tento model sloužil jako základ pro návrh a následnou implementaci testovací architektury, která kombinuje fyzické, emulované a virtualizované komponenty. Výsledné testovací prostředí umožňuje nejen simulaci běžného provozu, ale i testování výpadků, přetížení, zpoždění nebo útoků ve scénářích.

V rámci práce byl vytvořen referenční model infrastruktury a komunikační architektury Smart Grids, který poskytuje systematický přehled klíčových prvků (IED, RTU, PLC apod.) a datových toků podle norem IEC 61850 a IEC 60870. Tento model slouží jako základ pro návrh realistických scénářů a lépe propojuje domény IT a OT. Hlavním výsledkem je návrh a implementace sandboxového testovacího prostředí, který má modulární a škálovatelnou architekturu kombinující fyzické komponenty, emulované prvky a virtualizované systémy.

Testovací prostředí bylo následně validováno z hlediska funkčnosti a využitelnosti. Prokázalo schopnost realisticky napodobit datovou komunikaci v elektroenergetické infrastruktuře, včetně redundantních topologií a zátěžových stavů. Díky modulárnímu návrhu je architektura flexibilní a přizpůsobitelná různým výzkumným i školicím potřebám. Uživatelům umožňuje bezpečně experimentovat s protokoly, zařízeními i scénáři, které by v reálném prostředí byly neproveditelné.

Navržený přístup se odlišuje od dosavadních řešení v několika zásadních ohledech. Zatímco dostupná testovací prostředí se soustředí převážně na simulaci vybraných částí chytrých sítí, tato práce představuje modulární sandbox architekturu, která propojuje fyzické, emulované a virtualizované komponenty. Díky této kombinaci je možné realisticky modelovat nejen komunikační toky a protokoly (MMS, GOOSE, SV, IEC 60870-5-104), ale také kybernetické útoky a obranná opatření v prostředí, které je bezpečné a plně kontrolované.

Výsledná architektura tak překonává nedostatky dřívějších řešení, především absenci autentických datových sad, omezené možnosti školení personálu a nejednotné pokrytí bezpečnostních standardů. Přínos práce proto spočívá nejen v rozvoji vědeckého poznání v oblasti kybernetické bezpečnosti energetických sítí, ale i v poskytnutí prakticky využitelného nástroje pro provozovatele kritické infrastruktury, výzkumné organizace a vzdělávací instituce.

Originalita tohoto přístupu spočívá v propojení modelování hrozeb a praktického mapování na prvky komunikační elektroenergetické infrastruktury s příslušnými standardy, což jiné práce nezahrnují. Vytvořený rámec tak umožňuje nejen detailní identifikaci zranitelností, ale také jejich přímé srovnání s existujícími bezpečnostními normami. Díky tomu vzniká nástroj, který poskytuje jedinečný most mezi teoretickými metodikami kybernetické bezpečnosti a praktickými požadavky provozní praxe.

Součástí práce byla rovněž formální analýza přenosu zpráv v síti pomocí teorie front. Modely M/M/1, M/D/1 a MMPP byly aplikovány na zprávy GOOSE, SV a IEC 104 s cílem popsat chování sítě při běžném i přetíženém provozu. Kvantitativní analýza přinesla užitečné poznatky pro dimenzování sítě, posouzení ztrátovosti a vlivu redundance. Výsledky ukazují, že navržené testovací prostředí je schopno věrně simulovat i kritické scénáře a poskytuje solidní základ pro výzkum odolnosti a bezpečnosti chytrých sítí.

Originalita práce spočívá v propojení matematických modelů přenosových charakteristik s praktickou validací v implementovaném testovacím prostředí nabízí jedinečné spojení teoretické a aplikační roviny a umožňuje kvantitativně analyzovat dopady útoků a obranných mechanismů a zároveň je experimentálně ověřit v podmínkách blízkých reálnému provozu.

Autorova literatura

[1] Benedikt, J.; Vrtal, M.; Fujdiak, R.; aj.: Virtualization Platform for Urban Infrastructure. In *Proceedings of the 2022 22nd Inoternational Scientific Conference on Electric Power Engineering (EPE)*, 1, New York: IEEE, 2022, ISBN 978-1-6654-1057-1, str. 5, doi:10.1109/EPE54603.2022.9814159, https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=9814159.

[2] BLAŽEK, P.; FUJDIAK, R.; HODOŇ, M.; aj.: Communication Anomaly Detection in Cyber-Physical Systems. In *Sensors and Electronic Instrumentation Advances: Proceedings of the 5th Inoternational Conference on Sensors and Electronic Instrumentation Advances*, 2019, ISBN 978-84-09-14413-6, s. 311–316, https://www.sensorsportal.com/SEIA_2019/SEIA_2019_Proceedings_Conotents.pdf.

[3] Blažek, P.: Charakterizace signálů akustické emise pro shlukovou analýzu. In *STUDENT EEICT 2013 Proceedings of the 19th Conference Volume 1*, první, Brno: Vysoké učení technické v Brně, Fakulta elektrotechniky a komunikačních technologií, 2013, ISBN 978-80-214-4693-9, s. 80–83, http://www.feec.vutbr.cz/EEICT/2013/sbornik/01bakalarskeprojekty/02zpracovanisignaluobrazuadat/01-140217.pdf.

[4] Blažek, P.; Bohačík, A.; Fujdiak, R.; aj.: Smart Grids Transmission Network Testbed: Design, Deployment, and Beyond. *IEEE Open Journal of the Communications Society*, ročník 6, č. 1, 2024: s. 51–76, ISSN 2644-125X, doi:10.1109/OJCOMS.2024.3517340, https://ieeexplore.ieee.org/document/10798972.

[5] Blažek, P.; Fujdiak, R.; Mlýnek, P.; aj.: Development of Cyber-physical security testbedbased on IEC61850 architecture. *Elektronika Ir Elektrotechnika*, ročník 25, č. 5, 2019: s. 82–87, ISSN 1392-1215, doi:10.5755/j01.eie.25.5.24361, http://eejournal.ktu.lt/index.php/elt/article/view/24361.

[6] Blažek, P.; Gerlich, T.; Martinásek, Z.: Scalable DDoS Mitigation System. In *42st Inoternational Conference on Telecommunications and Signal Processing (TSP)*, ročník 42, 2019, ISBN 978-1-7281-1864-2, ISSN 1805-5435, s. 617–620, doi:10.1109/TSP.2019.8768869, https://ieeexplore.ieee.org/document/8768869.

[7] Blažek, P.; Gerlich, T.; Martinásek, Z.; aj.: Comparison of Linux Filtering Tools for Mitigation of DDoS Attacks. In *41st Inoternational Conference on Telecommunications and Signal Processing (TSP)*, ročník 41, Athens: Institute of Electrical and Electronics Engineers Inc., 2018, ISBN 978-1-5386-4695-3, ISSN 1805-5435, s. 145–149, doi:10.1109/TSP.2018.8441309, https://ieeexplore.ieee.org/document/8441309.

[8] Blažek, P.; Hajný, J.: Identifikace anomálií v datové komunikaci pomocí entropie. *Elektrorevue - Inoternetový časopis (http://www.elektrorevue.cz)*, ročník 18, č. 4, 2016: s. 1–5, ISSN 1213-1539.

[9] Blažek, P.; Smékal, D.; Martinásek, Z.: Porovnání technik směrování paketů pro adaptivní filtrační systém DDoS útoků. *Elektrorevue - Inoternetový časopis (http://www.elektrorevue.cz)*, ročník 19, č. 5, 2017: s. 1–8, ISSN 1213-1539.

[10] Dvořák, J.; Jeřábek, J.; Bečková, Z.; aj.: Multifunctional Electronically Reconfigurable and Tunable Fractional-Order Filter. *Elektronika Ir Elektrotechnika*, ročník 25, č. 1, 2019: s. 26–30, ISSN 1392-1215, doi:10.5755/j01.eie.25.1.22732, http://eejournal.ktu.lt/index.php/elt/article/view/22732.

[11] EG.D: Metodika testování bezpečnostních parametrů RTU. online, 2023, https://www.egd.cz/sites/default/files/2023-05/metodika_testovani_bezpecnostnich_parametru_rtu_v1.pdf.

[12] FUJDIAK, R.; BLAŽEK, P.; APVRILLE, L.; aj.: Modeling the Trade-off Between Security and Performance to Support the Product Life Cycle. In *2019 8th Mediterranean Conference on Embedded Computing (MECO)*, 2019, ISBN 978-1-7281-1740-9, s. 92–97, doi:10.1109/MECO.2019.8760043, "https://ieeexplore.ieee.org/document/8760043".

[13] FUJDIAK, R.; BLAŽEK, P.; CHMELAŘ, P.; aj.: Communication Model of Smart Substation for Cyber-Detection Systems. In *CN 2019: Computer Networks*, 26th Inoternational Conference, CN 2019, Kamień Śląski, Poland, June 25–27, 2019, Proceedings, 2019, ISBN 978-3-030-21951-2, ISSN 1865-0929, s. 256–271, doi:10.1007/978-3-030-21952-9\{_}20, https://link.springer.com/chapter/10.1007/978-3-030-21952-9_20.

[14] FUJDIAK, R.; BLAŽEK, P.; MIKHAYLOV, K.; aj.: On Track of Sigfox Confidentiality with End-to-End Encryption. In *Proceedings of the 13th Inoternational Conference on Availability, Reliability and Security*, 2019, ISBN 978-1-4503-6448-5, s. 1–6, doi:10.1145/3230833.3232805, https://dl.acm.org/doi/10.1145/3230833.3232805.

[15] Fujdiak, R.; Blažek, P.; Mlýnek, P.; aj.: Developing Battery of Vulnerability Tests for Industrial Control Systems. In *2019 10th IFIP Inoternational Conference on New Technologies, Mobility and Security (NTMS)*, 2019, ISBN 978-1-7281-1542-9, s. 1–5, doi:10.1109/NTMS.2019.8763810, https://ieeexplore.ieee.org/document/8763810.

[16] FUJDIAK, R.; MLÝNEK, P.; BLAŽEK, P.; aj.: Seeking the Relation between Performance and Security in Modern Systems: Metrics and Measures. In *41st Inoternational Conference on Telecommunications and Signal Processing (TSP)*, ročník 41, 2018, ISBN 978-1-5386-4695-3, ISSN 1805-5435, s. 288–293, doi:10.1109/TSP.2018.8441496.

[17] FUJDIAK, R.; MLÝNEK, P.; MRNUSTIK, P.; aj.: Managing the Secure Software Development. In *2019 10th IFIP Inoternational Conference on New Technologies, Mobility and Security (NTMS)*, 2019, ISBN 978-1-7281-1542-9, s. 1–4, doi:10.1109/NTMS.2019.8763845, https://ieeexplore.ieee.org/abstract/document/8763845.

[18] Fujdiak, R.; Mlýnek, P.; Malina, L.; aj.: Development of IQRF Technology: Analysis, Simulations and Experimental Measurements. *Elektronika Ir Elektrotechnika*, ročník 25, č. 1, 2019: s. 72–79, ISSN 1392-1215, doi:10.5755/j01.eie.25.2.22739, http://eejournal.ktu.lt/index.php/elt/article/view/22739.

[19] FUJDIAK, R.; POKORNÝ, J.; ZOBAL, L.; aj.: Security and Performance Trade-offs for Data Distribution Service in Flying Ad-Hoc Networks. In *2019 11th Inoternational Congress on Ultra Modern Telecommunications and Control Systems and Workshops (ICUMT)*, Ireland, Dublin, 2019, ISBN 978-1-7281-5763-4, s. 1–5, doi:10.1109/ICUMT48472.2019.8970670, https://ieeexplore.ieee.org/document/8970670.

[20] FUJDIAK, R.; UHER, V.; MLÝNEK, P.; aj.: IP traffic generator using container virtualization technology. In *10th Inoternational Congress on Ultra Modern Telecommunications and Control Systems and Workshops (ICUMT)*, 2018, ISBN 978-1-5386-9361-2, s. 1–6, doi:10.1109/ICUMT.2018.8631248, https://ieeexplore.ieee.org/document/8631248.

[21] Gerlich, T.; Blažek, P.: Srovnání systémů Suricata a Snort pro detekci útoků cílených na odepření služeb. *Elektrorevue - Inoternetový časopis (http://www.elektrorevue.cz)*, ročník 19, č. 6, 2017: s. 188–194, ISSN 1213-1539.

[22] Gerlich, T.; Blažek, P.; Churý, J.: Analýza filtračních schopností linuxových nástrojů. Praha, 2018, s. 31–32.

[23] Holasová, E.; Blažek, P.; Fujdiak, R.; aj.: Exploring the Power of Convolutional Neural Networks for Encrypted Industrial Protocols Recognition. *Sustainable Energy, Grids and Networks*, ročník 38, č. June 2024, 2024: s. 1–11, ISSN 2352-4677, doi:10.1016/j.segan.2023.101269, `https://www.sciencedirect.com/science/article/abs/pii/S2352467723002771`.

[24] Holasová, E.; Fujdiak, R.; Blažek, P.; aj.: Automated Neural Network Structure Design for Efficient Anomaly Identification. In *ICCNS 2023 Proceedings*, 2023, ISBN 979-8-4007-0796-4, s. 1–7.

[25] Holasová, E.; Kuchař, K.; Fujdiak, R.; aj.: Security Modules for Securing Industrial Networks. In *2021 2nd Inoternational Conference on Electronics, Communications and Information Technology (CECIT 2021)*, Institute of Electrical and Electronics Engineers Inc., 2022, ISBN 978-1-6654-3757-8, s. 1125–1132, doi:10.1109/CECIT53797.2021.00199, `https://ieeexplore.ieee.org/document/9742069`.

[26] Kuchař, K.; Blažek, P.: Identifying Anomalies in Industrial Networks: A Proposed Testbed for Experimental Evaluation. In *Proceedings II of the 29th Student EEICT 2023*, 1, Brno: Brno University of Technology, 2023, ISBN 978-80-214-6154-3, ISSN 2788-1334, s. 264–268, doi:10.13164/eeict.2023.264, `https://www.eeict.cz/eeict_download/archiv/sborniky/EEICT_2023_sbornik_2_v2.pdf`.

[27] Kuchař, K.; Blažek, P.; Fujdiak, R.: From Playground to Battleground: Cyber Range Training for Industrial Cybersecurity Education. In *ICCNS 2023 Proceedings*, 2023, ISBN 979-8-4007-0796-4, s. 1–6, doi:10.1145/3638782.3638814.

[28] Kuchař, K.; Fujdiak, R.; Blažek, P.; aj.: Simplified Method for Fast and Efficient Incident Detection in Industrial Networks. In *4th Cyber Security in Networking Conference*, 2020, ISBN 978-0-7381-4292-0, s. 1–3, doi:10.1109/CSNet50428.2020.9265536.

[29] Kuchař, K.; Holasová, E.; Fujdiak, R.; aj.: *Incident Detection System for Industrial Networks*. Springer, první vydání, 2022, ISBN 978-3-031-04424-3, s. 83–102, doi:10.1007/978-3-031-04424-3_5, `https://link.springer.com/chapter/10.1007/978-3-031-04424-3_5`.

