VĚDECKÉ SPISY VYSOKÉHO UČENÍ TECHNICKÉHO V BRNĚ
Edice Habilitační a inaugurační spisy, sv. 756
ISSN 1213-418X

Radek Fujdiak

MODERNÍ PROVOZNÍ TECHNOLOGIE

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
FAKULTA ELEKTROTECHNIKY A KOMUNIKAČNÍCH TECHNOLOGIÍ
ÚSTAV TELEKOMUNIKACÍ

Ing. Radek Fujdiak, Ph.D.

MODERNÍ PROVOZNÍ TECHNOLOGIE

MODERN OPERATIONAL TECHNOLOGIES

TEZE HABILITAČNÍ PRÁCE
V OBORU TELEINFORMATIKA

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
NAKLADATELSTVÍ VUTIUM

BRNO 2023

KLÍČOVÁ SLOVA
Provozní technologie (OT); Součásti OT; Procesy; Senzory; Akční členy; Aktuátory; Kontroléry; Rozhraní člověk-stroj (HMI); Komunikační techniky a technologie; IT/OT konvergence; Průmyslové aplikace

KEYWORDS
Operational Technology (OT); Components of OT; Processes; Sensors; Actuators; Controllers; Human-Machine Interface (HMI); Communication Techniques and Technologies; IT/OT Convergence; Industrial Applications

ARCHIVOVÁNO
Vědecké a zahraniční oddělení, Fakulta elektrotechniky a komunikačních technologií, Vysoké učení technické v Brně, Technická 3058/10, 616 00, Brno

ISBN 978-80-214-6162-8
ISSN 1213-418X

Obsah

O autorovi

Radek Fujdiak své bakalářské, magisterské i doktorské studium absolvoval na Fakultě elektrotechniky a komunikačních technologií Vysokého učení technického v Brně. Od roku 2014 působí na Ústavu telekomunikací FEKT VUT v Brně jako vědecký pracovník. Během tohoto působení se zapojil do výuky, výchovy pregraduálních/doktorských studentů a do řady výzkumných projektů, jejichž výsledky průběžně publikoval na konferencích a v prestižních časopisech.

Z hlediska pedagogické praxe průběžně vyučoval magisterské a bakalářské předměty a to i pro zahraniční studenty (mj. MVDP, CZKR, BDAK a BCZS). Je autorem/spoluautorem celé řady výukových materiálů, jako např. prezentací, online přednášek, interaktivních ukázek, laboratorních cvičení, aj. Byl a je vedoucí řady studentských prací (doktorské, magisterské i bakalářské), které jsou úspěšně řešeny či byly úspěšně obhájeny. Momentálně vedu 4 doktorandy. Kromě toho vedl i řadu stáží zahraničních studentů. Realizoval každoročně několik zvaných přednášek na zahraničních univerzitách či na akcích průmyslových partnerů.

Z hlediska vědy je autorem více než 100 publikačních prací, kde indexovaných databází Web of Science je 72 položek (431 citací bez autocitací, h-index 12) a databází SCOPUS je 79 položek (608 citací bez autocitací, h-index 18). Je také autorem/spoluautorem řady softwarových řešení, funkčních vzorků a řady užitných vzorů. V drtivé většině se jedná o produkty, které byly vytvořeny ve spolupráci s aplikační sférou v rámci grantových projektů či hospodářských smluv. Tematicky jsou tyto výsledky zasazeny do kybernetické bezpečnosti, průmyslových sítí, pokročilé virtualizace a datové analýzy. Je/byl hlavním řešitelem/spoluřešitelem či členem vědeckého týmu řady výzkumných projektů interního, národního, evropského či mezinárodního charakteru včetně hospodářského smluvního výzkumu. Radek Fujdiak je také členem výzkumné skupiny/laboratoře CyberGrid, která pomáhá k tvorbě bezpečného prostředí v energetice a průmyslu. V této oblasti spolupracujeme s mnoha lokálními a mezinárodními univerzitami, výzkumnými instituty, firmami či státními institucemi.

Úvod

Rozvoj průmyslu od 18. století, kdy byl poprvé představen tkalcovský stroj, až do současnosti, se stal příkladem neustálého posouvání hranic technologického pokroku. Tyto změny lze rozdělit do pěti průmyslových revolucí: Průmyslová revoluce (1760-1840), Průmyslová revoluce parního stroje (1840-1920), Elektrifikace a automatizace (1920-1960), Konvergence informačních a provozních technologií (1960-2010) a Průmysl 4.0 (od 2010). Průmyslová revoluce (1760-1840) byla charakterizována vynálezem a rozšířením mechanizovaných tkalcovských stavů, které přinesly zrychlení výroby textilních výrobků a změnu způsobu výroby. Průmyslová revoluce parního stroje (1840-1920) se zaměřila na rozšíření parního strojařství, které umožnilo výrobu většího množství produktů za kratší dobu, vedlo k růstu ekonomiky a k zlepšení životního standardu. Elektrifikace a automatizace (1920-1960) byla založena na elektrifikaci průmyslových výrobních linek a automatizaci výrobních procesů, což umožnilo výrobu produktů s vysokou efektivitou a zvýšení produktivity. Konvergence informačních a provozních technologií (1960-2010) přinesla plnou konvergenci informační technologie (Information Technology, IT) a provozní technologie (Operational Technology, OT) a vytvořila integrovanou informační a provozní architekturu, která umožnila nejen výrobu produktů s vysokou efektivitou, ale také řízení výroby a přenos dat v reálném čase. Tyto změny představovaly významný krok vpřed v historii průmyslu a umožnily výrobu produktů s vyšší kvalitou a nižšími náklady. V současnosti se již začíná mluvit o páté průmyslové revoluci, která bude zaměřena na rozvoj robotiky, umělé inteligence, obnovitelných zdrojů, dekarbonizace, deindustrializace, spolupráce mezi člověkem a robotem (kolaborativním robotem), bio-ekonomiky a dalších řešení, která přicházejí do průmyslového ekosystému. Tyto trendy představují budoucnost průmyslu, který bude více efektivní, udržitelný a spojený s informačními technologiemi. Samotný koncept chápání průmyslového světa se tak značným způsobem mění od technologií, až po samotné koncepty chápání výroby, či přístupu k jednotlivým průmyslovým procesům. Výroba se stává více flexibilní a pružnou, což umožňuje výrobcům reagovat na změny v poptávce a zlepšovat své procesy. Tyto změny vedou k vyšší konkurenceschopnosti průmyslových odvětví na světovém trhu a k zlepšení životního standardu pro spotřebitele. A právě zlepšení životního standardu pro spotřebitele je – mimo jiné, jedním z důvodů vzniku této práce, která se zabývá aktuální problematikou průmyslových sítí, resp. konkrétně moderním provozním technologiím, jejich součástem, a to od samotného procesu, přes zařízení, až po infrastrukturu a architekturu. V neposlední řadě nad rámec ucelené teoretické stránky s redefinovanou terminologií přináší tato práce také praktické poznatky z výzkumu a vývoje v rámci reálných průmyslových systémů včetně ukázky jejich realizace od návrhu, přes implementaci až k finalizaci.

1 Podstata a přehled práce

1.1 Motivace práce

V oblasti OT došlo v posledních letech k významným změnám, kdy se prostředí stává stále dynamičtějším a složitějším s konvergencí IT a OT. Digitalizace průmyslu vedla ke značnému pokroku, avšak současně komplikuje pochopení základních principů a technologií, které jsou v této oblasti důležité. Terminologie a pojmy používané k popisu OT a souvisejících technologií mohou být nekonzistentní a matoucí, kvůli kritické povaze mnoha OT systémů je tak nezbytné pečlivé a přesné pochopení daných termínů. V současnosti se rozšiřuje využití digitálních technologií v kritických infrastrukturách, jako jsou energetické, vodní, dopravní a komunikační systémy, což zdůrazňuje nutnost porozumět základním principům OT. Tyto systémy hrají klíčovou roli v našem každodenním životě a vyžadují integraci složitých technologií a procesů, aby byl zajištěn jejich spolehlivý provoz. Proto je nutné, aby vývoj a implementace nových OT technologií a procesů byly provedeny s pečlivostí a ohledem na jejich dopad na kritickou infrastrukturu a širší společnost. S rostoucím významem digitálních technologií a složitostí v oblasti OT se stává tento obor vzrušujícím a důležitým polem pro výzkum a publikování. S rostoucí závislostí na digitálních technologiích je zásadní dosáhnout komplexní porozumění základním principům a technologiím v této oblasti, což může pomoci organizacím lépe se připravit na výzvy a příležitosti, které představují rychle se měnící prostředí a neustálý vývoj OT. Tyto výzvy a příležitosti mohou být komplexní a vyžadují odbornou znalost a schopnost průběžně se vyvíjet a adaptovat se, aby byly tyto problémy dostatečně řešeny. Proto je třeba, aby se organizace a podniky snažily rozvíjet své znalosti a dovednosti v oblasti OT, aby mohly využívat potenciál digitálních technologií a zároveň minimalizovat rizika spojená s jejich využitím. Tato práce tak nabízí jasný a přesný pohled na základní principy a technologie v oblasti OT, a tím poskytuje cenné informace pro organizace, které se snaží rozvíjet své znalosti v této oblasti. V neposlední řadě je motivací nejednotnost v terminologii v rámci OT. Tento problém je způsoben rostoucím rozvojem jednotlivých odvětví v průmyslu, jejich slučováním, rozvojem různých technologií v rámci různých vývojových větví a aplikačních odvětví. Tyto faktory vedou k výskytu nekonzistentností v terminologii a teoretických poznatcích, což může být pro odborníky a laickou veřejnost obtížně srozumitelné. Motivací pro tuto práci je tedy sjednotit terminologii a teoretické poznatky v oblasti OT do jednoho uceleného celku, který bude jasně představovat OT a jejich význam pro společnost. Toto sjednocení terminologie a teoretických poznatků může pomoci odborníkům v této oblasti lépe komunikovat a spolupracovat, stejně jako může pomoci laické veřejnosti lépe pochopit důležitost OT pro naši společnost.