[30] Martinásek, Z.; Blažek, P.: Zátěžové testování odolnosti vůči DDoS útokům webových serverů. 2017, summary research report - contract. research.

[31] Martinásek, Z.; Blažek, P.; Šilhavý, P.; aj.: Methodology for Correlations Discovery in Security Logs. In *2017 9th Inoternational Congress on Ultra Modern Telecommunications and Control Systems and Workshops (ICUMT)*, Mnichov, Německo, 2017, ISBN 978-1-5386-3434-9, s. 294–298, doi:10.1109/ICUMT.2017.8255194, `https://ieeexplore.ieee.org/document/8255194`.

[32] Mlýnek, P.; Fujdiak, R.; Sláčik, J.; aj.: Zátěžový generátor provozu energetických protokolů - emulace provozu distribuční trafostanice pro ověření komunikačních technologií. In *ČK CIRED 2019*, 2019, ISBN 978-80-905014-8-5, s. 1–8.

[33] Mlýnek, P.; Šilhavý, P.; Sláčik, J.; aj.: Broadband PLC on Medium Voltage - Performance Measurements. In *Proceeding of ICUMT 2019*, 2019, ISBN 978-1-7281-5763-4, s. 1–5, doi: 10.1109/ICUMT48472.2019.8970818, `https://ieeexplore.ieee.org/document/8970818`.

[34] Pospíšil, O.; Blažek, P.; Fujdiak, R.; aj.: Active Scanning in the Industrial Control Systems. In *2021 Inoternational Symposium on Computer Science and Inotelligent Control (ISCSIC)*, Rome, Italy: IEEE CPS, 2021, ISBN 978-1-6654-1627-6, s. 1–6, doi:10.1109/ISCSIC54682.2021.00049, `https://ieeexplore.ieee.org/document/9644373/`.

[35] Pospíšil, O.; Blažek, P.; Kuchař, K.; aj.: Application Perspective on Cybersecurity Testbed for Industrial Control Systems. *SENSORS*, ročník 21, č. 23, 2021: s. 1–38, ISSN 1424-8220, doi:10.3390/s21238119, `https://www.mdpi.com/1424-8220/21/23/8119`.

[36] Sikora, M.; Blažek, P.: Systém prevence průniku Slow HTTP DoS a DDoS útoků. *Elektrorevue - Inoternetový časopis (http://www.elektrorevue.cz)*, ročník 19, č. 4, 2017: s. 1–8, ISSN 1213-1539.

[37] Sikora, M.; Krivulčík, A.; Fujdiak, R.; aj.: Design of Advanced Slow Denial of Service Attack Generator. In *2020 12th Inoternational Congress on Ultra Modern Telecommunications and Control Systems and Workshops (ICUMT)*, IEEE, 2020, ISBN 978-1-7281-9281-9, ISSN 2157-023X, s. 1–6, doi:10.1109/ICUMT51630.2020.9222423, `https://ieeexplore.ieee.org/document/9222423`.

[38] Sikora, M.; Krivulčík, A.; Fujdiak, R.; aj.: Návrh pokročilého generátoru pomalých DoS a DDoS útoků. *Elektrorevue - Inoternetový časopis (http://www.elektrorevue.cz)*, ročník 22, č. 3, 2020: s. 1–7, ISSN 1213-1539.

[39] Sikora, M.; Zeman, V.; Číka, P.; aj.: Zátěžový tester informačních a komunikačních technologií. *Elektrorevue - Inoternetový časopis (http://www.elektrorevue.cz)*, ročník 24, č. 2, 2022: s. 70–77, ISSN 1213-1539.

[40] Smékal, D.; Blažek, P.: High-Speed anomaly detection system using entropy calculation on FPGA. In *Proceedings of the 23rd Conference STUDENT EEICT 2017*, první, Brno: Vysoké učení technické v Brně, Fakulta elektrotechniky a komunikačních technologií, 2017, ISBN 978-80-214-5496-5, s. 415–419, `http://eeict.feec.vutbr.cz/2017/sbornik/EEICT_2017-sbornik-komplet-2.pdf`.

[41] Vrtal, M.; Benedikt, J.; Topolánek, D.; aj.: Power Grid and Data Network Simulator. In *Proceedings of the 2022 22nd Inoternational Scientific Conference on Electric Power Engineering (EPE)*, 1, New York: IEEE, 2022, ISBN 978-1-6654-1057-1, str. 4, doi:10.1109/EPE54603.2022.9814104, `https://ieeexplore.ieee.org/document/9814121`.

Literatura

[42] Cybersecurity protection for power grid control infrastructures. *International Journal of Critical Infrastructure Protection*, ročník 18, 2017: s. 20–33, ISSN 1874-5482, doi:https://doi.org/10.1016/j.ijcip.2017.07.002.

[43] IEEE Standard for Intelligent Electronic Devices Cybersecurity Capabilities. *IEEE Std 1686-2022 (Revision of IEEE Std 1686-2013)*, 2023: s. 1–36, doi:10.1109/IEEESTD.2023.10034445.

[44] IEEE Standard for Smart Energy Profile Application Protocol. *IEEE Std 2030.5-2023 (Revision of IEEE Std 2030.5-2018/Incorporates IEEE Std 2030.5-2023/Cor1-2024)*, 2024: s. 1–398, doi:10.1109/IEEESTD.2024.10785536.

[45] Adepu, S.; Kandasamy, N. K.; Mathur, A.: EPIC: An Electric Power Testbed for Research and Training in Cyber Physical Systems Security. In *Computer Security*, editace S. K. Katsikas; F. Cuppens; N. Cuppens; C. Lambrinoudakis; A. Antón; S. Gritzalis; J. Mylopoulos; C. Kalloniatis, Cham: Springer International Publishing, 2019, ISBN 978-3-030-12786-2, s. 37–52.

[46] Adhikari, U.; Morris, T.; Pan, S.: WAMS Cyber-Physical Test Bed for Power System, Cybersecurity Study, and Data Mining. *IEEE Transactions on Smart Grid*, ročník 8, č. 6, 2017: s. 2744–2753, doi:10.1109/TSG.2016.2537210.

[47] Aghamolki, H. G.; Miao, Z.; Fan, L.: A hardware-in-the-loop SCADA testbed. In *2015 North American Power Symposium (NAPS)*, 2015, s. 1–6, doi:10.1109/NAPS.2015.7335093.

[48] Ahmad, S.; Ahn, B.; Alvee, S. R. B.; aj.: Advanced Persistent Threat (APT)-Style Attack Modeling and Testbed for Power Transformer Diagnosis System in a Substation. In *2022 IEEE Power & Energy Society Innovative Smart Grid Technologies Conference (ISGT)*, 2022, s. 1–5, doi:10.1109/ISGT50606.2022.9817518.

[49] Ahmed, C. M.; Kandasamy, N. K.: A Comprehensive Dataset from a Smart Grid Testbed for Machine Learning Based CPS Security Research. In *Cyber-Physical Security for Critical Infrastructures Protection (CPS4CIP 2020), Revised Selected Papers*, *Lecture Notes in Computer Science*, ročník 12618, 2021, s. 123–135, doi:10.1007/978-3-030-69781-5_9.

[50] Alani, M.; Baker, T.: A Survey of Smart Grid Intrusion Detection Datasets. 06 2023, ISBN 9781643684048, doi:10.3233/AISE230004.

[51] Almgren, M.; Andersson, P.; Björkman, G.; aj.: *RICS-el: Building a National Testbed for Research and Training on SCADA Security (Short Paper): 13th International Conference, CRITIS 2018, Kaunas, Lithuania, September 24-26, 2018, Revised Selected Papers*. 01 2019, ISBN 978-3-030-05848-7, s. 219–225, doi:10.1007/978-3-030-05849-4_17.

[52] Alrashide, A.; Abdelrahman, M. S.; Kharchouf, I.; aj.: GNS3 Communication Network Emulation for Substation GOOSE Based Protection Schemes. In *2022 IEEE International Conference on Environment and Electrical Engineering and 2022 IEEE Industrial and Commercial Power Systems Europe (EEEIC / I&CPS Europe)*, 2022, s. 1–6, doi:10.1109/EEEIC/ICPSEurope54979.2022.9854689.

[53] Ashok, A.; Krishnaswamy, S.; Govindarasu, M.: PowerCyber: A remotely accessible testbed for Cyber Physical security of the Smart Grid. In *2016 IEEE Power & Energy Society Innovative Smart Grid Technologies Conference (ISGT)*, 2016, s. 1–5, doi:10.1109/ISGT.2016.7781277.

[54] Assante, M. J.; Lee, R. M.; Conway, T.: German Steel Mill Cyber Attack. Industrial control systems case study, SANS Institute, 2014, `https://ics.sans.org/media/ICS-CPPE-case-Study-2-German-Steelworks_Facility.pdf`.

[55] Baezner, M.; Cordey, S.: Hotspot Analysis: Cyber and Information Warfare in the Ukrainian Conflict. Hotspot analysis, Center for Security Studies, ETH Zürich, Říjen 2018, `https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/20181003_MB_HS_RUS-UKR%20V2_rev.pdf`.

[56] Bencsáth, B.; Pék, G.; Buttyán, L.; aj.: The Cousins of Stuxnet: Duqu, Flame, and Gauss. *Future Internet*, ročník 4, č. 4, 2012: s. 971–1003, doi:10.3390/fi4040971.

[57] CEN-CENELEC-ETSI Smart Grid Coordination Group: SGAM User Manual – Applying, testing & refining the Smart Grid Architecture Model (SGAM). SG-CG/M490/K, CEN-CENELEC-ETSI, Luxembourg, 2014.

[58] Cheminod, M.; Durante, L.; Valenzano, A.: Review of security issues in industrial networks. *IEEE Transactions on Industrial Informatics*, ročník 9, č. 1, 2013: s. 277–293, doi:10.1109/TII.2012.2198666.

[59] Cherepanov, A.; Lipovsky, R.: GreyEnergy: A successor to BlackEnergy. Technická zpráva, ESET Research, 2018, white-paper analysing GreyEnergy/TeleBots activity.

[60] (CISA), I.: ICS Focused Malware (Havex) Alert ICSA-14-178-01. Technická zpráva, U.S. Department of Homeland Security, CISA, Červen 2014, `https://www.cisa.gov/news-events/ics-advisories/icsa-14-178-01`.

[61] Conti, M.; Donadel, D.; Turrin, F.: A Survey on Industrial Control System Testbeds and Datasets for Security Research. *IEEE Communications Surveys & Tutorials*, ročník 23, č. 4, 2021: str. 2248–2294, ISSN 2373-745X, doi:10.1109/comst.2021.3094360, `http://dx.doi.org/10.1109/COMST.2021.3094360`.

[62] Cordey, S.: Trend Analysis: The Israeli Unit 8200 – An OSINT-based study. Cyber defense report, Center for Security Studies (CSS), ETH Zürich, Prosinec 2019, `https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/Cyber-Reports-2019-12-Unit-8200.pdf`.

[63] CrySyS Lab (Budapest University of Technology and Economics): Duqu: A Stuxnet-like malware found in the wild. *CrySyS Technical Report*, Oct 2011.

[64] Dayal, A.; Deng, Y.; Tbaileh, A.; aj.: VSCADA: A reconfigurable virtual SCADA test-bed for simulating power utility control center operations. In *2015 IEEE Power & Energy Society General Meeting*, 2015, s. 1–5, doi:10.1109/PESGM.2015.7285822.

[65] Dehlawi, Z.; Abokhodair, N.: Saudi Arabia's Response to Cyber Conflict: A Case Study of the Shamoon Malware Incident. In *2013 IEEE International Conference on Intelligence and Security Informatics (ISI)*, 2013, doi:10.1109/ISI.2013.6578789.

[66] Deng, W.; Pei, W.; Shen, Z.; aj.: IEC 61850 based testbed for micro-grid operation, control and protection. In *2015 5th International Conference on Electric Utility Deregulation and Restructuring and Power Technologies (DRPT)*, 2015, s. 2154–2159, doi:10.1109/DRPT.2015.7432606.

[67] Elbez, G.; Keller, H. B.; Hagenmeyer, V.: A Cost-efficient Software Testbed for Cyber-Physical Security in IEC 61850-based Substations. In *2018 IEEE International Conference on Communications, Control, and Computing Technologies for Smart Grids (SmartGridComm)*, 2018, s. 1–6, doi:10.1109/SmartGridComm.2018.8587456.

[68] ENISA: Communication network interdependencies in smart grids. Technická zpráva, ENISA, 2015.

[69] ENISA: NCSS Good Practice Guide. Technická zpráva, ENISA, 2016, doi:10.2824/48036.

[70] ENISA: Good Practices for Security of Internet of Things in the context of Smart Manufacturing. Technická zpráva, ENISA, 2018, doi:10.2824/851384.

[71] ENISA: ENISA Threat Landscape 2019/2020 - The year in review. Technická zpráva, ENISA, 2020, doi:10.2824/552242.

[72] ENISA: ENISA THREAT LANDSCAPE 2021. Technická zpráva, ENISA, 2021, doi:10.2824/324797.

[73] ENISA: ENISA THREAT LANDSCAPE 2022. Technická zpráva, ENISA, 2022, doi:10.2824/764318.

[74] ENISA: ENISA THREAT LANDSCAPE 2023. Technická zpráva, ENISA, 2023, doi:10.2824/782573.

[75] ENISA: GOOD PRACTICES FOR SUPPLY CHAIN CYBERSECURITY. Technická zpráva, ENISA, 2023, doi:10.2824/805268.

[76] ENISA: BEST PRACTICES FOR CYBER CRISIS MANAGEMENT. Technická zpráva, ENISA, 2024, doi:10.2824/767828.

[77] ENISA: ENISA THREAT LANDSCAPE 2024. Technická zpráva, ENISA, 2024, doi:10.2824/0710888.

[78] European Union Agency for Cybersecurity (ENISA): Appropriate security measures for smart grids: Guidelines to assess the sophistication of security measures implementation. ENISA Report, ENISA, Prosinec 2012, available online via ENISA Publications.

[79] European Union Agency for Cybersecurity (ENISA): Industry 4.0 Cybersecurity: Challenges & Recommendations. ENISA Report, ENISA, Květen 2019, `https://www.enisa.europa.eu/sites/default/files/publications/Industry%204.0%20-%20Cybersecurity%20Challenges%20and%20Recommendations.pdf`.

[80] European Union Agency for Cybersecurity (ENISA): Stock-taking of information security training needs in critical sectors. ENISA Report, ENISA, 2020, mapping of training needs for critical infrastructure sectors.

[81] Fan, Z.; Kulkarni, P.; Görmüs, S.; aj.: Smart Grid communications: Overview of research challenges, solutions, and standardization activities. *IEEE Communications Surveys & Tutorials*, ročník 15, č. 1, 2013: s. 21–38, doi:10.1109/SURV.2011.122211.00021.