1.2 Cíle práce

Cílem této práce je vymezit a analyzovat současný stav konvergence IT/OT a jejich vliv na průmysl. Růst digitalizace průmyslu v posledních letech přináší nové možnosti, ale také nové výzvy. Tyto změny se projevují také ve změněném prostředí, kde se organizace a podniky snaží přizpůsobit a rozvíjet své OT. Proto je nutné analyzovat a porozumět vlivům těchto změn na implementaci a přijetí OT. Dalším cílem práce je zkoumat nejednotnost terminologie v rámci OT, která vznikla v důsledku rozvoje jednotlivých odvětví a technologií. Tyto cíle vedou k definici a sjednocení terminologie v oboru OT, což pomůže v budoucnu lépe porozumět principům a technologiím v této oblasti. V rámci této práce se také analyzuje role standardů, norem a předpisů při utváření vývoje a implementace OT systémů. Tyto standardy a předpisy zajišťují bezpečný a spolehlivý provoz kritických infrastruktur, a proto je nutné je pečlivě zvážit při vývoji a implementaci nových OT systémů. V neposlední řadě bude tato práce ukazovat možnosti realizace dnešních průmyslových sítí pomocí OT technologií, od návrhu až po finalizaci. Tato ukázka bude demonstrovat, jak lze využít moderních technologií, jako je Průmysl 4.0 a internet věcí (IoT), k realizaci efektivního a spolehlivého provozu průmyslových sítí. Celkově tedy cílem této práce je analyzovat současný stav konvergence IT/OT a její vliv na průmysl, zkoumat výzvy a příležitosti, které přináší digitalizace průmyslu, a definovat prostředí OT v kontextu moderních technologií. Práce také zkoumá nejednotnost terminologie v rámci OT a zabývá se jejím sjednocením, roli standardů, norem a předpisů v utváření vývoje a implementace OT systémů a ukazuje možnosti realizace průmyslových sítí s využitím OT technologií. Tyto cíle jsou zásadní pro komplexní pochopení a rozvoj v oblasti OT a přispějí k lepší přípravě na výzvy a příležitosti, které přicházejí s digitalizací průmyslu. **Stěžejní otázky v rámci cílů práce tak lze shrnout takto:**

1. Jaké výzvy a příležitosti přináší digitalizace průmyslu?
2. Jak měnící se prostředí ovlivňuje přijetí a implementaci OT?
3. Jaká je současná úroveň jednotnosti terminologie používané v rámci OT a jak ji lze standardizovat?
4. Jakou roli hrají normy, předpisy a normy při utváření vývoje a implementace systémů OT?
5. Jaké jsou základní komponenty v rámci OT sítí a jak jsou napojeny na dnešní chápání průmyslových sítí?
6. Jaký je současný stav konvergence IT a OT a jaký je její dopad na průmysl?
7. Jak lze moderní OT technologie, jako je Průmysl 4.0 a IoT, využít k efektivnímu provozu průmyslových sítí?
8. Jaké překážky a řešení představuje implementace OT v průmyslových aplikací?

1.3 Přínos práce

Tato práce přináší řadu užitečných poznatků a přínosů v oblasti konvergence IT/OT. Prvním přínosem je analýza současného stavu konvergence IT/OT a jejího vlivu na průmysl. Tyto informace jsou pro organizace a podniky důležité, aby mohly lépe porozumět změnám, kterým čelí, a přizpůsobit se jim. Dalším přínosem je zkoumání výzev a příležitostí, které přináší digitalizace průmyslu. Tyto informace mohou být užitečné pro organizace při rozhodování o nových projektech a investicích, které mohou přinést významné konkurenční výhody. Tato práce také přináší sjednocení terminologie v oboru OT, což v budoucnu pomůže lepšímu porozumění principům a technologiím v této oblasti a pomohou v budoucnu vyhnout se nejasnostem a nedorozuměním. V rámci této práce se také analyzuje role standardů, norem a předpisů při utváření vývoje a implementace OT systémů. Tyto informace jsou pro organizace důležité pro správné a bezpečné fungování kritických infrastruktur. Tato práce dále představuje možnosti realizace dnešních průmyslových sítí pomocí OT technologií, od návrhu až po finalizaci. Celkově tedy tato práce přináší komplexní pohled na současný stav konvergence IT/OT, její vliv na průmysl, výzvy a příležitosti, které přináší digitalizace, sjednocení terminologie, analýzu role standardů, norem a předpisů a ukázku možností realizace průmyslových sítí pomocí OT technologií.

Návaznost na autorovy publikace. Autorovi publikace jsou v přímé souvislosti s tématikou této práce. Jedná se převážně o návaznost na dlouhodobý výzkum od roku 2017, tedy roku ukončení doktorského studia, v tématech, které jsou mj. základem pro praktickou část této práce. Jedná se tedy převážně o:

- Výzkum, vývoj a testování v oblasti funkčních a přenosových parametrů komunikačních i přenosových technologií v průmyslu (koexistence a interoperabilita [APub41, APub40, APub17, APub15]; výkonnostní, experimentální i funkční analýza, testování a měření [APub36, APub33, APub31, APub47, APub46, APub34, APub19, APub10, APub28]); nové způsoby využití stávajícíh dat [APub49]; blockchainové aplikace [APub14]; modelování a simulace [APub11, APub16, APub4, APub12, APub32]).
- Výzkum a vývoj v oblasti průmyslových testovacích polygonů, architektury a infrastruktury, kyber-fyzických systémů, kybernetických dvojčat a pokročilé virtualizace (komunikační a funkční modely [APub5]; kontejnerizace a virtualizace [APub18, APub1]; testovací a kyber-fyzické polygony [APub3, APub38, APub39]; emulace, modelování a simulace [APub50, APub51]; reálné aplikace [APub30, APub8]).
- Výzkum, vývoj a testování v oblasti kybernetické bezpečnosti a hrozeb v průmyslu (lehká kryptografie [APub6, APub27, APub48]; kybernetické útoky, je-

jich dopad a mitigace [APub45, APub43, APub29, APub52, APub42]; bezpečný návrh a vývojový životní cyklus [APub13, APub9, APub22]; bezpečnostní testování průmyslových sítí [APub7, APub23, APub24, APub35]; detekce anomálií a hrozeb [APub2, APub20, APub26, APub37, APub44, APub25, APub21]).

Návaznost na studijní materiály. Jako první je nutno zmínit autorovi dvě knižní publikace, které přináší v rámci knihy *Budování Cyber Range platformy s technologií cloud computingu* [APed11] zcela nové poznatky v oblastech kybernetických polygonů, edukace i trénování v kybernetické bezpečnosti, a to v návaznosti mj. na průmyslové aplikace. Z pohledu druhé knižní publikace *Counter measure techniques for cryptographic algorithms eliminating power analysis attacks (Extended Version)* jsou to pak převážně metody zajištění bezpečnosti proti fyzickým útokům postranními kanály. Jako další lze zmínit řadu studijních materiálů využívaných v rámci bakalářských kurzů (předměty: BVKS [APed10, APed5], BCZS [APed8], BIOT [APed6], BDAK [APed3, APed2], CZKR [APed4]) i magisterských kurzů (předměty: MKRI [APed1], MPPR [APed7], MVDP [APed9]) na VUT v Brně. Poznatky z těchto materiálů jsou převážně přeneseny do teoretické částí této práce.