[82] Fang, X.; Misra, S.; Xue, G.; aj.: Smart Grid – The New and Improved Power Grid: A Survey. *IEEE Communications Surveys & Tutorials*, ročník 14, č. 4, 2012: s. 944–980, doi: 10.1109/SURV.2011.101911.00087.

[83] Fang, X.; Misra, S.; Xue, G.; aj.: Smart Grid – The New and Improved Power Grid: A Survey. *IEEE Communications Surveys & Tutorials*, ročník 14, č. 4, 2012: s. 944–980, doi: 10.1109/SURV.2011.101911.00087.

[84] Figueroa-Lorenzo, S.; Añorga, J.; Arrizabalaga, S.: A Role-Based Access Control Model in Modbus SCADA Systems. A Centralized Model Approach. *Sensors*, ročník 19, č. 20, 2019: str. 4455, doi:10.3390/s19204455.

[85] Fu, Q.; Chen, J.: Design of experiment platform for digital substation based on IEC 61850. In *2016 5th International Conference on Computer Science and Network Technology (ICCSNT)*, 2016, s. 4–8, doi:10.1109/ICCSNT.2016.8069368.

[86] Hatzivasilis, G.; Ioannidis, S.; Smyrlis, M.; aj.: The THREAT-ARREST Cyber Range Platform. In *2021 IEEE International Conference on Cyber Security and Resilience (CSR)*, 2021, s. 422–427, doi:10.1109/CSR51186.2021.9527963.

[87] Hemmati, M.; Palahalli, H.; Gruosso, G.; aj.: Interoperability analysis of IEC61850 protocol using an emulated IED in a HIL microgrid testbed. In *2021 IEEE International Conference on Communications, Control, and Computing Technologies for Smart Grids (SmartGridComm)*, 2021, s. 152–157, doi:10.1109/SmartGridComm51999.2021.9632327.

[88] Holt, C.; Kong, A.; Leger, A. S.; aj.: Communications network emulation for smart grid test-bed. In *2016 IEEE Power and Energy Society General Meeting (PESGM)*, 2016, s. 1–5, doi:10.1109/PESGM.2016.7741999.

[89] Hong, J.; Girdhar, M.; Ten, C.-W.; aj.: Cybersecurity of Sampled Value Messages in Substation Automation System. In *2022 IEEE Power & Energy Society General Meeting (PESGM)*, 2022, s. 1–1, doi:10.1109/PESGM48719.2022.9916758.

[90] Hong, J.; Nuqui, R. F.; Kondabathini, A.; aj.: Cyber Attack Resilient Distance Protection and Circuit Breaker Control for Digital Substations. *IEEE Transactions on Industrial Informatics*, ročník 15, č. 7, 2019: s. 4332–4341, doi:10.1109/TII.2018.2884728.

[91] Huang, H.; Davis, C.; Davis, K.: Real-time Power System Simulation with Hardware Devices through DNP3 in Cyber-Physical Testbed. feb 2021, doi:10.1109/tpec51183.2021.9384947.

[92] Huang, H.; Wlazlo, P.; Mao, Z.; aj.: Cyberattack Defense With Cyber-Physical Alert and Control Logic in Industrial Controllers. *IEEE Transactions on Industry Applications*, ročník 58, č. 5, 2022: s. 5921–5934, doi:10.1109/TIA.2022.3186660.

[93] Idehen, I.; Overbye, T.; Klemesrud, L.: An Electric Power System Energy Management Platform (EMP) Research Testbed. In *2020 IEEE Texas Power and Energy Conference (TPEC)*, 2020, s. 1–6, doi:10.1109/TPEC48276.2020.9042576.

[94] IEEE: IEEE Recommended Practice for Data Communications Between Remote Terminal Units and Intelligent Electronic Devices in a Substation (IEEE Std 1379-2000). IEEE Std 1379-2000 (R2006), IEEE, Březen 2001, approved 2000-09-21; published 2001-03-16; withdrawn 2012-01-10.

[95] IEEE: Recommended Practice for Data Communications Between Remote Terminal Units and Intelligent Electronic Devices in a Substation (IEEE Std 1379-2000). IEEE Std 1379-2000 (Revision of IEEE Std 1379-1997), IEEE, Březen 2001, approved 21 September 2000; published 16 March 2001; withdrawn 10 January 2012.

[96] IEEE: Precision Clock Synchronization Protocol for Networked Measurement and Control Systems (IEEE Std 1588-2019; adopted as IEC 61588-2021). Technická zpráva, IEEE, Červen 2020.

[97] INCIBE-CERT: BLACKENERGY ICS malware analysis study. Technická zpráva, INCIBE, Únor 2024, analysis of malware evolution and industrial impact.

[98] Institute, E. . S.: Analysis of the Cyber Attack on the Ukrainian Power Grid. Březen 2016, technical report on December 23, 2015 outages.

[99] International Electrotechnical Commission: Telecontrol equipment and systems – Part 5-1: Transmission frame formats. International Standard IEC 60870-5-1:1990, IEC, Geneva, 1990.

[100] International Electrotechnical Commission: Telecontrol equipment and systems – Part 5-2: Data link transmission services. International Standard IEC 60870-5-2:1992, IEC, Geneva, 1992.

[101] International Electrotechnical Commission: Telecontrol equipment and systems – Part 5-3: General structure of application data. International Standard IEC 60870-5-3:1992, IEC, Geneva, 1992.

[102] International Electrotechnical Commission: Telecontrol equipment and systems – Part 5-4: Definition and coding of information elements. International Standard IEC 60870-5-4:1993, IEC, Geneva, 1993.

[103] International Electrotechnical Commission: Telecontrol equipment and systems – Part 6-601: Functional profile for providing connection-oriented transport service. International Standard IEC 60870-6-601:1994, IEC, Geneva, 1994.

[104] International Electrotechnical Commission: Telecontrol equipment and systems – Part 5-101: Companion standard for basic telecontrol tasks. International Standard IEC 60870-5-101:1995, IEC, Geneva, 1995.

[105] International Electrotechnical Commission: Telecontrol equipment and systems – Part 5-5: Basic application functions. International Standard IEC 60870-5-5:1995, IEC, Geneva, 1995.

[106] International Electrotechnical Commission: Telecontrol equipment and systems – Part 6-501: TASE.1 Service definitions. International Standard IEC 60870-6-501:1995, IEC, Geneva, 1995.

[107] International Electrotechnical Commission: Telecontrol equipment and systems – Part 6-502: TASE.1 Protocol definitions. International Standard IEC 60870-6-502:1995, IEC, Geneva, 1995.

[108] International Electrotechnical Commission: Telecontrol equipment and systems – Part 5-102: Companion standard for transmission of integrated totals. International Standard IEC 60870-5-102:1996, IEC, Geneva, 1996.

[109] International Electrotechnical Commission: Telecontrol equipment and systems – Part 5-103: Companion standard for interface of protection equipment. International Standard IEC 60870-5-103:1997, IEC, Geneva, 1997.

[110] International Electrotechnical Commission: Telecontrol equipment and systems – Part 6-701: Functional profile for providing the TASE.1 application service. International Standard IEC 60870-6-701:1998, IEC, Geneva, 1998.

[111] International Electrotechnical Commission: Telecontrol equipment and systems – Part 6-602: Telecontrol protocols compatible with ISO and ITU-T – TASE transport profiles. Technical Specification IEC TS 60870-6-602:2001, IEC, Geneva, 2001.

[112] International Electrotechnical Commission: Telecontrol equipment and systems – Part 6-505: TASE.2 User guide. Technical Report IEC TR 60870-6-505:2002, IEC, Geneva, 2002.

[113] International Electrotechnical Commission: Communication networks and systems for power utility automation – Part 8-1: Mappings to MMS. IEC 61850-8-1:2004+AMD1:2020, IEC, Geneva, 2004.

[114] International Electrotechnical Commission: Telecontrol equipment and systems – Part 5-104: Companion standard – Network access using standard transport profiles. International Standard IEC 60870-5-104:2006+AMD1:2016, IEC, Geneva, 2006.

[115] International Electrotechnical Commission: Telecontrol equipment and systems – Part 5-6: Guidelines for conformance testing. International Standard IEC 60870-5-6:2006, IEC, Geneva, 2006.

[116] International Electrotechnical Commission: Power systems management and associated information exchange – Data and communications security. Part 1: Communication network and system security – Introduction to security issues. Technical Specification IEC TS 62351-1:2007(E), IEC, Geneva, Květen 2007.

[117] International Electrotechnical Commission: Communication networks and systems for power utility automation – Part 6: Configuration description language (SCL). IEC 61850-6:2009+AMD1:2018+AMD2:2024, IEC, Geneva, 2009.

[118] International Electrotechnical Commission: Industrial communication networks – Network and system security – Part 1-1: Terminology, concepts and models. IEC 62443-1-1:2009, IEC, Geneva, 2009.

[119] International Electrotechnical Commission: Communication networks and systems for power utility automation – Part 7-2: Basic information and communication structure – Abstract communication service interface (ACSI). IEC 61850-7-2:2010+AMD1:2020, IEC, Geneva, 2010.

[120] International Electrotechnical Commission: Communication networks and systems for power utility automation – Part 7-3: Basic communication structure – Common data classes. IEC 61850-7-3:2010+AMD1:2020, IEC, Geneva, 2010.

[121] International Electrotechnical Commission: Communication networks and systems for power utility automation – Part 7-4: Basic communication structure – Compatible logical node classes and data object classes. IEC 61850-7-4:2010+AMD1:2020, IEC, Geneva, 2010.

[122] International Electrotechnical Commission: Communication networks and systems for power utility automation – Part 90-1: Use of IEC 61850 for the communication between substations. IEC TR 61850-90-1:2010(E), IEC, Geneva, 2010.

[123] International Electrotechnical Commission: Communication networks and systems for power utility automation – Part 7-1: Principles and models. IEC 61850-7-1:2011+AMD1:2020, IEC, Geneva, 2011.

[124] International Electrotechnical Commission: Communication networks and systems for power utility automation – Part 9-2: Sampled values over Ethernet. IEC 61850-9-2:2011+AMD1:2020, IEC, Geneva, 2011.

[125] International Electrotechnical Commission: Communication networks and systems for power utility automation – Part 7-410: Basic communication structure – Hydroelectric power plants. IEC 61850-7-410:2012+AMD1:2015, IEC, Geneva, 2012.

[126] International Electrotechnical Commission: Communication networks and systems for power utility automation – Part 90-5: Use of IEC 61850 to transmit synchrophasor information according to IEEE C37.118. IEC TR 61850-90-5:2012, IEC, Geneva, 2012.

[127] International Electrotechnical Commission: Communication networks and systems for power utility automation – Part 5: Communication requirements for functions and device models. IEC 61850-5:2013+AMD1:2022, IEC, Geneva, 2013.

[128] International Electrotechnical Commission: Security for industrial automation and control systems – Part 3-3: System security requirements and security levels. IEC 62443-3-3:2013, IEC, Geneva, 2013.

[129] International Electrotechnical Commission: Telecontrol equipment and systems – Part 5-7: Security extensions to IEC 60870-5-101 and IEC 60870-5-104. Technical Specification IEC TS 60870-5-7:2013(E), IEC, Geneva, 2013.

[130] International Electrotechnical Commission: Telecontrol equipment and systems – Part 6-503: TASE.2 Services and protocol. International Standard IEC 60870-6-503:2014, IEC, Geneva, 2014.

[131] International Electrotechnical Commission: Telecontrol equipment and systems – Part 6-702: Functional profile for providing the TASE.2 application service. International Standard IEC 60870-6-702:2014, IEC, Geneva, 2014.

[132] International Electrotechnical Commission: Telecontrol equipment and systems – Part 6-802: TASE.2 Object models. International Standard IEC 60870-6-802:2014, IEC, Geneva, 2014.

[133] International Electrotechnical Commission: Telecontrol equipment and systems – Part 5-601: Transmission protocols – Conformance test cases for the IEC 60870-5-101 companion standard. Technical Specification IEC TS 60870-5-601:2015(E), IEC, Geneva, 2015.

[134] International Electrotechnical Commission: Telecontrol equipment and systems – Part 5-604: Conformance test cases for the IEC 60870-5-104 companion standard. Technical Specification IEC TS 60870-5-604:2016(E), IEC, Geneva, 2016.

[135] International Electrotechnical Commission: Power systems management and associated information exchange – Data and communications security. Part 7: Network and System Management data object models. International Standard IEC 62351-7:2017, IEC, Geneva, 2017.

[136] International Electrotechnical Commission: Power systems management and associated information exchange – Data and communications security. Part 4: Security for profiles including MMS. International Standard IEC 62351-4:2018+AMD1:2020, IEC, Geneva, 2018.

[137] International Electrotechnical Commission: Security for industrial automation and control systems – Part 4-1: Secure product development lifecycle requirements. IEC 62443-4-1:2018, IEC, Geneva, 2018.

[138] International Electrotechnical Commission: Security for industrial automation and control systems – Part 4-2: Technical security requirements for IACS components. IEC 62443-4-2:2019, IEC, Geneva, 2019.

[139] International Electrotechnical Commission: Communication networks and systems for power utility automation – Part 90-4: Network engineering guidelines. IEC TR 61850-90-4:2020, IEC, Geneva, 2020.

[140] International Electrotechnical Commission: Communication networks and systems for power utility automation – Part 90-9: Use of IEC 61850 for Electrical Energy Storage Systems. IEC TR 61850-90-9:2020, IEC, Geneva, 2020.

[141] International Electrotechnical Commission: Power systems management and associated information exchange – Data and communications security. Part 6: Security for IEC 61850 profiles. International Standard IEC 62351-6:2020, IEC, Geneva, 2020.

[142] International Electrotechnical Commission: Power systems management and associated information exchange – Data and communications security. Part 8: Role-based access control. International Standard IEC 62351-8:2020, IEC, Geneva, 2020.

[143] International Electrotechnical Commission: Security for industrial automation and control systems – Part 3-2: Security risk assessment and system design. IEC 62443-3-2:2020, IEC, Geneva, 2020.

[144] International Electrotechnical Commission: Communication networks and systems for power utility automation – Part 7-510: Turbines modeling concepts and guidelines. IEC TR 61850-7-510:2021, IEC, Geneva, 2021.

[145] International Electrotechnical Commission: Industrial communication networks – High-availability automation networks – Part 3: Parallel Redundancy Protocol (PRP) and High-availability Seamless Redundancy (HSR). IEC 62439-3:2021 (revision of IEC 62439-3:2016), IEC, Geneva, 2021.

[146] International Electrotechnical Commission: Communication networks and systems for power utility automation – Part 90-7: Object models for power converters in distributed energy resources systems. IEC TR 61850-90-7:2023, IEC, Geneva, 2023.

[147] International Electrotechnical Commission: Power systems management and associated information exchange – Data and communications security. Part 3: Communication network and system security – Profiles including TCP/IP. International Standard IEC 62351-3:2023, IEC, Geneva, 2023.

[148] International Electrotechnical Commission: Power systems management and associated information exchange – Data and communications security. Part 5: Security for profiles including IEC 60870-5 and DNP3. International Standard IEC 62351-5:2023, IEC, Geneva, 2023.

[149] International Electrotechnical Commission: Power systems management and associated information exchange – Data and communications security. Part 9: Cyber security key management for power system equipment. International Standard IEC 62351-9:2023, IEC, Geneva, 2023.

[150] International Electrotechnical Commission: Security for industrial automation and control systems – Part 2-4: Requirements for IACS service providers. IEC 62443-2-4:2023, IEC, Geneva, 2023.

[151] International Electrotechnical Commission: Security for industrial automation and control systems – Part 2-1: Security program requirements for IACS asset owners. IEC 62443-2-1:2024, IEC, Geneva, 2024.

[152] International Electrotechnical Commission: Telecontrol equipment and systems – Part 6-1: Application context and organization of standards. Technical Report IEC 60870-6-1, IEC, Geneva, n.d.

[153] International Electrotechnical Commission: Telecontrol equipment and systems – Part 6-2: Use of basic standards (OSI layers 1–4). Technical Report IEC 60870-6-2, IEC, Geneva, n.d.

[154] ISO/IEC: Information technology – Open Systems Interconnection – Basic Reference Model: The Basic Model. ISO/IEC 7498-1:1994, ISO/IEC, Geneva, 1994.

[155] ISO/IEC: Industrial automation systems – Manufacturing Message Specification – Part 1: Service definition. ISO/IEC 9506-1:2003 (2nd edition), ISO/IEC, Geneva, Switzerland, 2003.

[156] Jarmakiewicz, J.; Maślanka, K.; Parobczak, K.: Development of cyber security testbed for critical infrastructure. In *2015 International Conference on Military Communications and Information Systems (ICMCIS)*, 2015, s. 1–10, doi:10.1109/ICMCIS.2015.7158687.

[157] Johnson, B.; Caban, D.; Krotofil, M.; aj.: Attackers Deploy New ICS Attack Framework "TRITON" and Cause Operational Disruption to Critical Infrastructure. *Mandiant (FireEye) Technical Blog*, Prosinec 2017, incident report detailing IT→OT intrusion, deployment on SIS engineering workstation, safe-state fail behavior.

[158] Jouini, M.; Ben Mnaouer, A.; Rabai, L. B. A.: Cyber security issues in SCADA networks: A survey. *Procedia Computer Science*, ročník 32, 2014: s. 1053–1060, doi:10.1016/j.procs.2014.03.064.

[159] Kabir-Querrec, M.; Mocanu, S.; Thiriet, J.-M.; aj.: A Test bed dedicated to the Study of Vulnerabilities in IEC 61850 Power Utility Automation Networks. In *2016 IEEE 21st International Conference on Emerging Technologies and Factory Automation (ETFA)*, 2016, s. 1–4, doi:10.1109/ETFA.2016.7733644.

[160] Karnouskos, S.: Stuxnet worm impact on industrial cyber-physical system security. In *IECON 2011 – 37th Annual Conference of the IEEE Industrial Electronics Society*, 2011, doi:10.1109/IECON.2011.6120048.

[161] Khan, F. B.; Asad, A.; Durad, H.; aj.: Dragonfly Cyber Threats: A Case Study of Malware Attacks Targeting Power Grids. *Journal of Computing & Biomedical Informatics*, ročník 4, č. 2, 2023: s. 172–185, doi:10.56979/402/2023.

[162] Khan, R.; Maynard, P.; McLaughlin, K.; aj.: Threat Analysis of BlackEnergy Malware for Synchrophasor based Real-time Control and Monitoring in Smart Grid. In *4th International Symposium for ICS & SCADA Cyber Security Research*, 2016, s. 53–63, doi:10.14236/ewic/ICS2016.7.

[163] Kleinrock, L.: *Queueing Systems. Volume I: Theory.* Wiley-Interscience, 1975, ISBN 9780471491101.

[164] Krishnan, V. V. G.; Gopal, S.; Nie, Z.; aj.: Cyber-power testbed for distributed monitoring and control. In *2018 Workshop on Modeling and Simulation of Cyber-Physical Energy Systems (MSCPES)*, 2018, s. 1–6, doi:10.1109/MSCPES.2018.8405400.

[165] Kushner, D.: The Real Story of Stuxnet. *IEEE Spectrum*, ročník 50, č. 3, 2013: s. 48–53, doi:10.1109/MSPEC.2013.6471059.

[166] Labonne, A.; Caire, R.; Braconnier, T.; aj.: Teaching Digital Control of Substation and IEC 61850 With a Test Bench Validation. *IEEE Transactions on Power Systems*, ročník 36, č. 2, 2021: s. 1175–1182, doi:10.1109/TPWRS.2020.3010446.

[167] Langner, R.: To Kill a Centrifuge: A Technical Analysis of What Stuxnet's Creators Tried to Achieve. Hotspot analysis, Center for Security Studies, ETH Zürich, 2013.

[168] Lee, S.; Lee, S.; Yoo, H.; aj.: Design and implementation of cybersecurity testbed for industrial IoT systems. *The Journal of Supercomputing*, ročník 74, 09 2018: str. 4506–4520, doi:10.1007/s11227-017-2219-z.

[169] León, H.; Montez, C.; Valle, O.; aj.: Real-Time Analysis of Time-Critical Messages in IEC 61850 Electrical Substation Communication Systems. *Energies*, ročník 12, 06 2019: str. 2272, doi:10.3390/en12122272.

[170] Mashima, D.; Roomi, M. M.; Ng, B.; aj.: Towards Automated Generation of Smart Grid Cyber Range for Cybersecurity Experiments and Training. In *2023 53rd Annual IEEE/IFIP International Conference on Dependable Systems and Networks - Supplemental Volume (DSN-S)*, 2023, s. 49–55, doi:10.1109/DSN-S58398.2023.00024.

[171] Maynard, P.; McLaughlin, K.; Sezer, S.: Modelling Duqu 2.0 Malware using Attack Trees with Sequential Conjunction. In *Proceedings of the 2nd International Conference on Information Systems Security and Privacy (ICISSP)*, 2016, s. 465–472, doi:10.5220/0005745704650472.

[172] Maynard, P.; Mclaughlin, K.; Sezer, S.: An Open Framework for Deploying Experimental SCADA Testbed Networks. 08 2018, s. 89–98, doi:10.14236/ewic/ICS2018.11.

[173] Maynard, P.; McLaughlin, K.; Sezer, S.: Decomposition and sequential-AND analysis of known cyber-attacks on critical infrastructure control systems. *International Journal of Critical Infrastructure Protection*, ročník 28, 2020: str. 100–112, doi:10.1016/j.ijcip.2020.100112.

[174] McDaniel, P.; McLaughlin, S.: Security and privacy challenges in the smart grid. *IEEE Security & Privacy*, ročník 7, č. 3, 2009: s. 75–77, doi:10.1109/MSP.2009.76.

[175] McLaughlin, S.; Konstantinou, C.; Wang, X.; aj.: The Cybersecurity Landscape in Industrial Control Systems. 2016, s. 1039–1057, doi:10.1109/JPROC.2015.2512235.

[176] Minh, Q. N.; Nguyen, V.; Quy, V. K.; aj.: Edge Computing for IoT-Enabled Smart Grid: The Future of Energy. *Energies*, ročník 15, č. 17, 2022: str. 6140, doi:10.3390/en15176140.

[177] MST Insurance Solutions, Inc.: Hack at Steel Mill Causes Physical Damage. Cyber case study, MST Insurance Solutions, 2021, https://mstis.com/wp-content/uploads/2021/08/Cyber-Case-Study-Hack-at-Steel-Mill-Causes-Physical-Damage.pdf.

[178] National Institute of Standards and Technology (NIST): Guide to Data-Centric System Threat Modeling. NIST Special Publication 800-154 (Draft), NIST, Gaithersburg, MD, USA, Březen 2016, draft version published for public comment.

[179] (NCCIC/ICS-CERT), C.: CRASHOVERRIDE Malware. Technická zpráva, Cybersecurity and Infrastructure Security Agency, Jul 2017, iCS-ALERT-17-206-01.

[180] Negi, R.; Kumar, P.; Ghosh, S.; aj.: Vulnerability Assessment and Mitigation for Industrial Critical Infrastructures with Cyber Physical Test Bed. In *2019 IEEE International Conference on Industrial Cyber Physical Systems (ICPS)*, 2019, s. 145–152, doi:10.1109/ICPHYS.2019.8780291.

[181] Nelson, N.: The Impact of Dragonfly Malware on Industrial Control Systems. GIAC Gold Certification Paper, SANS Institute, Leden 2016.

[182] Networks, N.; ICS-CSI: TRITON: The First ICS Cyber Attack on Safety Instrument Systems. Technická zpráva, Nozomi Networks / ICS-CSI, 2018, technical analysis white-paper; details TriStation protocol, payloads, reverse-engineering of Triconex PLC communication.

[183] Ngueta, G.; Lamine, M.; Sadeg, B.: Cybersecurity in smart grids: Challenges, technologies, and future directions. *Computer Standards & Interfaces*, ročník 75, 2021, doi:10.1016/j.csi.2021.103493.

[184] O'Toole, Z.; Moya, C.; Rubin, C.; aj.: A Cyber-Physical Testbed Design for the Electric Power Grid. In *2019 North American Power Symposium (NAPS)*, 2019, s. 1–5, doi:10.1109/NAPS46351.2019.9000312.

[185] Oyewumi, I. A.; Jillepalli, A. A.; Richardson, P.; aj.: ISAAC: The Idaho CPS Smart Grid Cybersecurity Testbed. In *2019 IEEE Texas Power and Energy Conference (TPEC)*, 2019, s. 1–6, doi:10.1109/TPEC.2019.8662189.

[186] Pirta-Dreimane, R.; Romanovs, A.; Bikovska, J.; aj.: Enhancing Smart Grid Resilience: An Educational Approach to Smart Grid Cybersecurity Skill Gap Mitigation. *Energies*, ročník 17, č. 8, 2024, doi:10.3390/en17081876.

[187] Ravikumar, G.; Hyder, B.; Govindarasu, M.: Efficient Modeling of IEC-61850 Logical Nodes in IEDs for Scalability in CPS Security Testbed. In *2020 IEEE/PES Transmission and Distribution Conference and Exposition (T&D)*, 2020, s. 1–5, doi:10.1109/TD39804.2020.9299665.

[188] Ravikumar, G.; Hyder, B.; Govindarasu, M.: Hardware-in-the-Loop CPS Security Architecture for DER Monitoring and Control Applications. In *2020 IEEE Texas Power and Energy Conference (TPEC)*, 2020, s. 1–5, doi:10.1109/TPEC48276.2020.9042578.

[189] Roomi, M. M.; Ong, W. S.; Hussain, S. M. S.; aj.: IEC 61850 Compatible OpenPLC for Cyber Attack Case Studies on Smart Substation Systems. *IEEE Access*, ročník 10, 2022: s. 9164–9173, doi:10.1109/ACCESS.2022.3144027.

[190] Salazar, L.; Castro, S.; Lozano, J.; aj.: A Tale of Two Industroyers: Technical Deep Dive into the 2016 Ukraine Power Grid Attack. *IEEE Symposium on Security and Privacy*, 2024, doi:10.1109/sp54263.2024.00162.

[191] Shostack, A.: *Threat Modeling: Designing for Security*. Indianapolis: Wiley, 2014, ISBN 978-1118809990.

[192] Singh, P.; Garg, S.; Kumar, V.; aj.: A testbed for SCADA cyber security and intrusion detection. In *2015 International Conference on Cyber Security of Smart Cities, Industrial Control System and Communications (SSIC)*, 2015, s. 1–6, doi:10.1109/SSIC.2015.7245683.

[193] Smadi, A. A.; Ajao, B. T.; Johnson, B. K.; aj.: A Comprehensive Survey on Cyber-Physical Smart Grid Testbed Architectures: Requirements and Challenges. *Electronics*, ročník 10, č. 9, 2021, ISSN 2079-9292, doi:10.3390/electronics10091043.
URL `https://www.mdpi.com/2079-9292/10/9/1043`

[194] of Standards, N. I.; Technology: Guide to Operational Technology (OT) Security. Technická Zpráva NIST Special Publication NIST SP 800-82r3, Change Notice 3 September 09, 2023, U.S. Department of Commerce, Washington, D.C., 2023, doi:https://doi.org/10.6028/NIST.SP.800-82r3.

[195] Tan, H. C.; Adeeb Hossain, M.; Mashima, D.; aj.: High-fidelity Intrusion Detection Datasets for Smart Grid Cybersecurity Research. 2024, s. 340–346, doi:10.1109/SmartGridComm60555.2024.10738043.

[196] Tebekaemi, E.; Wijesekera, D.: Designing An IEC 61850 Based Power Distribution Substation Simulation/Emulation Testbed for Cyber-Physical Security Studies. 10 2016, ISBN 978-1-61208-512-8, s. 41–49.

[197] Urias, V.; Van Leeuwen, B.; Richardson, B.: Supervisory Command and Data Acquisition (SCADA) system cyber security analysis using a live, virtual, and constructive (LVC) testbed. In *MILCOM 2012 - 2012 IEEE Military Communications Conference*, 2012, s. 1–8, doi:10.1109/MILCOM.2012.6415818.

[198] Valenzuela, J.; Wang, J.; Bissinger, N.: Real-time intrusion detection in SCADA systems. In *Proceedings of the 2013 IEEE Power and Energy Society General Meeting*, IEEE, 2013, doi:10.1109/PESMG.2013.6672480.

[199] Vellaithurai, C. B.; Biswas, S. S.; Srivastava, A. K.: Development and Application of a Real-Time Test Bed for Cyber–Physical System. *IEEE Systems Journal*, ročník 11, č. 4, 2017: s. 2192–2203, doi:10.1109/JSYST.2015.2476367.

[200] Xiao, B.; Starke, M.; King, D.; aj.: Implementation of system level control and communications in a Hardware-in-the-Loop microgrid testbed. In *2016 IEEE Power & Energy Society Innovative Smart Grid Technologies Conference (ISGT)*, 2016, s. 1–5, doi:10.1109/ISGT.2016.7781245.

[201] Xu, L.; Li, H.; Zhang, Z.; aj.: Performance Testing and Analysis of Multi-vendor IEDs under PRP Configuration. In *2020 IEEE 4th Conference on Energy Internet and Energy System Integration (EI2)*, 2020, s. 2108–2113, doi:10.1109/EI250167.2020.9346647.

[202] Yadav, G.; Paul, K.: Architecture and Security of SCADA Systems: A Review. *arXiv preprint*, ročník abs/2001.02925, 2020, review highlights vulnerabilities due to Internet connectivity and weak architecture.

[203] Yang, Y.; Jiang, H. T.; McLaughlin, K.; aj.: Cybersecurity test-bed for IEC 61850 based smart substations. In *2015 IEEE Power & Energy Society General Meeting*, 2015, s. 1–5, doi:10.1109/PESGM.2015.7286357.