Výzkumné projekty a hospodářské smlouvy. Autor práce se aktivně účastnil řady výzkumných projektů interního, národního, evropského či mezinárodního charakteru, stejně tak v případě hospodářských smluv, a to jako řešitel (R), další řešitel či spoluřešitel (S), či člen řešitelského týmu (C):

- V rámci účasti na interních projektech se jednalo výzkum a vývoj elektronických, informačních a průmyslových komunikačních systémů včetně jejich kybernetické bezpečnosti: FEKT-S-14-2352 (S) [APro4], FEKT-S-17-4184 (S) [APro5], FAST/FEKT-J-16-3344 (S) [APro3], FEKT-S-20-6312 (S) [APro6], FEKT/FIT-J-18-5434 (C) [APro7], FEKT/FIT-J-19-5905 (C) [APro8], a FEKT/FIT-J-19-5906 (C) [APro9].
- V rámci účasti na národních projektech se jednalo o oblasti kyberbezpečnostního dohledu nad průmyslovými sítěmi, kritickou infrastrukturou, pokročilou virtualizací a kyber-fyzickými polygony, jednalo se o projekty: VI20172019057 (C) [APro17], FV20487 (S) [APro10], TJ01000381 (S) [APro13], TJ02000332 (R) [APro14], TK02030013 (S) [APro15], VI20192022132 (S) [APro18], FV40366 (S) [APro11], FW01010474 (S) [APro12], a TK03010091 (C) [APro16].
- V rámci účasti na nadnárodních projektech (mj. AQUAS (C)[APro2] a RUGGEDISED (C) [APro1]) se jednalo především o oblasti průmyslových sítích a problematiky kontradikce užitných parametrů jako výkon, pracovní bezpečnost či kyberbezpečnost.

2 Provozní technologie

Provozní technologie, někdy také označované jako operační technologie, jsou zjednodušeně veškerý hardware a software používaný k řízení, monitorování a/nebo udržování fyzických aktiv, procesů nebo událostí. Pro příklad tedy lze říci, že se jedná o obrábění, svařování, lisování, tvarování plastů a mnoho dalších. Tyto technologie se používají (nejen) k výrobě výrobků, které splňují požadavky zákazníka co nejpřesněji, a to co nejefektivněji, k čemuž se právě využívají dnes i moderní technologie pro monitorování, řízení či plánování. To znamená obsáhnutí technologií od fyzických zařízení, tedy např. různých aktuátorů, tedy pohybových zařízení, která dokážou pohybovat nebo ovlivňovat pozici objektů (například při výrobě automobilů mohou být aktuátory použity k ovládání pohybu lisovacích forem nebo k ovládání pohybu svařovacích ramen), až po kontrolní centra, ekonomická či manažerská oddělení.

Tyto technologie jsou páteřním prvkem pro mnoho podniků či firem, jelikož jsou součástí jejich každodenní produkční činnosti [18]. Dnes jsou však OT již součástí téměř všech oblastí lidské činnosti [13], včetně energetiky (naftařství, plynárenství, elektroenergetiky či teplárenství), chemického průmyslu, výrobního a strojírenského průmyslu, vodohospodářství, zpracování odpadu, přepravy, logistiky, potravinářství, zemědělství, zdravotnictví, hutnictví a těžařského průmyslu, ale i spousty dalších oblastí, např. i prosté automatizace budov či domácností. OT tak hrají klíčovou roli v zajišťování tzv. kritické výroby a kritické infrastruktury, jakož i v udržování jejich efektivního fungování. Kritická výroba a kritická infrastruktura jsou dva pojmy, které se týkají klíčových aspektů hospodářství a bezpečnosti jednotlivých zemí. Kritická výroba zahrnuje sektory, jako jsou energie, zdroje, zásobování potravinami a zdravotnictví, které jsou nezbytné pro chod společnosti. Tyto sektory musí být neustále v provozu, aby se zajistilo, že populace má přístup k základním potřebám a službám. Kritická infrastruktura zahrnuje komunikační systémy, dopravní sítě, vodárny a elektrárny, které jsou rovněž klíčové pro fungování společnosti. Tyto systémy musí být chráněny proti vnějším hrozbám, jako jsou přírodní katastrofy, teroristické útoky nebo kybernetické útoky, aby se zajistilo, že budou fungovat neustále a bezpečně.

S pojem kritická výroba se však převážně setkáváme v rámci např. Spojených států amerických. V rámci České republiky (ČR) se využívá hlavně pojmu kritická infrastruktura, definována v ČR dle zákona č. 240/2000 Sb. [19], tedy jako prvek kritické infrastruktury nebo systém prvků kritické infrastruktury, jehož narušení by mělo závažný dopad na bezpečnost státu, zabezpečení základních životních potřeb obyvatelstva, zdraví osob nebo ekonomiku státu. Z definice však tedy kritická výroba v ČR spadá do kritické infrastruktury.

2.1 Základní terminologie

Na začátek je z pohledu terminologie důležité vysvětlit rozdíly v rámci překladu termínu OT v odborných českých textech. Je nutno říci, že aktuálně neexistuje přímá (přesná) definice termínu OT či jeho překladu. Objevují se aktuálně dvě hlavní varianty:

- provozní technologie (zkratkou jako OT, ale někdy také česky jako PT) [4],
- operační technologie (jako přímý překlad, zkratkou jako OT) [14].

Termínově se jedná o ekvivalenty a synonyma. V rámci českého jazyka je však termín *operační technologie* spojen převážně s vyjádřením funkční (provozu-schopná) technologie [6] či s termínem v souvislosti např. se zdravotnickými (chirurgickými) operacemi [2]. Pro ČR lze dále sledovat oficiální směr překladů pro OT z evropských direktiv a nařízení, kde je využíván překlad:

- *Operational technology* jako operační technologie [6], ve smyslu funkční (provozuschopné) technologie, systém či síť.
- *Operational technology* jako provozní technologie [7, 8], ve smyslu programovatelných digitálních systémů nebo zařízení, které interagují s fyzickým prostředím nebo řídí zařízení, která interagují s fyzickým prostředím.

Termín provozní technologie se tak jeví z tohoto pohledu jako vhodnější, díky souladu s platnou legislativou, a bude proto i dále v textu v tomto smyslu používán. Z pohledu zkratky pak je používání OT oproti PT mnohem více zažité, kdy zkratka PT je používána minimálně, a tedy i z tohoto důvodu bude používáno terminologie – provozní technologie (OT).

Termín OT je spjat také s průmyslovými řídicími systémy (ICS, Industrial Control Systems). Termín ICS vznikl jako reakce na rozdílnou terminologii způsobenou různým vývojem jednotlivých odvětví, kdy se v posledních 30 letech hledal termín, který by zahrnoval všechny formy průmyslové automatizace (IA, Industrial Automation) [3]. První návrhy směřovaly do termínu – řídicí systém (Control System), to však bohužel zahrnovalo terminologicky nejen IA, ale také oblasti jako automatizaci budov (Building Automation), či automatizaci domácnosti (Home Automation). Z této problematiky tak vzešel hybridní termín – průmyslový řídicí systém (ICS, Industrial Control System), který byl velmi rychle přijat širokou odbornou veřejností, a který se začal používat jako termín zahrnující veškeré formy IA. ICS je používán mj. i Národním institutem standardů a technologií (NIST, National Institute of Standards and Technologies), např. v rámci publikace NIST SP 800-82 [16].

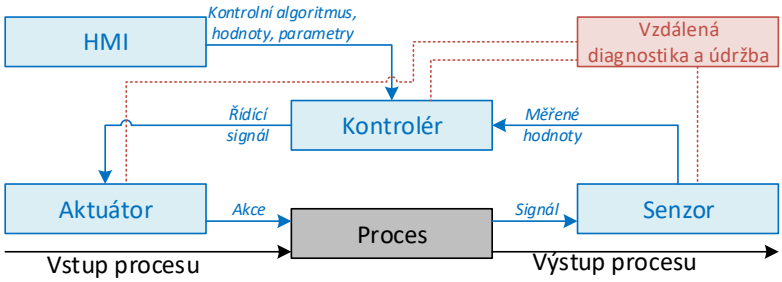
S ohledem k OT, ICS a IA se lze také ještě setkat s označením průmyslová automatizace a řídicí systémy (IACS, Industrial Automation and Control Systems), což je termín představený Mezinárodní společností pro automatizaci (ISA, International Society of Automation). Nutno zmínit, že do roku 2006 byl IACS označo-