[204] Yang, Z.; Wang, Y.; Xing, L.; aj.: Relay Protection Simulation and Testing of Online Setting Value Modification Based on RTDS. *IEEE Access*, ročník 8, 2020: s. 4693–4699, doi:10.1109/ACCESS.2019.2963228.

[205] Zhang, Y.; Wang, L.; Sun, H.; aj.: Distributed Intrusion Detection System in a Multi-Layer Network Architecture of Smart Grids. *IEEE Transactions on Smart Grid*, ročník 2, č. 4, 2011: s. 796–808, doi:10.1109/TSG.2011.2162040.

[206] Zhioua, S.: The Middle East under Malware Attack: Dissecting Cyber Weapons. *Proceedings of NFSP 2013 / King Fahd University, survey paper*, 2013.

[207] Zhu, R.; Hong, J.; Liu, C.-C.; aj.: Cyber System Recovery for IEC 61850 Substations. In *2021 IEEE Power & Energy Society Innovative Smart Grid Technologies Conference (ISGT)*, 2021, s. 1–5, doi:10.1109/ISGT49243.2021.9372195.

[208] Zhu, R.; Liu, C.-C.; Hong, J.; aj.: Intrusion Detection Against MMS-Based Measurement Attacks at Digital Substations. *IEEE Access*, ročník 9, 2021: s. 1240–1249, doi:10.1109/ACCESS.2020.3047341.

Seznam symbolů a zkratek

ACL Access Control List

ASN.1 Abstract Syntax Notation One

BPL Broadband over Powerline

CIM Common Information Model

CPS Cyber-Physical Systems

CT Current Transformer

DCS Distributed Control System

DMS Distribution Management System

DER Distributed Energy Resources

DNP3 Distributed Network Protocol verze 3

DoS Denial of Service (Odepření služby)

DSO Distribution System Operator

DSP Digital Signal Processing

DTS Distribution Transformer Station

GDPR General Data Protection Regulation

EMS Energy Management System

ERP Enterprise Resource Planning

GOOSE Generic Object Oriented Substation Events

HMI Human-Machine Interface

HSR High-availability Seamless Redundancy

ICS Industrial Control Systems

IED Intelligent Electronic Device

IoT Internet of Things

IP Internet Protocol

IPsec Internet Protocol Security

IT Information Technology

KPI Key Performance Indicator

LAN Local Area Network

LTE Long Term Evolution

MMS Manufacturing Message Specification

MTU	Master Terminal Unit
MU	Merging Unit
NN	Nízké napětí
OT	Operational Technology
PLC	Programmable Logic Controller
PRP	Parallel Redundancy Protocol
RTU	Remote Terminal Unit
SAS	Substation Automation System
SCADA	Supervisory Control and Data Acquisition
SCL	Substation Configuration Language
SGAM	Smart Grid Architecture Model
SLA	Service Level Agreement
SSH	Secure Shell
SV	Sampled Values
TCP	Transmission Control Protocol
TLS	Transport Layer Security
TSO	Transmission System Operator
UDP	User Datagram Protocol
UM	Universal monitor
VN	Vysoké napětí
VPN	Virtual Private Network
VT	Voltage Transformer
Wi-Fi	Wireless Fidelity
XML	eXtensible Markup Language

Seznam příloh

A Příloha A MITRE ATT&C tabulky

Tab. A.1: MITRE ATT&CK pro GOOSE

	Technika	**ID**	**Popis**
S	Spoof Reporting Message	T0854	Útočník se vydává za legitimní GOOSE zařízení a vysílá falešné rámce s cílem změnit stav vstupů u IED.
T	Manipulation of Control	T0858	Útočník manipuluje s GOOSE rámcem za účelem spuštění/potlačení ochranné funkce nebo ovládání.
R	Nepokryto v MITRE ATT&CK	—	Framework ATT&CK neobsahuje explicitní techniku pro chybějící logování GOOSE zpráv.
I	Sniffing Network Traffic	T0842	Pasivní sledování GOOSE rámců může vést k odhalení struktury systému, stavových proměnných nebo ID zařízení.
D	Denial of Control	T0804	Útočník zahlcuje přijímače falešnými GOOSE zprávami nebo záměrně způsobí chybu v dekódování.
E	Nepokryto specificky pro GOOSE	—	Elevace oprávnění je relevantnější pro zařízení než pro samotný protokol.

Tab. A.2: MITRE ATT&CK pro Sampled Values

	Technika	**ID**	**Popis**
S	Spoof Reporting Message	T0854	Útočník se vydává za Merging Unit a vysílá falešné SV rámce obsahující zmanipulovaná měření (např. proudy, napětí).
T	Manipulation of I/O	T0855	Do rámců SV jsou vkládány úmyslně nesprávné hodnoty, aby bylo dosaženo změny chování ochran.
R	Nepokryto v MITRE ATT&CK	—	Není zahrnuta technika pro chybějící zpětné dohledání (např. logy SV zpráv).
I	Sniffing Network Traffic	T0842	Odposlech SV rámců umožňuje získání informací o síťové zátěži, frekvenci, zatížení fáze apod.
D	Denial of Control	T0804	Spoofovaný nebo zahlcený tok SV dat může způsobit ztrátu vstupů pro ochrany (IED), což vede k výpadku ochranné funkce.
E	Nepokryto specificky pro SV	—	SV protokol neimplementuje oprávnění; relevantní až pro MU zařízení.

Tab. A.3: MITRE ATT&CK pro MMS

	Technika	**ID**	**Popis**
S	Masquerading	T0853	Útočník se vydává za legitimní IED nebo klienta a odesílá MMS zprávy, které přijímající zařízení považuje za důvěryhodné.
T	Unauthorized Command Message	T0851	Útočník modifikuje obsah MMS zprávy za účelem spuštění nebo blokace ovládací funkce (např. ON/OFF výstup).
R	Nepokryto	—	MITRE ATT&CK neobsahuje specifickou techniku pro nedostatečné logování MMS transakcí.
I	Sniffing Network Traffic	T0842	Pasivní odposlech MMS zpráv umožňuje útočníkovi číst parametry, názvy proměnných, topologii zařízení.
D	Denial of Control	T0804	Zahlcení MMS serveru (např. IED) může vést k výpadku odpovědí a ztrátě funkce SCADA řízení.
E	Valid Accounts	T0886	Pokud má útočník přístup k platným účtům (např. heslům uloženým v konfiguračním souboru), může ovládat MMS komunikaci se zvýšenými právy.

Tab. A.4: MITRE ATT&CK pro IEC 104

	Technika	**ID**	**Popis**
S	Masquerading	T0853	Útočník se vydává za legitimní klienta nebo server a naváže spojení s gateway/RTU bez autentizace.
T	Unauthorized Command Message	T0851	Útočník upraví obsah IEC 104 ASDU za účelem změny stavů, spínání výstupů nebo podvržení alarmů.
R	Nepokryto	—	Chybí pokrytí auditního deficitu – běžný problém, ale není součástí ATT&CK.
I	Sniffing Network Traffic	T0842	Odposlech IEC 104 (plain text) umožňuje čtení ASDU (např. měření, alarmy, stavy).
D	Denial of Control	T0804	Flood nebo segmentace TCP spojení vede k zablokování komunikačního kanálu mezi SCADA a RTU.
E	Valid Accounts	T0886	Pokud je RTU přístupná např. přes VPN a nechráněna heslem, může být ovládána útočníkem s vyššími právy.

Tab. A.5: MITRE ATT&CK pro SCADA

	Technika	**ID**	**Popis**
S	Masquerading	T0853	Útočník se vydává za důvěryhodný zdroj dat nebo příkazů pro SCADA (např. RTU nebo IED).
T	Unauthorized Command Message	T0851	SCADA je podvedena k vykonání příkazu, který nepochází z oprávněného zdroje nebo byl pozměněn v přenosu.
R	Nepokryto	—	Framework neobsahuje techniku pro nedostatečné logování příkazů nebo dat ve SCADA systému.
I	Sniffing Network Traffic	T0842	Odposlech komunikace (např. přes IEC 104) může odhalit topologii, stavy a parametry systému.
D	Denial of Control	T0804	SCADA server může být zahlcen dotazy, falešnými zprávami nebo zahlcením protokolového kanálu.
E	Valid Accounts	T0886	Získání přihlašovacích údajů správce umožňuje útočníkovi úplný přístup ke SCADA funkcím.

Tab. A.6: MITRE ATT&CK pro IEC 104 gateway

	Technika	**ID**	**Popis**
S	Masquerading	T0853	Útočník se vydává za legitimního SCADA klienta naváže spojení s gateway.
T	Unauthorized Command Message	T0851	Úprava příkazů v rámci komunikace s cílem změnit logiku nebo stavové hodnoty.
R	Nepokryto	—	Neexistuje ATT&CK technika pro případ, kdy gateway neuchovává záznamy o přijatých a přeposlaných zprávách.
I	Sniffing Network Traffic	T0842	Gateway přenáší data mezi OT/IT – odposlech umožňuje získat kompletní přehled o stavu systému.
D	Denial of Control	T0804	Flooding nebo nekompatibilní segmentace zpráv může způsobit přerušení toku mezi SCADA a zařízeními.
E	Valid Accounts	T0886	Gateway může obsahovat správní rozhraní bez dostatečné autentizace – umožňuje eskalaci oprávnění.

Tab. A.7: MITRE ATT&CK pro RTU

	Technika	**ID**	**Popis**
S	Masquerading	T0853	Útočník předstírá, že je operátor a posílá zprávy zařízení, které mu důvěřuje.
T	Unauthorized Command Message	T0851	Úprava/podvržení příkazů přijatých RTU – např. ovlivnění přepnutí stavu výstupu.
R	Nepokryto	—	Neexistuje technika pro případ, kdy gateway neuchovává záznamy o přijatých a přeposlaných zprávách.
I	Sniffing Network Traffic	T0842	Pasivní odposlech IEC 104 komunikace s RTU umožňuje číst měření a stavové informace.
D	Denial of Control	T0804	RTU může být zahlcena dotazy nebo napadena opakovaným připojováním z podvržených klientů.
E	Valid Accounts	T0886	Při přímém připojení k RTU nebo přes otevřené služby (např. SSH, RDP) lze zneužít výchozí účty.

Tab. A.8: MITRE ATT&CK pro IED

	Technika	**ID**	**Popis**
S	Masquerading	T0853	Útočník předstírá, že je jiný síťový uzel nebo validní klient (např. EWS), a odesílá zprávy do IED.
T	Unauthorized Command Message	T0851	Odeslání podvrženého ovládacího signálu pomocí MMS nebo změna konfigurace přes službu.
R	Nepokryto	—	IED většinou neuchovává logy o změnách logiky nebo konfigurace – ATT&CK nemá přímý ekvivalent.
I	Sniffing Network Traffic	T0842	IED komunikuje přes MMS, GOOSE a SV – odposlech těchto zpráv umožňuje odhalení vnitřní logiky a dat.
D	Denial of Control	T0804	Zahlcení IED (např. útoky na SV nebo GOOSE) může způsobit selhání ochranných funkcí.
E	Valid Accounts	T0886	Získání přístupu ke konfiguraci přes výchozí účet, USB, nebo síťovou službu umožňuje změnit chování IED.

Tab. A.9: MITRE ATT&CK pro MU

	Technika	**ID**	**Popis**
S	Spoof Reporting Message	T0854	Útočník napodobuje MU a vysílá falešné SV rámce, které se tváří jako autentická měření.
T	Manipulation of I/O	T0855	Do digitálních měření jsou záměrně vloženy nesprávné hodnoty nebo změněny koeficienty převodu.
R	Nepokryto	—	MU obvykle neuchovává žádné logy ani konfigurační historii – ATT&CK framework to nezachycuje.
I	Sniffing Network Traffic	T0842	Odposlech SV zpráv od MU odhaluje skutečná měřená data (napětí, proud, fázové posuny).
D	Denial of Control	T0804	Útoky na MU mohou přerušit přenos SV zpráv a způsobit výpadek vstupních dat do IED.
E	Valid Accounts	T0886	Pokud MU umožňuje konfiguraci bez RBAC, může útočník změnit parametry měření nebo spustit firmware update.

Tab. A.10: MITRE ATT&CK pro Inženýrská stanice

	Technika	**ID**	**Komentář**
S	Masquerading	T0853	Útočník se vydává za inženýrskou stanici nebo autentizovaného uživatele a navazuje spojení s IED.
T	Modify Controller Tasking	T0850	Změna parametrizace zařízení nebo logiky ochrany (např. v SCL souborech) bez oprávnění.
R	Nepokryto	—	Inženýrské stanice často postrádají auditní stopu o změnách – ATT&CK to přímo neřeší.
I	Data from Information Repositories	T0802	Získání dat z konfiguračních souborů, databází zařízení nebo parametrizačních nástrojů.
D	Execution through API/Tool Abuse	T0859	Útok na nástroj, kterým se mění konfigurace (např. XML editor) může vést k chybné konfiguraci a selhání systému.
E	Valid Accounts	T0886	Získání přihlašovacích údajů k inženýrské stanici umožní úpravu všech zařízení v síti.

B Příloha - Popis Analyzovaných testovacích prostředí

Článek [64] popisuje architekturu testovacího prostředí VSCADA zaměřenou na modelování a simulaci ve výzkumu energetických systémů. Prostředí je čistě softwarově definované a architektura umožňuje simulovat různé scénáře řízení/monitorování, které využívají protokol OPC UA. Komunikace probíhá mezi SCADA serverem a HMI jednotkou. Pro simulaci energetických scénářů je použito prostředí Python, který z databáze načítá data z modelů. Testování probíhalo na modelu IEEE 39-bus. Testovací prostředí lze klasifikovat jako virtualizační nástroj energetické infrastruktury, která je jednoduše škálovatelná, ale simulace jednotlivých vrstev je omezena na scénáře, obsažené v modelech jako je např. IEEE 39-bus.

V článku [203] autoři realizovali komplexní kyberneticko-fyzikální testovací prostředí pro zkoumání potenciálních zranitelností kybernetické bezpečnosti a dopadu kybernetických útoků na inteligentní rozvodny založené na standardu IEC 61850. Jedná se o fyzický testbed, který emuluje elektrickou stanici s komunikačními protokoly GOOSE, SV a MMS. Pro komunikaci s dohledovým centrem SCADA je použit protokol IEC 60870-5-104. Výhodou oproti jiným testovacím prostředím je možnost fuzzy testování fyzických zařízení Testovací prostředí lze klasifikovat jako emulátor od nejnižší procesní vrstvy až po komunikaci ke SCADA. Fyzická realizace však do značné míry omezuje škálovatelnost a tím i možnost simulace komplexnějších scénářů na úrovni distribuční nebo přenosové soustavy.