ván organizací ISA jako výrobní a průmyslové systémy (M&CS, Manufacturing and Control Systems). ISA označení IACS využívá ve spojitosti s kybernetickou bezpečností v sérii standardů a norem označovaného jako ISA-99 [11] (známého také jako IEC/ANSI/ISA 62433 [15]). Série standardů ISA-99 byla vytvořena v rámci výboru 99 organizace ISA a nesla tedy označení ISA-99. Následně byla série akreditována a publikována Americkým Národním Standardizačním Institutem (ANSI), kde došlo v roce 2010 k přečíslování na ANSI/ISA-62443. Série pak byla převzata i Mezinárodní elektrotechnickou komisí (IEC, International Electrotechnical Commission) jako IEC 62443, což je již označení v oboru široce známé. Z definice standardu IEC 62443-1-1 [10], IACS pokrývá řídicí systémy využívané ve výrobních a zpracovatelských závodech, systémech kontroly životního prostředí, geograficky rozsáhlých systémech (mj. elektřina, plyn a voda), potrubí a petrochemický průmysl, ale i další průmyslová odvětví a aplikace, jako jsou doprava, kde se využívá automatizované nebo dálkově ovládané či monitorované procesy (aktiva). Mnoho odborníků v tomto ohledu kritizuje definici dalšího termínu v podobě IACS, který dále rozděluje komunitu a terminologii, a omezuje tak využití případných užitečných standardů i v jiných odvětvích než jen v průmyslu (např. zdravotnictví) [5]. Právě *průmyslová* v tomto ohledu implikuje na omezení aplikační oblasti pouze pro průmyslovou oblast. Stejně tak z definice uvedené oblasti jako *další průmyslová odvětví*. Nicméně v tomto kontextu je nejspíše myšlen obecný *průmysl*, čemuž by odpovídal i fakt ve využívání termínu IACS vůči informačním technologiím (IT, Information Technology) jako antonymum. Tedy velmi obdobně jako je tomu u zažitých antonym IT a OT. Právě díky tomu je mnohdy OT a IACS zaměňováno či považováno za synonyma, alespoň v některých aplikačních odvětví. To však terminologicky není zcela správně.

OT se odkazují na historický pojem, který zahrnuje široké spektrum technologií, systémů a infrastruktur zaměřených na jakoukoliv činnost v rámci průmyslových procesů, a to jak v oblasti hardwaru, tak i softwaru. Hlavním účelem OT je tedy zajistit spolehlivý provoz těchto průmyslových procesů včetně veškerých jeho funkcionalit. Na druhé straně, IACS je pojem, který byl nově definován v normě IEC 62443, a který se primárně zaměřuje na kybernetickou bezpečnost v automatizačních systémech. IACS tak má mnohem specifičtější zaměření než široký pojem OT a lze ho tedy z principu považovat za podmnožinu OT. ICS je pak často zaměňováno s IACS/OT, ale ve skutečnosti se jedná o specifický typ průmyslového systému, který se zaměřuje pouze na řízení a monitorování průmyslových procesů. Systémy automatizace a řízení budov, které se nezabývají přímo průmyslovými procesy, nejsou zahrnovány do kategorie ICS, ale spadají do širší kategorie OT/IACS. Z tohoto důvodu lze konstatovat, že ICS je podmnožinou OT.

2.2 Hlavní komponenty OT

Přejděme nyní na hlavní komponenty OT systémů. Na obrázku níže (obr. 2.1) můžeme vidět obecnou ukázku OT systému z pohledu jeho komponent a základního logického propojení.



Obr. 2.1: Obecný model s komponentami OT [9].

Jednotlivé části můžeme tedy popsat jako:

- **Proces** je ve smyslu k OT myšlen jako průmyslový proces, např. výrobní proces, technologický proces nebo proces řízení budov. Tyto procesy se skládají z několika kroků a mají určité cíle, kterých je třeba dosáhnout. Proces se řídí a monitoruje prostřednictvím dalších komponent, jako jsou aktuátory, senzory, kontroléry, rozhraní člověk-stroj (Human Machine Interface, HMI), či blok vzdálené diagnostiky a údržby. Tyto komponenty pomáhají zajistit, aby byl proces řízen správně, a aby se dosáhlo požadovaných výsledků. Může to být například proces v rámci výrobní linky, nebo chladícího systému.
- **Senzor** je zařízení, které měří určité fyzikální veličiny (např. rychlost, teplotu, průtok) a převádí je na signál, který může být snadno interpretován. Tyto signály pak poskytují informace o stavu procesu, který se sleduje. Senzor funguje tak, že reaguje na určitou vstupní veličinu a generuje výstupní signál, který je funkčně související s touto veličinou. Tyto informace se poté přenášejí do kontroléru, který je využije k řízení procesu. Jedná se tedy např. o teploměr, průtokoměr apod.
- **Aktuátor** (akční člen) je zařízení, které slouží k realizaci změny výstupního stavu na základě vstupního signálu ze řídicího systému (přenosu povelu z kontroléru na řízený proces). Tyto signály mohou být buď manuální, nebo automatické. Zjednodušeně aktuátory tedy slouží k pohybu či řízení mechanismu (systému) a je to právě ten mechanismus, jímž řídicí systém ovlivňuje dané

prostředí. Aktuátory pro svoji funkcionalitu využívají zdroj energie (obvykle elektrický proud, hydraulický tlak nebo pneumatický tlak) a přeměňují tuto energii na pohyb. Například v průmyslových procesech se aktuátor může používat k řízení teploty, tlaku nebo polohy. V závislosti na aplikaci se mohou aktuátory lišit v konstrukci, velikosti a typu použité energie. Tyto rozdíly ovlivňují jejich účinnost a účel použití v konkrétní aplikaci. Může se jednat např. o motor nebo ventil.

- **Kontrolér** je zařízení nebo program, který automaticky reguluje řízenou veličinu, resp. slouží k automatizaci a řízení procesu. Může to být jednoduchý mechanický nebo elektronický systém, softwarově založený, jako například ovladač tiskárny, nebo hardwarový, jako např. řídicí systém robota. Kontrolér může být například počítač nebo programovatelný logický kontrolér (Programmable Logic Controller, PLC).
- **HMI** je grafické uživatelské rozhraní, které umožňuje operátorům monitorovat stav procesů, měnit nastavení řízení a ručně přepínat automatické řízení v případě nouze. HMI také umožňuje inženýrovi nebo operátorovi konfigurovat bod nastavení nebo algoritmy a parametry řízení v kontroléru. Zobrazuje také informace o stavu procesu, historické informace, zprávy a další informace pro operátory, administrátory, manažery, partnery a jiné oprávněné uživatele. Operátoři a inženýři používají HMI k monitorování a konfiguraci bodů nastavení, algoritmů řízení, odesílání příkazů a úpravě a určení parametrů v kontroléru. Jednat se může např. o dotykový displej na průmyslovém počítači, fyzické panely s tlačítky a indikačními světly, ale i např. mobilní či webové aplikace.
- **Vzdálená diagnostika a údržba** spojuje činnosti, které umožňují provádět diagnostiku a údržbu systému, a to zvenčí bezpečnostního perimetru tohoto systému, většinou převážně prostřednictvím internetu nebo jiných sítí. Tyto funkce usnadňují správu a kontrolu systému na dálku, což může šetřit čas a zdroje. Navíc umožňují včasnou identifikaci a řešení problémů, což zvyšuje spolehlivost a funkčnost systému. Tyto funkce také umožňují vzdálenou údržbu a opravy bez nutnosti fyzického přístupu, což může být výhodné v situacích, kdy není možné přístup k systému fyzicky zajistit v daný moment. Příklad může být pouhý vzdálený přístup k PLC nebo složitější jako např. systém dispečerského řízení a sběru dat (Supervisory Control and Data Acquisition, SCADA) či distribuovaný řídicí systém (Distributed Control System, DCS).

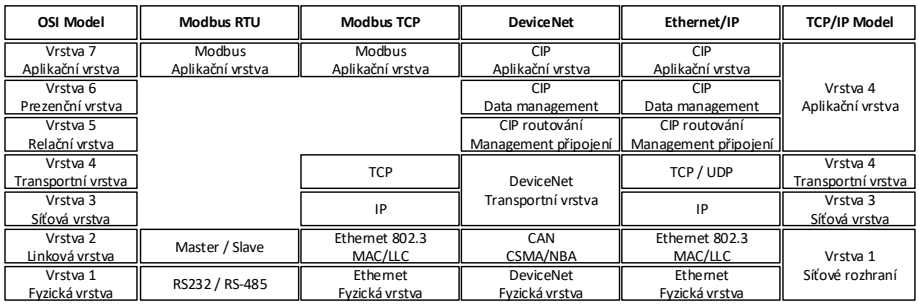
2.3 Komunikační techniky a technologie v OT

Většina průmyslových komunikačních protokolů není přímo založena ani na sedmivrstvém modelu ISO/OSI, ani na čtyřvrstvém modelu TCP/IP. Místo toho mají často svůj vlastní komunikační model a architekturu protokolu navrženou speciálně pro potřeby průmyslových automatizačních a řídicích systémů. Zatímco koncepty a principy modelů ISO/OSI a TCP/IP mohou být v těchto protokolech přítomny, jsou obvykle implementovány přizpůsobenějším a optimalizovaným způsobem, který bere v úvahu specifické požadavky průmyslových sítí, jako jsou data v reálném čase, přenos, determinismus a spolehlivost. Například mnoho průmyslových komunikačních protokolů používá zjednodušenou nebo upravenou verzi vrstvy datového spojení a fyzické vrstvy z modelu ISO/OSI a nemusí zahrnovat vyšší vrstvy, jako jsou vrstvy relace, prezentace a aplikace. To pomáhá snížit režii a zajistit rychlou a efektivní komunikaci v řídicích systémech v reálném čase. Na obrázku níže můžeme vidět, jak jsou některé průmyslové protokoly vsazeny v rámci modelů ISO/OSI či TCP/IP.