Další prostředí, které je popsané v článku [189] je založené na open-source knihovně OpenPLC61850. Knihovna podporuje softwarovou simulaci a hardwarovou implementaci na zařízeních, jako jsou Raspberry Pi, Arduino a ESP8266. Součástí knihovny je i OpenPLC editor, který podporuje standard IEC 61131-3 pro programovatelné logické automaty a slouží k vykonávání řídicí logiky. Z pohledu komunikace jsou zastoupeny protokoly ModBus, DNP3 a díky autorům článku i protokol MMS ze standardu IEC 61850. V článku není uveden rozbor testovacího prostředí, ale dle popisu se jedná o virtualizační nástroj s možností simulace komunikace výše zmíněných protokolů. Knihovna umožňuje simulovat komunikaci jednotlivých prvků jako jsou IED, HMI nebo i SCADA. Není však uvedeno na jaké úrovni je možné modelovat jednotlivá zařízení např. z pohledu simulace snímaných veličin napětí, proudu nebo stavových jako je jistič, odpojovač nebo uzemňovač. Testovací prostředí lze klasifikovat virtualizační nástroj, který umožňuje simulovat datovou komunikaci výše uvedených protokolů bez možnosti podrobné emulace zařízeních vyskytujících se v energetické infrastruktuře.

V článcích [188] [187] autoři navrhli kyberfyzikální systém pro simulaci rozsáhlých modelů sítě v prostředí digitálního simulátoru pro monitorování a řízení DER, včetně standardních komunikačních protokolů jako je IEEE 2030.5 [44], IEC 61850, DNP3 nebo Modbus TCP. Prostředí je složeno z fyzických reálných prvků a emulovaných zařízení, kde celek je reprezentován jako HIL. Jako vstupní data pro testovací scénáře jsou používány např. IEEE 39 a IEEE 13 sběrnice. Autoři v článcích uvádějí, že navržený systém je možné škálovat dle možností hardwaru, což dokazují na několika případových studií zaměřených na protokoly GOOSE, MMS nebo DNP3. Dle realizace se jedná o rozsáhlé a komplexní testovací prostředí s možností emulace reálných zařízení, které je zaměřeno primárně na kyberbezpečnost.

Článek [204] obsahuje popis testovacího prostředí, které je zaměřeno na testování ochranných relé pro elektrické stanice. Prostředí se skládá ze čtyř hlavních součástí: simulátoru RTDS, zařízení pro zpracování dat, zařízení reléové ochrany a pracovní stanice pro simulaci systému. Pro testování ochran je možné v prostředí simulovat různé stavy jako je např. porucha při zkratu nebo kmitání frekvence napájecích systému. Samotné prostředí je zaměřeno na testování výše zmíněných ochran. Komunikace dle standardu IEC 61850 je v článku řešena minimálně a jde spíše o podpůrnou službu,

aby bylo možné nastavit testované ochrany.

V článku[67] autoři popisují softwarové testovací prostředí pro studium elektrických rozvoden založených na IEC 61850. Prostředí je založeno na open-source softwarových nástrojích jako je knihovna libiec61850 pro simulaci protokolů ze standardu IEC 61850, GNS3 síťový simulátor, SCAPY pro manipulaci se síťovou komunikací, wireshark pro analýzu síťové komunikace a matlab/-simulink pro simulaci elektrického energetického systému. Simulace probíhá ve virtuálních strojích s operačním systémem Ubuntu a uvedeného popisu jsou simulována všechna základní zařízení elektrické stanice jako je MU,CB, IED a RTU. Sami autoři uvádějí, že testovací prostředí slouží k simulaci a testování síťových útoků na protokoly ze standardu IEC 61850 a některé části prostředí nemusí odpovídat reálnému systému. Testovací prostředí lze klasifikovat simulátor elektrická stanice od procesní vrstvy až po úroveň rozvodny. Není zde však zastoupen žádný dohledový systém.

V Článku [180] je popsáno testovací prostředí, které se zaměřuje na emulaci elektrické stanice z distribuční soustavy. Prostředí je rozděleno do čtyř úrovní, kde nultá až druhá úroveň odpovídají úrovni procesu, pole a rozvodny dle standardu IEC 61850. Poslední třetí úroveň odpovídá správě a řízení, kde se nachází SCADA. Dle popisu prostředí umožňuje simulaci řady protokolu jako jsou např. MMS, GOOSE, SV, IEC 60870-5-101/104, DNP3 nebo ModbusTCP. V článku je jen velmi stručně uveden podrobný popis, jak a čím jsou jednotlivé úrovně realizovány a autoři se primárně zabývají posuzování zranitelností a penetrační testování.

Článek [91] popisuje integraci nových balíku pro dynamickou simulaci energetických systémů do již realizovaného kyberneticko-fyzikálního testovacího prostředí energetického systému, které podporuje přenos dat v reálném čase pomocí protokolu DNP3. Jádrem prostředí je simulační nástroj PWDS (PowerWorld Dynamic Studio), který je softwarový balík pro modelování, simulaci a analýzu dynamického chování energetických systémů. Jedná se o komplexní nástroj, který umožňuje modelovat a analyzovat širokou škálu jevů v elektrizační soustavě. Lze jej také použít jako zdroj dat pro protokoly C37.118 a DNP3. Mimo PWDS je součástí prostředí i SEL RTAC (Schweitzer Engineering Laboratories Real-Time Automation Controller), což je výkonná a flexibilní hardwarová platforma určená pro automatizaci a řízení energetických systémů v reálném čase. Vyvinula a prodává ji společnost Schweitzer Engineering Laboratories. RTAC se běžně používá pro řadu aplikací v energetických systémech, včetně aplikací pro dohledové řízení a sběr dat (SCADA), automatizaci rozvoden, ochranu a řízení a synchronní fázory. Testovací prostředí lze klasifikovat simulátor rozsáhlé energetické sítě, kde jednotlivé elektrické stanice mohou s dohledovým centrem komunikovat pomocí protokolu DNP3.

V článku [200] je navrženo a realizováno testovací prostředí založené na metodice HIL pro vyhodnocování a posuzování provozu a řízení mikrosítě. Prostředí se skládá z RTDS pro modelování mikrosítě, řídicích jednotek CompactRIO pro řízení IED, prototypu systému EMS a SCADA. Energetická část prostředí je simulována v RTDS. Pro komuniakci mezi zařízeními se používá protokol Modbus TCP. EMS je implementována v prostředí MATLAB a má tři části, hlavní uživatelské rozhraní (UI), optimalizaci a vizualizaci. SCADA je implementována v nástroji LabView. Testovací prostředí bylo primárně navrženo pro testování uzavřených smyček, jako je řízení distribuovaných zdrojů energie (DER) a mikrosítí. Datová komunikace je řešena v minimálním zastoupení pomocí protokolu Modbus TCP a infrastrukturu by se dala označit na úrovni zjednodušené elektrické stanice se zaměřením na energetickou část.

Autoři v článku [201] realizují virtuální digitální testovací zařízení elektrické stanice, která slouží pro analýzu dopadu různých vadných komponent v datové komunikační síti a poruchových stavů v elektrické síti na funkčnost a výkonnost. Za hlavní přínos autoři označují formulace metodiky analýzy dat založené na Q-Q metodě [1] pro ověření dat z experimentu a provedení statistické

[1] Q-Q je technika pro identifikaci a lokalizaci poruch v elektrických přenosových vedeních.

analýzy pro kvantifikaci vlivu různých topologií redundance sítě na výkonnost ochran a řídicích zařízení. Testovací prostředí plně virtualizované pomocí RTDS, kde jsou použity čtyři testovací modely Swansea North 1, Whitson/Seabank, Swansea North 3 a Rassau. Testovací prostředí se nezabývá problematikou datové komunikace, ale zaměřuje se na specificky na energetickou část.

Autoři v článku [87] představují testovací prostředí pro kontrolu protokolu GOOSE ze standardu IEC 61850. Jádrem testovacího prostředí je Typhoon HIL[2], který je složen z řadu softwarových nástrojů a knihoven pro návrh a simulaci výkonové elektroniky a výkonových systémů. Autoři se zaměřují na emulaci IED jednotky, která obsahuje ochranné relé, měřící jednotku, jistič a komunikuje pomocí protokolu GOOSE. Testovací prostředí lze klasifikovat simulátor části elektrické stanice, kde škálovatelnost je závislá na počtu HIL jednotek.

V článku [93] je představeno výzkumného testovacího prostředí pro řízení energie (EMP), monitorování a řízení energetických systémů. Jádrem prostředí je simulátor, který napodobuje provoz energetického systému. Díky emulaci provozních zařízení se simulátor používá k dalšímu přenosu dat o síti prostřednictvím systému SCADA do softwaru EMS. Prostředí je zaměřeno na simulaci dat pomocí protokolu DNP3 mezi SCADA a RTU jednotkami, které jsou simulovány pomocí nástroje PowerWorld Dynamic Studio, který by popsán již u článku [91]. Data pro SCADA jsou přenášena do DTS (Dispatcher Training Simulator) [3]. Primární zaměření testovacího prostředí tedy není na datovou komunikaci, ale jak školících nástroj pro dispečerské řízení.

V článku [52] by navrženo a realizováno testovací prostředí emulace komunikace pro lokální síť na testovacím pracovišti FIU (Florida International University) Smart Grid Testbed. Prostředí je složeno z fyzických ochran ABB, GNS3 pro simulaci síťových prvků a Rasbperry Pi pro simulaci zátěže pomocí protokolu iperf3. Primární zaměření testovacího prostředí je na kybernetickou bezpečnost fyzických zařízení v elektrické stanici, která komunikuje pomocí standardu IEC 61850, specifiky pomocí protokolu GOOSE, který je přenášen mezi ochrannými jednotkami a jednotkou pro zprávu rozvodny. Testovací prostředí lze klasifikovat jako emulátor elektrické stanice. Škálovatelnost je však velmi omezena, vzhledem k použití reálných fyzických zařízení.

Autoři v článku [192] navrhují testovací prostředí, které simuluje energetický systém SCADA. Prostředí se skládá z generátoru provozu, simulovaných zařízení, jako jsou RTU, MTU a HMI a komunikačního kanálu realizovaného pomocí protokol IEC-60870-5-101 a nebo DNP3. Úroveň procesu a pole je realizována pomocí PSAT (Power System Analysis Toolbox) [4], který předává data do RTU. Výše zmíněné komunikační protokoly potom zajišťují přenos dat do MTU, kde je dostupná i HMI jednotka pro zobrazení a ovládání. Poslední hlavní částí testovacího prostředí je modul komparátoru, který pro zpracování dat přijatých dat na MTU. Testovací prostředí lze klasifikovat jako simulátor rozsáhlejší elektrické stanice, kde se vyskytuje více RTU řízení pomocí MTU a lokální SCADA systémem.

Článek [208] je zaměřen na IDS pro protokol ze standardu IEC 61850. Specificky jde o identifikaci zfalšovaných měřených hodnot ve zprávách MMS protokolu. Realizované testovací prostředí v tomto článku se skládá z fyzických a simulovaných částí, kde jádrem je RTDS, ke kterému jsou připojeny ochranná zařízení rozvodny, komunikační bránu rozvodny, výkonové zesilovače a časovou synchronizaci fyzické ochrany a řídicí hardware se simulovaným prostředím. Pro simulaci energetického infrastruktury je použit IEEE 39-Bus model, který zahrnuje 39 sběrnic, 10 generátorů a 46 přenosových vedení. vedení. Představuje zjednodušenou verzi reálné elektrizační soustavy, ale je dostatečně složitá, aby byla užitečná pro analýzu a simulační studie elektrizační soustavy. Testovací prostředí lze klasifikovat emulátor elektrické sítě s možností škálovatelnost díky simulační části.

[2]Poskytovatelem systémů HIL pro výkonovou elektroniku, https://www.typhoon-hil.com.
[3]DTS je software určený k realistickému a interaktivnímu školení dispečerů energetických soustav.
[4]PSAT je open source softwarový balík pro analýzu a návrh malých a středních elektrických systémů.

Autoři v článku [207] navrhují novou strategii zotavení zařízení SAS založeného na IEC 61850 po kybernetickém útoku. Napadené části jsou izolovány v místní síti rozvodny pomocí dynamické rekonfigurace sítě, která je realizována pomocí centralizovaného řídicího systému softwarově definované sítě (SDN). Pro simulaci scénářů za účelem testování navrženého řešení bylo vytvořené testovací prostředí reprezentující elektrickou stanici založenou na standardu IEC 61850. Síťová infrastruktura je virtualizována v nástroji Mininet, který slouží pro implementaci SDN. Pro centralizované řízení SDN je použit řadič POX s rozšířením RECOVERY [86]. Tyto nástroje dohromady tvoří SDN kontrolér, který je připojen do fyzické části testovacího prostředí, kde jsou IED, MU nebo HMI jednotky. V případě útoku SDN kontrolér zablokuje provoz z infikované jednotky. Z pohledu testovacích prostředí jde o reprezentaci elektrické stanice s fyzickými prvky pro testování bezpečnostních incidentů.

V článku [185] je představeno testovací prostředí pro kybernetickou bezpečnost inteligentních sítí ISSAC (The Idaho CPS SCADA Cybersecurity testbed at the University of Idaho). Dle autorů je prostředí mezioborové, distribuované a rekonfigurovatelné, napodobuje realistickou energetickou infrastrukturu a poskytuje nástroje potřebné k vývoji a testování integrovaných řešení kybernetické bezpečnosti. Simulaci elektrické sítě zajišťuje RTDS, na které jsou pomocí analogových a digitálních rozhraní připojeny IED. RTAC zpracovává měření SCADA propojením s IED pomocí protokolů DNP3, IEC 61850 GOOSE a analogových vstupů. Komunikace RTAC a SCADA probíhá prostřednictvím protokolu DNP3 a RTDS komunikují se SCADA pomocí protokolů IEC 61850 a DNP3. Mimo tyto protokoly jeden modul RTAC obsluhuje synchronní data IEEE C37.118. Testovací prostředí lze klasifikovat jako emulátor rozsáhlé energetické sítě s reálnými a emulovanými prvky, který umožňuje škálovat jednotlivá zařízení dle dostupného hardwaru. Simulace jednotlivých úrovní je zajištěna od procesní úrovně až po dohledové centrum.

Autoři v článku [92] představují testovací prostředí RESLab, které navazuje na metodiku popsanou v článku [91]. Prostředí se skládá ze čtyř částí RTAC, PWDS, CORE emulátor a Layer 3 přepínač a slouží primárně na kybernetickou bezpečnost. Prostředí je plně virtualizované a pro komunikaci je použit protokol DNP3. Testovací prostředí lze klasifikovat jako simulátor na úrovni cele infrastruktury, kde je možné pomocí nástroje PWDS simulovat celé energetické sítě a pomocí RTAC prvky z jedné elektrické stanice. Škálovatelnost je omezena pouze danými softwarovými nástroji.