<table>
<tr><th colspan="2">OSI Model</th><th>Protokoly:</th><th colspan="2">TCP/IP Model</th></tr>
<tr><td rowspan="3">Data</td><td>Vrstva 7
Aplikační vrstva</td><td>Modbus, DeviceNet,
Ethernet/IP, ...</td><td rowspan="3">Vrstva 4
Aplikační vrstva</td><td rowspan="3">Data</td></tr>
<tr><td>Vrstva 6
Prezenční vrstva</td><td>Kompresní algoritmy</td></tr>
<tr><td>Vrstva 5
Relační vrstva</td><td>NFS, SQL, SMB, RPC,
P2P, SCP, SDP, SIP, ...</td></tr>
<tr><td>Segmenty</td><td>Vrstva 4
Transportní vrstva</td><td>TCP / UDP</td><td>Vrstva 4
Transportní vrstva</td><td>Segmenty</td></tr>
<tr><td>Pakety</td><td>Vrstva 3
Síťová vrstva</td><td>IP (IPv4, IPv6, ARP,
IGMP, ICMP, ...)</td><td>Vrstva 3
Síťová vrstva</td><td>Pakety</td></tr>
<tr><td>Vrstva 2
Linková vrstva</td><td>Vrstva 2
Linková vrstva</td><td>Ethernet, ...</td><td rowspan="2">Vrstva 1
Síťové rozhraní</td><td rowspan="2">Bity a rámce</td></tr>
<tr><td>Vrstva 1
Fyzická vrstva</td><td>Vrstva 1
Fyzická vrstva</td><td>RS-232, UTP kabely
(CAT5, CAT6), ...</td></tr>
</table>

Obr. 2.2: Ukázka zjednodušeného pohledu na protokoly v rámci průmyslu v kontextu modelů ISO/OSI a TCP/IP [17].

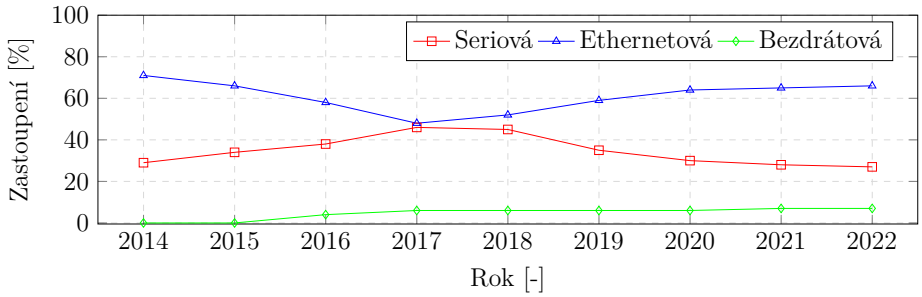
Nicméně situace v rámci průmyslových protokolů nelze vnímat takto zjednodušeně, jednotlivé vrstvy jsou skutečně mnohdy značně odlišné od běžných protokolů v rámci ISO/OSI či TCP/IP. To platí nejen v rámci poslední vrstvy, ale v rámci celé struktury v rámci komunikačního modelu, viz příklad uvedený na obrázku níže pro vybrané (nejběžnější) průmyslové komunikační protokoly, o kterých budeme mluvit blíže také dále (Modbus RTU, Modbus TCP, DeviceNet, Ethernet/IP, EtherCAT a Profinet).



Obr. 2.3: Ukázka podrobného zobrazení vrstev ISO/OSI a TCP/IP vybraných průmyslových protokolů [12].

V kontextu průmyslových sítí se pro přenos dat a komunikaci používají různé techniky. Tyto techniky lze široce rozdělit do různých typů na základě režimu přenosu dat, konektivity, spolehlivosti a duplexního režimu. Hlavní příklady komunikačních technik jsou: proudový a blokový přenos; spojovaný a nespojovaný přenos; spolehlivý a nespolehlivý přenos; simplex, half-duplex a plný-duplex; unicast, anycast, broadcast a multicast. Dále je nutno stanovit si médium pro přenosové technologie. V rámci OT sítí se jedná převážně o tři základní typy: sériová komunikace, ethernetová komunikace a bezdrátová komunikace. Optická komunikace je převážně pak v rámci WAN a GAN sítí, které pro zjednodušení nebudeme v tomto případě uvažovat. **Sériová komunikace** je jednoduchý a starší typ komunikačního protokolu, který používá jednu sériovou linku pro přenos dat. Tyto linky se často používají v průmyslových aplikacích k propojení jednotlivých zařízení a automatizačních systémů. Sériové komunikace mohou využívat různé protokoly, jako například RS-232, RS-485 nebo USB. Tyto protokoly se liší v rámci přenosového rozsahu, rychlosti přenosu a dalších specifických funkcí. **Ethernetová komunikace** je v současnosti nejrozšířenější typ komunikačního protokolu, který se používá v průmyslových aplikacích. Tyto sítě využívají jednoduchých a robustních protokolů, jako je například TCP/IP, které umožňují efektivní komunikaci mezi zařízeními a automatizačními systémy. Ethernetové sítě mohou být propojeny pomocí kabelů, jako jsou například ethernetové kabely kategorie CAT5 či CAT6. **Bezdrátová komunikace** je typ komunikačního protokolu, který umožňuje propojení zařízení a automatizačních systémů bez nutnosti použití kabelů. Tyto sítě využívají různých frekvenčních pásem a protokolů, jako je například Wi-Fi či Zigbee. Bezdrátové sítě se často používají v průmyslových aplikacích k propojení zařízení v obtížně přístupných nebo mobilních prostředích. Vývoj v čase v rámci zastoupení těchto sítí, viz obrázek 2.4, zdroj statistických dat je společnost Hardware meet Software Network[1].

[1]https://www.hms-networks.com/



Obr. 2.4: Vývoj v rámci zastoupení jednotlivých typů médií v průmyslu.

V průmyslových sítích hrají také velmi významnou roli v celkovém návrhu a funkčnosti sítě fyzické i logické topologie. Fyzická topologie se týká fyzického uspořádání sítě a způsobu propojení zařízení. To zahrnuje typ použitého kabelu (jako je měděný nebo optický kabel), typ použitého konektoru a uspořádání zařízení v síti (jako je hvězdicová nebo kruhová konfigurace). Logická topologie se týká způsobu přenosu dat po síti, nezávisle na fyzickém uspořádání. To zahrnuje používané komunikační protokoly, jako je Ethernet, TCP/IP nebo Modbus, a způsob přenosu dat z jednoho zařízení do druhého. Při návrhu průmyslových sítí je třeba pečlivě zvážit jak fyzické, tak logické topologie, protože ovlivňují celkový výkon, spolehlivost a bezpečnost sítě. Z pohledu logické topologie je nutno dále zmínit tři základní techniky, které dnes dopomáhají s realizací logické topologie nad rámec samotných protokolů, a tedy i oddělit skutečnou fyzickou topologii od té logické: Virtualizace síťových funkcí (Network Function Virtualization, NFV), softwarově definované sítě (Software-Defined Networking, SDN) a Cloud computing. Všechny tyto technologie souvisejí s topologií průmyslové sítě, protože mění způsob, jakým jsou sítě navrhovány, nasazovány a spravovány. Cílem těchto technologií je zjednodušit síťové operace a učinit je flexibilnějšími a škálovatelnějšími. NFV umožňuje síťovým funkcím, jako jsou brány firewall, směrovače a nástroje pro vyrovnávání zátěže, běžet na virtuálních počítačích namísto na fyzických zařízeních. To umožňuje nasadit a spravovat síťové funkce jako software namísto vyhrazeného hardwaru, což může zvýšit efektivitu a snížit náklady. SDN na druhé straně odděluje řídicí rovinu od datové roviny v síti. Řídicí rovina, která je zodpovědná za rozhodování o síťovém provozu, běží na centralizovaném řadiči, zatímco datová rovina, která se stará o předávání paketů, běží na přepínačích. Toto oddělení odpovědností umožňuje automatizovat mnoho síťových operací, jako je dopravní inženýrství a prosazování bezpečnostní politiky, což může zjednodušit správu sítě a snížit prostoje. Cloud computing je mezitím model poskytování služeb IT, ve kterém jsou zdroje poskytovány přes internet na základě platby za použití. To může zahrnovat infrastrukturu jako službu (IaaS), platformu jako službu (PaaS),

software jako službu (SaaS) a zařízení jako službu (DaaS). Díky využití cloud computingu mohou průmyslové sítě získat přístup ke škálovatelným výpočetním zdrojům na vyžádání, aniž by musely investovat a udržovat vlastní infrastrukturu. Z pohledu architektury topologie pak rozdělujeme v průmyslových sítích nejčastěji topologii: sběrnicovou, hvězdicovou, kruhovou, stromovou, propojenou (MESH) a hybridní.

V neposlední řadě je také důležité rozlišovat sítě v rámci jejich rozsahu a geografického rozložení v průmyslových aplikacích, protože každý typ sítě má své specifické vlastnosti a výhody/nevýhody v závislosti na svém rozsahu a geografickém rozložení. Rozlišování těchto sítí v průmyslových aplikacích umožňuje správně volit síť pro konkrétní účely a zajistit, že bude mít dostatečný výkon a bezpečnost pro danou aplikaci. Tyto sítě také ovlivňují, jak budou zařízení komunikovat, a jak bude možné provádět vzdálenou diagnostiku a údržbu. Výběr správné sítě je tedy klíčový pro úspěšnou implementaci průmyslových aplikací. Dnes již existuje značné množství typů sítí dle rozlohy, hlavními zástupci jsou:

- **Nano sítě.** ($\approx$ stovky nm, okolí nanozařízení) jsou sítě, které se vyskytují v okolí nanozařízení.
- **Komunikace v blízkém poli** (Near Field Communication, NFC) ($\approx$ desítky cm, okolí zařízení) je typ sítě, která se používá k blízkému komunikačnímu styku mezi zařízeními v okolí zařízení, tj. v rozmezí asi 10 cm.
- **Síť v blízkosti těla** (Body Area Network, BAN) ($\approx$ jednotky m, okolí těla) jsou sítě, která se vyskytují v okolí lidského těla a používají se k přenosu dat mezi zařízeními, která jsou připojena k tělu.
- **Osobní síť** (Personal Area Network, PAN) ($\approx$ <10 m, pracovní místo) je typ sítě, který se obvykle používá k propojení zařízení v blízkosti jednoho uživatele, jako jsou například chytré telefony, tablety, počítače a další zařízení.
- **Domácí síť** (Home Area Network, HAN) ($\approx$ desítky m, domácnost) se často používá pro komunikaci mezi zařízeními v domácnosti, jako jsou počítače, telefony, televize, hračky a chytrá domácí zařízení.
- **Lokální síť** (Local Area Network, LAN) ($\approx$ stovky m, budova) je typ sítě, který slouží k propojení počítačů a dalších zařízení v jedné lokalitě, jako je budova, kancelář nebo škola.
- **Kampus síť (Campus Area Network, CAN)** ($\approx$ jednotky km, kampus) jsou sítě, které se obvykle používají pro propojení různých budov na stejném areálu, jako je například univerzita nebo výrobní kampus.
- **Metropolitní síť** (Metropolitan Area Network, MAN) ($\approx$ desítky km, město) jsou určeny pro komunikaci mezi různými lokálními sítěmi a sítěmi většího rozsahu, jako jsou rozlehlé sítě (WAN).
- **Rozlehlé sítě** (Wide Area Network, WAN) ($\approx$ stovky km, kampus) jsou určeny pro široké geografické oblasti.

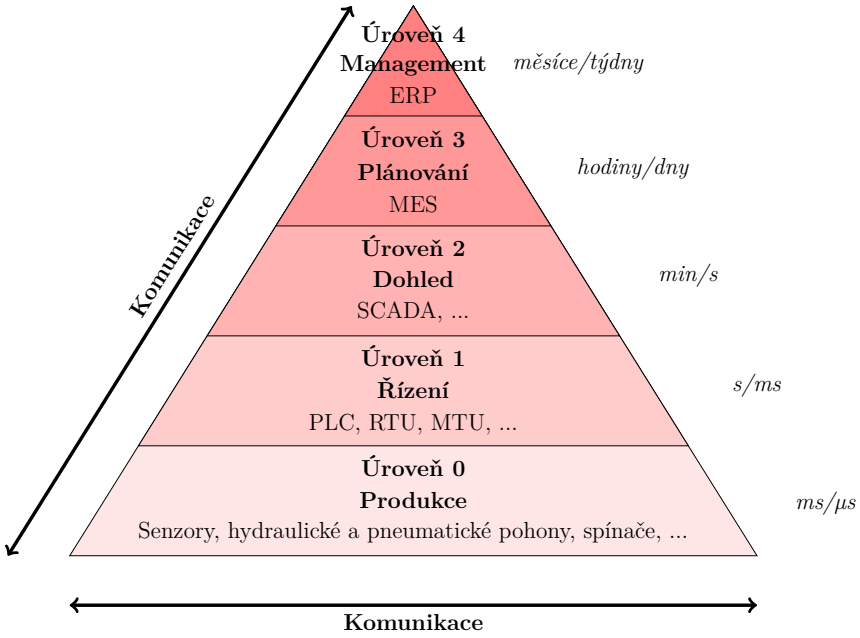
2.4 Architektura OT

V rámci OT, architektura označuje celkový návrh a strukturu systémů používaných k řízení a monitorování fyzických procesů. Efektivní OT architektura je zásadní pro zajištění spolehlivého a bezpečného provozu průmyslových procesů a zároveň podporuje obchodní cíle, jako je efektivita, produktivita a bezpečnost. Architektura OT zahrnuje integraci různých komponent, včetně hardwaru, softwaru a komunikačních systémů, stejně jako organizační a provozní procesy, které tyto komponenty podporují. Architektura musí být navržena tak, aby splňovala specifické potřeby a požadavky organizace s přihlédnutím k faktorům, jako je velikost a složitost systému, typ řízených procesů a požadovaná úroveň zabezpečení a bezpečnosti. Aktuálně neexistuje žádný univerzální přístup k architektuře OT, který by se dal popsat jako tzv. "one-fits-all"řešení. Architektura, která je nejvhodnější pro konkrétní organizaci, bude záviset na řadě faktorů, včetně konkrétních řízených procesů, velikosti a složitosti systému, regulačních požadavků a požadavků na dodržování předpisů a obchodních cílů organizace. Jedním z přístupů k architektuře OT, který si získal široké přijetí, je použití vrstvené architektury, která může poskytnout rámec pro organizaci různých součástí systému OT. Tento přístup obvykle zahrnuje rozdělení systému do několika vrstev, z nichž každá má specifickou sadu funkcí a odpovědností. Přesný počet a složení vrstev se může lišit v závislosti na konkrétních potřebách organizace, ale některé běžné vrstvy v architektuře OT mohou zahrnovat následující:

- **Fyzická vrstva**, která zahrnuje senzory, akční členy a další fyzické komponenty, které se používají k řízení a monitorování fyzických procesů.
- **Řídicí vrstva**, která zahrnuje řadiče a další zařízení, která se používají ke správě fyzických komponent a zajišťují, že fungují v rámci specifikovaných parametrů.
- **Dohledová vrstva**, která zahrnuje rozhraní člověk-stroj (HMI) a další softwarové nástroje používané k monitorování a řízení systému a také k poskytování dat a analýz nadřízenému managementu.
- **Podniková vrstva**, která zahrnuje obchodní systémy a procesy, které se používají k řízení organizace jako celku, a může zahrnovat funkce, jako je řízení zásob, logistika a řízení dodavatelského řetězce.

Tento vrstvený přístup může poskytnout užitečný rámec pro organizaci různých součástí OT systému a zajištění jejich efektivní spolupráce. Je však důležité mít na paměti, že přesné složení a struktura každé vrstvy bude záviset na konkrétních potřebách a požadavcích organizace a může být nutné ji odpovídajícím způsobem upravit. I přesto, že tedy neexistuje jeden model, který by byl vhodný pro všechny případy, byl výše uvedený vrstvený model tedy přijat širokou škálou odborníků, protože z něj lze čerpat jak hierarchické složení, tak síťové složení atd. Z tohoto

důvodu vznikly tzv. referenční modely, kde jedním z nich je např. model popsaný v rámci standardu ANSI/ISA-95. Jedná se o pyramidové schéma jednotlivých úrovní automatizace, které je zobrazeno na obr. 2.5. V rámci jednotlivých úrovní probíhá jak horizontální, tak i vertikální obousměrná komunikace. V rámci obrázku jsou také zobrazeny jednotlivé příklady zařízení i účelu jednotlivých úrovní, kde v neposlední řadě můžeme také vidět časovou náročnost procesů v jednotlivých úrovních.



Obr. 2.5: Pyramidové referenční schéma automatizačních úrovní dle ANSI/ISA-95.