Autoři v článku [66] představují testovací prostředí pro provoz, řízení a ochranu mikrosítě založené na IEC 61850 s RT-LAB. Prostředí je složeno ze softwaru RT-LAB [5], simulátor IED a rozhraních simulující komunikaci protokolů MMS, GOOSE a SV mezi klientem a serverem respektive vydavatele a odběratelem. Dle popisu prostředí obsahuje mimo simulátor i reálné ochranné zařízení na úrovni pole. Na úrovni procesu je pro simulaci použit výše zmínění nástroj RT-LAB a fyzická zařízení jako je emulátor větrné energie a systém ukládání energie do baterií. Testovací prostředí lze klasifikovat jako emulátor na úrovni elektrické stanice s možností škálovatelnosti pomocí simulačních nástrojů.

V článku [90] se autoři zaměřují na koncept pro detekci a zmírnění kybernetických útoků na automatizační systémy rozvoden, které jsou vybaveny protokoly ze standardu IEC 61850. Dle popisu jsou pro komunikaci použity tři základní protokoly MMS, GOOSE a SV. Pro testování kybernetických útoků bylo realizováno testovací prostředí, které bylo integrováno do modelu energetické soustavy BPA (Bonneville Power Administration) [6]. V testovacím prostředí jsou zahrnuty fyzické a simulované prvky jako je (RTDS), ochranná zařízení rozvodny, komunikační brána rozvodny,

[5] RT-LAB je platforma pro simulaci a testování v reálném čase vyvinutá společností OPAL-RT Technologies

[6] Federální agentura, která je zodpovědná za správu a přenos elektrické energie v severozápadní oblasti Tichého oceánu Spojených států.

výkonové zesilovače a časovou synchronizaci fyzické ochrany a řídicí hardware se simulovaným prostředím. Testovací prostředí lze klasifikovat energetickou infrastrukturu reprezentující jednu elektrické stanice.

Autoři v článku [164] popisují testovací prostředí kybernetické energetiky pro ověřování distribuovaných aplikací v energetické síti. Primární zaměření prostředí je pro testování DMC (Distributed Monitoring and Control), specificky na DRAS (Distributed Remedial Action Scheme) , který navržen tak, aby zvyšoval spolehlivost a bezpečnost energetických systémů tím, že rychle odhalí a izoluje poruchy nebo poruchy dříve, než mohou způsobit rozsáhlé výpadky. Pro simulaci energetické soustavy se používá RTDS. Analogové hodnoty napětí a proudu jsou předávány PMU jednotkám, které data převádějí a posílají pomocí protokolu IEEE C37.118. Platforma CISCO Fog zajišťuje simulaci infrastruktury mezi jednotlivými PMU. Testovací prostředí lze klasifikovat jako nástroj pro simulaci a testování energetické infrastruktury, za účelem ověření systému DMC. Mimo protokol IEEE C37.118, který je spíše podpůrný protokolem, aby byla zajištěna funkčnost celého procesu, není v testovacím prostředí řešena datová komunikace.

Článek [166] popisuje testovací prostředí Smart-Grid zaměřené na výuku standardu IEC 61850 pro studenty a odborníky. Prostředí zahrnuje emulaci zátěží a generátorů středního napětí s nadřazeným systémem řízení a sběru dat, které jsou realizovány pomocí reálných fyzických zařízeních. Celkově se jedná o replikaci jednoho pole v rámci elektrické stanice. V rámci článku je primárně řešen protokol GOOSE, který se v edukativních podmínkách testuje na experimentech reprezentující reálné situace. Pomocí tohoto testovacího prostředí jsou navrženy výukové materiály zaměřené na nastavení a konfiguraci ochranných relé s využitím sémantiky jazyka xml. Testovací prostředí lze klasifikovat jako reprezentaci malé elektrické stanice, která je primárně určena pro výukové případy, ale vzhledem k její konfiguraci by mohla být použita i pro jiné účely.

Autoři v článku [159] se zaměřují na výzkum kybernetických rizik a jejich zmírňování v systémech automatizace energetických zařízení podle normy IEC 61850. Výzkum probíhá na testovacím prostředí, které je součástí experimentální platformy G-ICS (GreEn-ER1 Industrial Control Systems Sandbox) zaměřené na interoperabilitu a kybernetickou bezpečnost ICS. Prostředí se skládá ze simulátoru energetické sítě, IED, HMI a doplněné o konfigurační pracovní stanice. V rámci článku autoři představují kybernetické Injection útoky na protokol GOOSE. Testovací prostředí lze klasifikovat jako emulátor na úrovni elektrické stanice.

Článek [184] popisuje návrh kyberneticko-fyzického testovacího prostředí, které se skládá ze tří hlavních komponent: EMS, komunikace a fyzického simulátoru energetické soustavy. V rámci simulace elektrické stanice je simulátor energetické soustavy realizován pomocí OPAL-RT, který komunikuje pomocí protokolů GOOSE a SV s IED. Nad těmito prvky je RTU jednotka, který pomocí MMS protokolu komunikuje s IED a OPAL-RT. Komunikace mezi Elektrickou stanici a EMS je zprostředkováno pomocí protokolů DNP3 nebo MMS přes komunikační infrastruktury, která je realizována pomocí síťového simulátoru. Dále autoři uvádějí útoky typu DoS nebo Injection na vytvořenou infrastrukturu. Testovací prostředí je z části ve formě návrhu a z článku není jasné, jak jsou nebo budou některé prvky realizovány.

Testovací prostředí popsané v článku [48] slouží pro ověření praktických modelů útoků na systém diagnostiky energetických transformátorů (PTDS) v digitální rozvodně pomocí pokročilých trvalých hrozeb (APT) a navrhuje bezpečnostní testovací prostředí pro vývoj budoucího zabezpečení zabudovaného do PTDS proti APT. Návrh testovacího prostředí je rozdělen na dvě části – simulace fyzického systému elektrické stanice a simulace kybernetického sytému. Simulace fyzického systému je řešena pomocí OPAL-RT. Kybernetický systém je emulován pomocí reálných síťových zařízeních a serveru. IED, SDU (substation diagnostic unit) a PTDU (Power transformer diagnosis unit) jsou emulovány pomocí jednodeskových počítačů Raspberry Pi a komunikují spolu

pomocí průmyslového síťového protokolu Modbus TCP nebo standardu IEC 61850. Dále autoři uvádějí síťové útoky jako Brute Force, MITM nebo DoS na realizované prostředí. Testovací prostředí popsané v tomto článku je z části ve formě návrhu a autoři uvádějí jen počáteční výsledky. Dle navrženého řešení lze prostředí klasifikovat jako emulátor elektrické stanice.

Emulátor komunikační sítě popsaný v článku [88] je součástí testovacího prostředí inteligentních sítí. Součástí prostředí jsou reálné IED od společnosti SEL (Schweitzer Engineering Laboratories), datových koncentrátorů (PDC - Phasor Data Concentrator) a uživatelského rozhraní pro sběr a řízení dat. Simulaci sítě zajišťuje software Riverbed Modeler s využitím softwaru SITL ((System-in-the-Loop) pro propojení IED a fyzického hardwaru se simulací sítě. Energetický protokol pro komunikaci z PMU jednotek byl použit IEEE 37.118. Prostředí není primárně zaměřeno na simulaci energetických komunikačních protokolů, ale zaměřuje se na problematiku plošného monitorování a řízení inteligentních sítí a význam komunikační sítě pro poskytování spolehlivých dat v reálném čase řídicímu systému. Testovací prostředí lze klasifikovat jako simulátor energetických sítí s možností sběru dat z reálných zařízeních komunikujících protokole IEEE C37.118.

Kyberneticko-fyzikální testovací prostředí představené v článku [199] je dle autorů komplexní systém, který umožňuje integraci hardwarové jednotky pro měření fázorů a koncentrátoru fázorových dat do testovacího zařízení a podrobné modelování komunikační sítě pro energetickou soustavu. Prostředí je výsledkem integrace RTDS, který simuluje energetickou soustavu v reálném čase a NS-3, který simuluje komunikační síť. IED jednotky jsou realizovány pomocí reálných zařízení od společnosti SEL, která byla popsána u předešlého článku [199]. Pro komunikaci mezi energetickými zařízeními je použit standard IEC 61850, DNP3 a IEEE 37.118. Testovací prostředí lze klasifikovat jako simulační nástroj s reálnými prvky pro sběr dat na úrovni energetické sítě.

Testovací prostředí popsané v článku [47] je navrženo a realizováno pro testování schémat řízení energie, kybernetických útoků na energetickou síť a strategií jejich zmírnění. Jedná se o modulární prostředí, kde je představeno několik komunikačních architektur s různými kombinacemi hardwaru a softwaru. Společným prvkem je všechny modely je PI-server od společnosti OSIsoft, který slouží k pro správu a analýzu dat v reálném čase. Je zde přestaven model, kde na úrovni energetické sítě je pomocí Matlab/Simulink simulován požadovaný model, který je předán simulátoru OPAL-RT a následně jsou data přenášena do PI-serveru. Druhá model zahrnuje PMU od společnosti SEL jednotky komunikující protokolem IEEE C37-118. Třetí model je založen na simulačním nástroji LabView, což je grafický programovací nástroj pro testování, měření a automatizaci, který se široce používá jako virtuální přístrojový nástroj. Poslední model představuje měření dat reálných solárních panelů, které přenášejí energii do bateriových systémů, které komunikují protokoly DNP3 nebo ModBus TCP. Testovací prostředí lze klasifikovat jako modulární simulátor, který představuje různé modely simulace dat na energetické úrovni.

Systém WAMS představený v článku [46] je kyberneticko-fyzikální testovací prostředí, které pomocí RTDS a HIL umožňuje modelování událostí a kybernetických útoků na energetickou soustavu. Hlavní přínosem článku je automatický simulační a řídicí engine pro náhodné modelování kybernetických událostí, včetně poruch energetického systému, nepředvídaných událostí, řídicích akcí a kybernetických útoků. Prostředí je schopno simulovat různě velké energetické systémy a vytvářet datové sady bez nutnosti měnit konfiguraci hardwaru. Fyzická procesní vrstva je realizována pomocí zmíněného RTDS, které předává analogová a stavová data PMU a HW/SW relé. Komunikace mezi IED a dalšími zařízení probíhá pomocí protokolů MODBUS, DNP3, IEC 61850 a IEEE C37.118. Testovací prostředí lze klasifikovat jako modulární emulátor na úrovni rozsáhlejší elektrické stanice s lokální centrálním řízením.

EPIC (Electrical Power and Intelligent Control) v článku [45] je rozsáhlé fyzické testovací prostředí výkonem 72 kVA, které napodobuje reálný energetický systém v malé inteligentní síti. Skládá

se ze čtyř částí výroba (Generation), přenos (Transmission), mikrosíť (Micro-grid) a inteligentní domácnost (Smart Home), kde každá část je řízena PLC s jedním nadřazeným PLC připojeném ke SCADA. Fyzická část je složena ze dvou generátorů, fotovoltaických panelů a baterií. Komunikace probíhá pomocí protokolů GOOSE a MMS ze standardu IEC 61850 mezi IED a SCADA. Prostředí slouží pro výzkumné účely v oblasti simulace dat a zranitelností, kde je možné si testovací prostředí i pronajmout pro vlastní účel. EPIC lze klasifikovat jako emulační nástroj pro simulaci a testování v oblasti energetické energetických systémů, kde jsou zastoupeny prvky od výroby elektrické energie až po její spotřebu.

Kybernetické bezpečnostní testovací prostředí SCADA popsané v článku [156] je zaměřeno na oblast energetické kritické infrastruktury. Článek se zaměřuje na rozbor hrozeb v KI a jejich mitigace. Testovací prostředí je složeno z reálné IED a RTU od společnost i Elkomtech, kde vstupní analogové a stavové hodnoty jsou generovány pomocí nástroje LabView. Komunikace je v rámci rozvodny realizována standardem IEC 61850 a pro spojení se SCADA je použit protokol IEC 60870-5-104. Monitorování komunikace zajišťují IPS/IDS systémy Snort a Bro. Prostředí lze klasifikovat jako emulátor elektrické stanice s komunikací do SCADA s možností simulací kybernetických hrozeb.

Článek [172] popisuje virtualizační testovací prostředí, která simuluje komunikaci datových energetických protokolů. Prostředí je založeno na virtualizačním nástroji Oracle VirtualBox a implementuje dva typy profilů: (i) provozní, který definuje nasazení uzlů, simulátorů a konfiguraci sítě a (ii) konfigurační pro konfiguraci uzlů reprezentujících konkrétní průmyslová zařízení (např. HMI, RTU). Procesní vrstva se simulací analogových a stavových veličin není v rámci článku zahrnut, ale autoři uvádějí, že jej lze jej snadno integrovat pomocí softwaru třetích stran. Prostředí podporuje energetické protokol IEC 60870-5-104 a OPC-UA pro prvky HMI a RTU. Testovací prostředí lze klasifikovat jako virtualizační simulátor komunikace v rámci rozsáhlejší rozvody, která obsahuje více RTU.

PowerCyber CPS vyvinutý na Iowa State University (ISU) [53] je hybridní testovací prostředí složení z hardwaru a softwaru, emulovaných komponent a RTDS. Prostředí se skládá ze SCADA od společnosti Siemens, který zahrnuje systém automatizace rozvodny (SICAM PAS), software řídicího centra (Power TG), čtyři ochranná relé (Siemens 7SJ610, 7SJ82), tři jednotky měření fázorů (PMU) SEL 421 a koncentrátor fázorových dat (PDC). Komunikaci mezi prvky zajišťují protokoly DNP3, IEC 61850 a IEEE C37.118. Testovací prostředí lze klasifikovat jako emulátor elektrické stanice se simulovanými vstupy z RTDS a OPAL-RT s možností komunikace do SCADA.

RICS-el popsaný v článku [51] je virtuální testovací prostředí postavené nad infrastrukturou Cyber Range And Training Environment (CRATE) ve Švédské agentuře pro obranný výzkum (FOI). Prostředí je postaveno na virtualizačním nástroji VirtualBox a skládá se ze segmentu OT a IT. OT síť obsahuje tři RTU komunikující prostřednictvím protokolu IEC 60870-5-104. Na RTU je připojen emulátor páteřní vysokonapěťovou 400kV síť s dvaceti rozvodnami. IT síť obsahuje boty, kteří simulují odesílaní a čtení e-mailů, vyhledávání na webu nebo otevírání, úpravu a zavíraní dokumentů. Oba segmenty zajišťují širokou škálu scénářů, které je možné pomocí prostředí simulovat. RICS-el lze klasifikovat jako komplexní virtualizační prostředí, které umožňuje simulovat mimo energetickou infrastrukturu i IT segment a tím rozšířit škálu použití např. pro výukové účely nebo simulaci objemových dat. V článku však nejsou popsány bližší informace k jednotlivým částem, ať už je to simulátor elektrické sítě, realizace RTU nebo SCADA.

V článku [197] autoři představují testovací prostředí složené z virtualizovaných komponentů pomocí nástroje OPNET a simulovaných prvků pomocí virtuálních strojů, na kterých jsou relizovány síťové a koncové prvky. Prostředí je složeno z IT podnikové sítě a OT sítě, kde jsou obsaženy SCADA, HIMI, RTU a IED jednotky. Pro komunikaci v rámci OT jsou implementovány proto-

koly Modbus/TCP, DNP3 a IEC 60870. Zaměření testovacího prostředí je na možnost simulace a analýzu kybernetických hrozeb. Prostředí lze klasifikovat jako simulátor energetické datové infrastruktury s možností realizace komplexních scénářů díky přítomnosti IT segmentu.