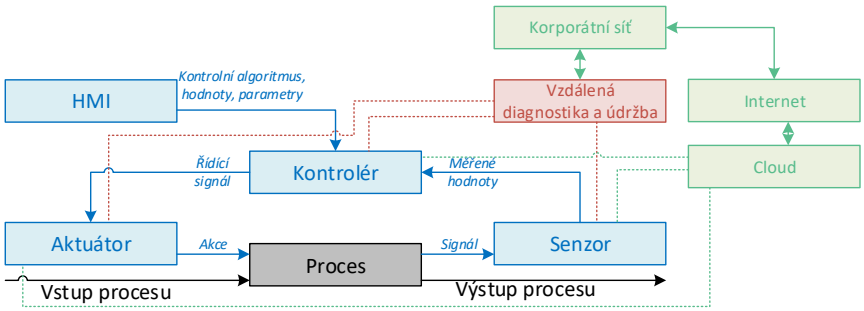
Referenční model je tak rozdělen do pěti úrovní:

- **Úroveň 4 Management** (Management level). Jedná se o úroveň, kde jsou integrovány systémy plánování podnikových zdrojů (ERP, Enterprise Resource Planning). Na této úrovni shromažďuje vysoký management data, analyzuje je a reaguje na vzniklé potřeby společnosti. Jedná se obvykle o sadu různých počítačových softwarových aplikací, které dovolují vnitřní pohledu do fungování společnosti do nejmenších detailů a dovoluje tedy sledování od výroby po prodej, nákup, financování, výplaty, efektivitu, produktivitu a další. Tato úroveň tak dovoluje vrcholovému managementu transparentnost chodu společnosti.
- **Úroveň 3 Plánování** (Planning level). Jedná se o úroveň, která integruje systémy jako řízení specializované expedice (Just-In-Sequence, JIS – Just-In-Time, JIT – Transportation Management Systems, TMS), řízení intralogistiky (Warehouse Management System, WMS), řízení výroby (Manufacturing

Execution System, MES), řízení kvality (Quality Management System, QMS), řízení údržby (Enterprise Asset Management, EAM) a pokročilé plánování (Advanced Planning and Scheduling, APS) či řízení provozu (MOM, Manufacturing Operation Management). Jedná se o úroveň monitorující celý výrobní proces v dané společnosti od surovin až po hotový produkt. To umožňuje managementu přijímat rozhodnutí na základě těchto informací jako např. upravovat stavy objednávek surovin či přepravení plány. Vše tedy na základě skutečných dat získaných z úrovní níže.

- **Úroveň 2 Dohled** (Supervisory level). Tato úroveň zahrnuje systémy vzdáleného i lokálního dohledu, příkladem může být systémy pro SCADA či distribuované řídicí systémy (Distributed Control System, DCS), které jsou určeny k centrálnímu řízení více systému z jednoho bodu, může se např. jednat o dohledové centrum nad přenosovou sítí zahrnující jednotlivé trafostanice, může se jednat o jednotlivé čističky vody apod. Je nutno zde rozlišovat HMI, které je spíše na lokální úrovni níže. Tato úroveň skutečně slouží pro centrální řízení více systémů dohromady, tak aby mohl být dán větší kontext jednotlivým procesům.
- **Úroveň 1 – Řízení** (Control level). Jedná se o úroveň zahrnující lokální HMI, PLC, MTU, RTU a další zařízení, které mají za účel řídit jednotlivé fyzické prvky úrovně 0, tedy zařízení vykonávající již skutečné fyzické úkony.
- **Úroveň 0 – Produkce** (Field level). Tato nejnižší úroveň obsahuje jednotlivé prvky, které již vykonávají fyzické úkony na základě signálů řízení z vyšších úrovní. Jedná se o akční členy, senzory, motory, hydraulické a pneumatické jednotky, různé spínače a další.

Tento model již částečné zahrnuje i IT systémy, kde pro úpravu např. našeho představeného modelu OT bychom mohli tento model jednoduše upravit jako na obr. níže, který by pak lépe odpovídal aktuální situaci.



Obr. 2.6: Aktualizované schéma OT modelu o IT součásti.

3 Případové studie a demonstrace

Tato část ukazuje praktickou aplikaci teorií a konceptů diskutovaných v předchozích částech. Hlavním cílem je ukázat, jak se komponenty OT sítí, komunikační techniky a technologie a architektura OT sítí spojují ve scénářích reálného světa. Sekce je rozdělena do tří podsekcí, z nichž každá představuje demonstraci navrženou v laboratoři pro konkrétní odvětví:

- První sekce zdůrazňuje použití OT v případu balicí výrobní linky a ukazuje integraci různých komponent, jako jsou procesy, senzory, akční členy, ovladače, HMI a vzdálená diagnostika, aby se vytvořil účinný a efektivnější výrobní proces.
- Druhá sekce se zaměřuje na aplikaci OT v městské čistírně vody, přičemž zdůrazňuje význam komunikačních a přenosových technologií, topologií a referenčních modelů pro zajištění efektivního a bezpečného provozu procesu úpravy vody.
- Třetí sekce představuje ukázku použití OT v pivovaru, ukazuje integraci IT/OT v chemickém/potravinářském průmyslu. Ukázka zdůrazňuje důležitost konvergence IT/OT a roli referenčních modelů při vytváření efektivního výrobního procesu.

Každá sekce je rozdělena na shrnutí, použité komponenty, vstupní kritéria (včetně předpokladů, vývoje a návrhu), technický popis, testování a verifikace. Celkově tato kapitola poskytuje komplexní a praktický přístup k pochopení aplikace OT ve scénářích reálného světa. Je nutno zmínit, že tyto demonstrátory byly vytvořeny v rámci výzkumné činnosti pro projekt reg. č. FV40366 [APro11] (Datový monitoring pro zvýšení spolehlivosti procesů chytrých továren), podpořený Ministerstvem průmyslu a obchodu České republiky. Jedná se o komplexní průmyslový testovací polygon, který umožňuje edukaci, testování a výzkum nových moderních průmyslových řešení, a to jak v rámci řešení otázek interoperability, tak i otázek bezpečnosti či potřeb generování datových sad pro umělou inteligenci, které dnes představují hlavní překážku v budování efektivních algoritmů. Samotný polygon byl dále také komercializován, a to prostřednictvím firmy GreyCortex s.r.o. a firmy Vodafone Czech Republic a.s. Polygony i jeho data byly využity v rámci prestižních publikací ve vlastních impaktovaných časopisech a mezinárodních konferencích, ale také ve studentských soutěžních příspěvcích (vytvořených pod vedením autora). Výuka v rámci vytvořených prostředí pak navazuje pomocí kybernetické arény (BUTCA) přes výukové scénáře (v oboru Informační bezpečnosti) a dále také prostřednictvím bakalářských, diplomových a doktorských prací. Bližší popis pro přínos těchto výsledků byl již představen v předchozích kapitolách, viz mj. příslušná kap. *Přínos práce*.

3.1 Příklad I: Průmyslová balicí smyčka

3.1.1 Vstupní předpoklady

Bezpečnostní incidenty jsou v rámci průmyslových zařízení stále více časté. To je způsobeno zejména propojením IT (Information Technology) a OT (Operational Technology) infrastruktur. Toto propojení přispělo nejen k snazší dosažitelnosti těchto sítí a možnému propojení k jiným OT infrastrukturám skrze IT sítě, ale vystavilo také OT sítě útokům vyskytujícím se v IT sítích. Aby bylo možné zajistit vyšší úroveň bezpečnosti, je nutné kombinovat nejnovější technologie a přístupy. K umožnění tohoto vývoje je však zapotřebí dat, na základě kterých bude tento výzkum proveden. Pro tyto účely bylo vytvořeno testovací prostředí (testbed) Balicí smyčky. Vytvořená balicí smyčka slouží k vytváření datových sad. Hlavní výhodou vytvořené smyčky je velmi blízké přiblížení vytvořeného pracoviště reálnému prostředí. Další výhodou je vytvoření softwarových verzí, které jsou z pohledu generovaných dat totožné s těmi fyzickými. Účely testovacího prostředí:

- Dlouhodobý sběr dat ze standardního i nestandardního provozu.
- Vytvoření datových sad.
- Průzkum vektorů útoků.
- Simulace kybernetických útoků a anomálií.
- Simulace anomálií na fyzických zařízeních.
- Optimalizace výsledných řešení.