Testovací prostředí představené v článku [168] je vybudováno za účelem výzkumu v oblasti metod zabezpečení ICS/SCADA. Prostředí je koncipované, aby osahovalo všechny důležité prvky jako je IED, HMI, RTU, SCADA a EMS, které jsou emulovány na desktopových počítačích. Komunikaci zajišťují protokoly DPN3, 61850, ICCP/TASE.2. Vzhledem k oblasti zaměření jsou součástí prostředí i IDS a Firewall, které zajišťují zabezpečení jednotlivých částí. Pro testování jsou v rámci scénářů simulovány různé útoky, na kterých jsou ověřovány detekčních schopnosti implementovaných IDS. Prostředí lze klasifikovat jako bezpečnostní simulační nástroj pro SCADA/ICS. Výhodou je použití protokolu TASE.2, který se používá pro výměnu dat mezi SCADA.

Experimentální testovací prostředí z článku [85] bylo realizováno za účelem testovací a výukové metodiky. Podnětem pro realizaci bylo vytvoření prostředí na open-source nástrojích jako je IEDScout vyvinutý společností OMICRON a knihovna libiec61850 vyvíjení společnosti MZ Automation. Prostředí je složeno ze zmíněných nástrojů, které simulují prvky na jednotlivé vrstvách elektrické stanice dle standardu IEC 61850. Komunikace probíhá dle definovaných protokolů GOOSE, SV a MMS. Analýza komunikace probíhá pomocí nástroje Wireshark. V článku jsou uvedeny pouze počáteční testování navrženého prostředí a autoři sami uvádějí, že se jedná o předběžné výsledky, které měli potvrdit vhodnost vybraných nástrojů. Prostředí lze klasifikovat jako jednoduchou simulaci elektrické stanice pomocí standardu IEC 61850.

Dle autorů v článku [196] je hlavním cílem pro vytvoření testovacího prostředí potencionální kybernetická zranitelnost datových sítí v oblasti energetiky. Prostředí se skládá ze elektrické sítě simulované pomocí Matlab, virtualizovaných MU a IED, protokolů GOOSE, SV a MMS zproztředkovávající komunikace mezi zařízeními dle standardu IEC 61850 a stanic simulující kybernetické zranitelnosti na jednotlivé části systému. Dle autorů není testovací prostředí ve finální fázi a v budoucím výzkumu ho plánují rozšířit o reálné IED, SCADA a o simulaci kybernetických hrozeb pro analýzu jejich dopadu. Prostředí lze klasifikovat jako emulátor na úrovni elektrické stanice s možností simulace kybernetické incidentů.

C Příloha - Logické uzly pro IED 1 a IED 4

Název	Datový typ
Interlocking	
CILO1CFMod	ENC
CILO1DCNamPlt	LPL
CILO1EXNamPlt	LPL
CILO1STBeh	ENS
CILO1STEnaCls	SPS
CILO1STHealth	ENS
CILO1STMod	ENC
Logical device LN	
LLN0BREventsRCB01	-
LLN0CFMod	ENC
LLN0DCNamPlt	LPL
LLN0EXNamPlt	LPL
LLN0GOgcbEvents	-
LLN0STBeh	ENS
LLN0STHealth	ENS
LLN0STMod	ENC
Physical device LN	
LPHD1DCPhyNam	DPL
LPHD1STPhyHealth	ENS
LPHD1STProxy	SPS
Switch controller 1	
CSWI1CFMod	ENC
CSWI1CFPos	DPC
CSWI1COPos	DPC
CSWI1DCNamPlt	LPL
CSWI1ORPos	DPC
CSWI1STBeh	ENS
CSWI1STHealth	ENS
CSWI1STMod	ENC
CSWI1STPos	DPC

Tab. C.1: Logické veličiny generované zařízením IED1 (1. část)

Název	Datový typ
Switch controller 2	
CSWI2CFMod	ENC
CSWI2CFPos	DPC
CSWI2COPos	DPC
CSWI2DCNamPlt	LPL
CSWI2ORPos	DPC
CSWI2STBeh	ENS
CSWI2STHealth	ENS
CSWI2STMod	ENC
CSWI2STPos	DPC
Interlocking	
XCBR1CFBlkCls	SPC
XCBR1CFBlkOpn	SPC
XCBR1CFLoc	SPS
XCBR1CFMod	ENG
XCBR1COBlkCls	SPC
XCBR1COBlkOpn	SPC
XCBR1COLoc	SPS
XCBR1DCNamPlt	LPL
XCBR1STBeh	ENS
XCBR1STBlkCls	SPC
XCBR1STBlkOpn	SPC
XCBR1STHealth	ENS
XCBR1STLoc	SPS
XCBR1STMod	ENC
XCBR1STOpCnt	INS
XCBR1STPos	DPC
Circuit switch	
XSWI2CFBlkCls	SPC
XSWI2CFBlkOpn	SPC
XSWI2CFLoc	SPS
XSWI2CFMod	ENC
XSWI2COBlkCls	SPC
XSWI2COBlkOpn	SPC
XSWI2COLoc	SPS
XSWI2DCNamPlt	LPL
XSWI2STBeh	ENS
XSWI2STBlkCls	SPC
XSWI2STBlkOpn	SPC
XSWI2STHealth	ENS
XSWI2STLoc	SPS
XSWI2STMod	ENC
XSWI2STOpCnt	INS
XSWI2STPos	DPC
XSWI2STSwTyp	ENS

Tab. C.2: Logické veličiny generované zařízením IED1 (2 část)

Název	Datový typ
Generic process I/O	
GGIO1CFMod	ENC
GGIO1CFSPCSO1	SPC
GGIO1CFSPCSO2	SPC
GGIO1CFSPCSO3	SPC
GGIO1CFSPCSO4	SPC
GGIO1COSPCSO1	SPC
GGIO1COSPCSO2	SPC
GGIO1COSPCSO3	SPC
GGIO1COSPCSO4	SPC
GGIO1DCNamPlt	LPL
GGIO1MXAnIn1	MV
GGIO1MXAnIn2	MV
GGIO1MXAnIn3	MV
GGIO1MXAnIn4	MV
GGIO1STBeh	ENS
GGIO1STHealth	ENS
GGIO1STInd1	SPS
GGIO1STInd2	SPS
GGIO1STInd3	SPS
GGIO1STInd4	SPS
GGIO1STMod	ENC
GGIO1STSPCSO1	SPC
GGIO1STSPCSO2	SPC
GGIO1STSPCSO3	SPC
GGIO1STSPCSO4	SPC
Logical device LN	
LLN0CFMod	ENC
LLN0DCNamPlt	LPL
LLN0EXNamPlt	LPL
LLN0GOgcbEvents	STS
LLN0STBeh	ENS
LLN0STHealth	ENS
LLN0STMod	ENC

Tab. C.3: Logické veličiny generované zařízením IED2 (1. část)

Název	Datový typ
Physical device LN	
LPHD1DCPhyNam	DPL
LPHD1STPhyHealth	ENS
LPHD1STProxy	SPS
Time overcurrent	
PTOC1CFMod	ENC
PTOC1DCNamPlt	LPL
PTOC1SPTmACrv	CURVE
PTOC1STBeh	ENS
PTOC1STHealth	ENS
PTOC1STMod	ENC
PTOC1STOp	ACT
PTOC1STStr	ACD
Protection trip conditionning	
PTRC1CFMod	ENC
PTRC1DCNamPlt	LPL
PTRC1STBeh	ENS
PTRC1STHealth	ENS
PTRC1STMod	ENC
PTRC1STOp	ACT
PTRC1STTr	ACT

Tab. C.4: Logické veličiny generované zařízením IED2 (2. část)

Název	Datový typ
Logical device LN	
LLN0STMod	ENC
Měřící logická jednotka	
MMXU1CFAvAPhs	MV
MMXU1CFAvPhVPhs	MV
MMXU1CFMaxAPhs	MV
MMXU1CFMaxPhVPhs	MV
MMXU1CFMinAPhs	MV
MMXU1CFMinPhVPhs	MV
MMXU1CFMod	ENC
MMXU1DCNamPlt	LPL
MMXU1MXAvAPhs	MV
MMXU1MXAvPhVPhs	MV
MMXU1MXMaxAPhs	MV
MMXU1MXMaxPhVPhs	MV
MMXU1MXMinAPhs	MV
MMXU1MXMinPhVPhs	MV
MMXU1STBeh	ENS
MMXU1STHealth	ENS
MMXU1STMod	ENC
Proudový transformátor LN	
TCTR1CFAmp	MV
TCTR1MXAmp	MV
TCTR2CFAmp	MV
TCTR2MXAmp	MV
TCTR3CFAmp	MV
TCTR3MXAmp	MV
TCTR4CFAmp	MV
TCTR4MXAmp	MV
Napěťový transformátor LN	
TVTR1CFVol	MV
TVTR1MXVol	MV
TVTR2CFVol	MV
TVTR2MXVol	MV
TVTR3CFVol	MV
TVTR3MXVol	MV
TVTR4CFVol	MV
TVTR4MXVol	MV

Tab. C.5: Logické veličiny generované zařízením IED3 a IED4

Datový bod (IEC 61850)	**Typ**	**IOA (IEC 60870)**	**Jednotka**
IED1_XCBRGenericIO$CSWI1$CF$Pos	int	1006	pozice*
IED1_XCBRGenericIO$CSWI2$CF$Pos	int	1014	pozice*
IED1_XCBRGenericIO$XCBR1$ST$Pos	int	1040	pozice
IED1_XCBRGenericIO$XSWI2$ST$Pos	int	1055	pozice
IED2_PTOCGenericIO$GGIO1$CF$SPCSO1	bool	2001	vyp/zap
IED2_PTOCGenericIO$GGIO1$CF$SPCSO2	bool	2002	vyp/zap
IED2_PTOCGenericIO$GGIO1$CF$SPCSO3	bool	2003	vyp/zap
IED2_PTOCGenericIO$GGIO1$CF$SPCSO4	bool	2004	vyp/zap
IED3_SMVMUnn$MMXU1$MX$AvAPhs	float	3008	A
IED3_SMVMUnn$MMXU1$MX$AvPhVPhs	float	3009	V
IED3_SMVMUnn$TCTR1$MX$Amp	float	3018	A
IED3_SMVMUnn$TCTR2$MX$Amp	float	3020	A
IED3_SMVMUnn$TCTR3$MX$Amp	float	3022	A
IED3_SMVMUnn$TVTR1$MX$Vol	float	3026	V
IED3_SMVMUnn$TVTR2$MX$Vol	float	3028	V
IED3_SMVMUnn$TVTR3$MX$Vol	float	3030	V
IED4_SMVMUnn$MMXU1$MX$AvAPhs	float	4008	A
IED4_SMVMUnn$MMXU1$MX$AvPhVPhs	float	4009	V
IED4_SMVMUnn$TCTR1$MX$Amp	float	4018	A
IED4_SMVMUnn$TCTR2$MX$Amp	float	4020	A
IED4_SMVMUnn$TCTR3$MX$Amp	float	4022	A
IED4_SMVMUnn$TVTR1$MX$Vol	float	4026	V
IED4_SMVMUnn$TVTR2$MX$Vol	float	4028	V
IED4_SMVMUnn$TVTR3$MX$Vol	float	4030	V

**ovládatelná hodnota*

Tab. C.6: Mapování dat z modelu IEC 61850 do IEC 60870-5-104.

D Příloha - Tabulky pro Testování BPL komunikace pomocí Emulační jednotky

Tab. D.1: Seznam požadavků na naměření a přenášení informací – VN pole

H-kód	**popis prvku**	**Typ 104**	**Poznámka**
f3QM	Vypínač vypnut	DP (TI 4/31)	každé pole
f4QM	Vypínač zapnut	DP (TI 4/31)	každé pole
f3QV	Odpojovač QV vypnut	DP (TI 4/31)	každé pole
f4QV	Odpojovač QV zapnut	DP (TI 4/31)	každé pole
f3QE	Uzemňovač vypnut	DP (TI 4/31)	každé pole
f4QE	Uzemňovač zapnut	DP (TI 4/31)	každé pole
H8311L	Ztráta ovládacího napětí	SP (TI2/30)	každé pole
H891T	Vypnutí jističe pohonu vypínače	SP (TI2/30)	každé pole
H912CCB	Pohon vypínače nenastřádán	SP (TI2/30)	každé pole
F5RS	Ovládání Místně/Dálkově	SP (TI2/30)	každé pole
H850OFF	Přítomnost zpětného napětí není	DP (TI 4/31)	každé pole
H850ON	Přítomnost zpětného napětí je	DP (TI 4/31)	každé pole
H231A	Pokles tlaku SF6	SP (TI2/30)	každé pole – modulární/1 pole – kompaktní
H854WA1T	Vypnutí jističe MTN	SP (TI2/30)	dle technologie/ 1x na sběrně
H8313YL	Ztráta signalizačního napětí	SP (TI2/30)	každé pole/dle koncepce
H9940DRO	Otevření dveří VN nástavby	SP (TI2/30)	každé pole/dle koncepce
H111T	Působení nadproudové ochrany	SP (TI2/30)	každé pole/sloučeny 50 I> a 67 I>
H121T	Působení zkratové ochrany	SP (TI2/30)	každé pole/sloučeny 50 I» a 67 I»
H141T	Působení nadproudové zemní ochrany	SP (TI2/30)	každé pole/ 50N I>, 50N I», 67N I>, 67N I»
H410A	Zemní spojení vývodu výstraha	SP (TI2/30)	každé pole
H101GPF	Porucha systému chránění	SP (TI2/30)	každé pole
H111SIL	Ztráta komunikace ochrany	SP (TI2/30)	každé pole
H111IF	Vnitřní porucha ochrany	SP (TI2/30)	každé pole
f1QM	Vypínač vypnout	DP (TI 4/46)	každé pole
f2QM	Vypínač zapnout	DP (TI 4/46)	každé pole
mU12	Sdružené napětí U12	ME (TI 36)	každé pole/sběrna (dle umístění měničů)
mI2	Proud I2	ME (TI 36)	každé pole
mP	3f Činný výkon	ME (TI 36)	každé pole
mQ	3f Jalový výkon	ME (TI 36)	každé pole
mVZDALP	lokátor poruch	ME (TI 36)	každé pole

Tab. D.2: Počet objektů a datové typy pro NN rozvaděč

1x NN rozvaděč	**12x NN rozvaděč**
12x SP (TI2/30)	144x SP (TI2/30)
3x DP (TI 4/31)	36x DP (TI 4/31)
1x SC (TI 2/45)	12x SC (TI 2/45)
1x DP (TI 4/46)	12x DP (TI 4/46)
5x ME (TI 36)	60x ME (TI 36)