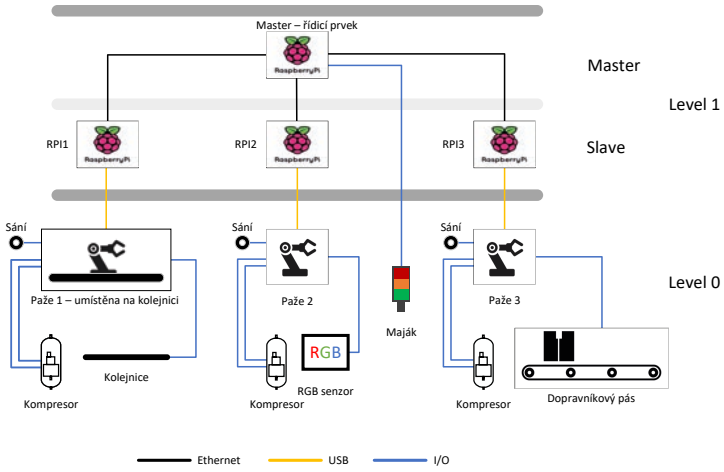
Tabulka 3.1 zobrazuje dále jednotlivé požadavky, které byly stanoveny před začátkem vývoje průmyslového testbedu. Aby bylo možné jednotlivé požadavky zajistit, je nutné brát v úvahu jejich nasazení již při návrhu a vývoji průmyslové smyčky. Mezi nejvíce kritické body je možné zařadit požadavky na zajištění dostatečné přesnosti a opakovatelnosti při zachování stabilního chodu. Je tak nutné brát v úvahu jednotlivé okolní vlivy, které mohou způsobit změnu běhu programu oproti ostatním, jako je například odlišný čas potřebný pro resetování souřadnicového systému robotické paže atp.

Tab. 3.1: Jednotlivé požadavky na vytvářený testbed.

Požadavek na testbed
Využití průmyslového protokolu
Implementace šifrované verze protokolu
Zajištění stabilního chodu
Zajištění přesnosti a opakovatelnosti
Vytvoření virtualizované verze
Možnost grafické vizualizace
Zajištění snadné správy, modifikovatelnosti

3.1.2 Technický popis

Balicí smyčka je sestavena na experimentálním pracovišti sestávající se ze tří zařízení Dobot Magician s využitím průmyslového protokolu Modbus TCP. Pracoviště má za cíl demonstrovat balicí linku využívající dopravníkový pás k předávání *výrobku* na další určenou polohu, kde bude následně zpracován (obsloužen) další robotickou paží (rukou). Logické sestavení experimentálního pracoviště je vyobrazeno na obrázku 3.1. Síťové zapojení lze rozdělit dle Purdue modelu na dva levely. Level 0 obsahuje samotné aktivní prvky ovládané skrze zařízení na vyšší úrovni (jejich chování je plně řízeno skrze slave, resp. master stanici), kromě signalizačního majáku, který je přímo řízen master stanicí. Tento level obsahuje robotické paže a další připojené komponenty, jako RGB senzor a dopravníkový pás. Level 1 lze dále rozdělit na master a slave zařízení, kde komunikace je plně řízena master zařízením a slave zařízení pouze vykonává a monitoruje vykonávané činnosti. Z důvodu simulace PLC bylo využito zařízení RPi, které komunikují průmyslovým protokolem Modbus TCP.

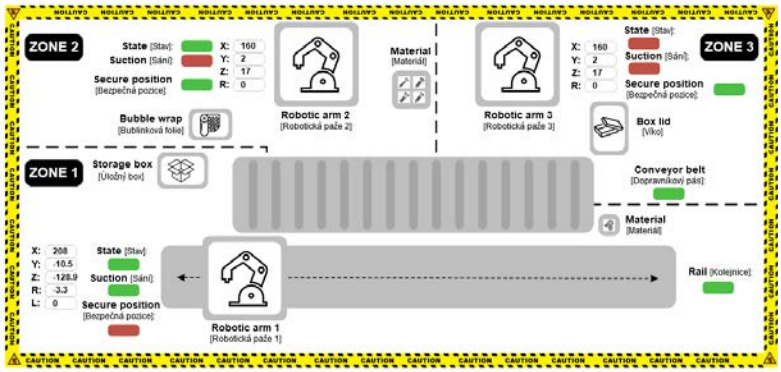


Obr. 3.1: Logická architektura balicí smyčky.

Experimentální pracoviště je složeno ze tří robotických paží. Každá robotická paže má umístěné porty na předloktí a na své základně (jak je zmíněno výše). Každá robotická paže má připojen kompresor v portech *GP1* a *SW1*. Ovládání rotace *přísavky* umístěné na konci robotické paže je připojeno do portu *GP3-port1* na předloktí paže. Robotická paže *1* je dále připevněna ke kolejnici, k tomu jsou využity porty *Communication port* a *Stepper 2*. Robotická paže *2* má připojen RGB senzor do portu *GP2* a robotická paže *3* má připojen dopravníkový pás do portu *GP2*. Fotodokumentace na obrázku 3.2.

Obr. 3.2: Fotodokumentace experimentálního pracoviště (balicí smyčka).

Z důvodu využívání průmyslové komunikace je možné nejen zpracovávat komunikaci v reálném čase, ale také vyčítat jednotlivé paměťové bloky na slave stanici. Zde jsou uloženy jednotlivé parametry, které jsou vyhodnocovány a vykonány slave stanicí. Vyčítání a zobrazování je prováděno pomocí monitorovacího a řídicího softwaru OpenMuc [1]. Obrázek 3.3 zobrazuje vizualizaci skrze tento software. U každé robotické paže jsou zobrazeny její pozice (X, Y, Z, R, L), stav, sání a dosažená pozice. Graficky vizualizován je také stav dopravníkového pásu a kolejnice. Tato provedená vizualizace dále přibližuje vytvořený testbed reálnému nasazení. Je tak možné jej prezentovat, jako případný HMI, který umožňuje nejen zobrazování pozic jednotlivých zařízení, ale také umožňuje zaslání příkazů na jednotlivé stanice.



Obr. 3.3: Vizualizce OpenMUC pro balicí smyčku.

3.1.3 Výsledky z testování a verifikace

Jednotlivé dosažené výsledky z celkového testování jsou zobrazeny v rámci tabulky 3.2. Tabulka zobrazuje hodnoty, které byly předpokládány před začátkem testování. Z tabulky však vyplývá, že zejména v oblasti schopnosti generování dat byl základní požadavek překonán. Za největší přínos tohoto testbedu je možné označit generování rozmanitých dat založených na skutečném procesu získaném na reálných hardwarových zařízeních. Díky vzniku virtualizovaných verzí je možné nejen provádět rozšíření zapojení, ale i provádět navazující výzkum čistě na virtualizovaných verzích. To by však nebylo možné dosáhnout bez základního využití hardwarových prvků. Mezi další navazující výzkum a vývoj lze například označit zpracování vygenerovaných dat pomocí technik strojového učení a neuronových sítí pro účely detekce anomálií, vytváření komunikačních vzorů, vytváření otisků zařízení atp.

Tab. 3.2: Srovnání výsledků testování.

Prvek testování, ověření	Požadavek/předpoklad	Otestováno
Bezpečnost – kontrola	Implementace zabezpečeného protokolu	Implementace zabezpečeného protokolu + bezpečnostních funkcí v rámci kódu
Schopnost generování dat, srovnání dopadů použitého šifrování	1 MB/jeden cyklus	2,2 MB (nešifrovaná verze, 3 paže) 5,1 MB (šifrovaná verze, 3 paže)
Testování doby RTT	0,2 s	0,1008 s (medián)
Parametr čekání – měření rozdílu	1 s (jedno kolo)	1,2 s (jedno kolo, medián)
Určení úzkého hrdla, dopad na šířku pásma při deaktivovaném parametru čekání	0,4 Mb/s	0,2 Mb/s

Tabulka 3.3 pa již zobrazuje kontrolu dodržení jednotlivých požadavků na průmyslovou balicí smyčku před zahájením vývoje. Veškeré parametry byly dodrženy. V rámci sloupce poznámky je uvedeno jakým způsobem byl daný požadavek splněn.

Tab. 3.3: Jednotlivé implementované požadavky na vytvořený testbed.

Požadavek na testbed	**Zajištěno**	**Poznámka**
Využití průmyslového protokolu	Ano	Modbus/TCP
Implementace šifrované verze protokolu	Ano	Modbus/TCP Security
Zajištění stabilního chodu	Ano	Využití parametru čekání z pohledu (dobot, skript)
Zajištění přesnosti a opakovatelnosti	Ano	Volbou robotické paže
Vytvoření virtualizované verze	Ano	Bez nutnosti fyzického připojení paží
Možnost grafické vizualizace	Ano	OpenMuc
Zajištění snadné správy, modifikovatelnosti	Ano	Pomocí konfiguračním skriptů

3.2 Příklad II – Čisticka

3.2.1 Vstupní předpoklady

Tento testbed se snaží přiblížit reálné čističce odpadních vod (ČOV), založené na technologii Sequencing Batch Reactor (SBR) to je označení pro nádrž, ve které dochází zároveň k biologickému čištění pomocí provzdušňování, a k separaci vzniklého kalu od vyčištěné vody. Testovací prostředí bylo navrženo dle reálné čistírny odpadních vod, která pracuje v malé obci. Hlavním cílem stavby tohoto testbedu byla možnost sběru procesních dat a síťových dat a především také, jak bylo výše zmíněno generování nestandardního provozu pro vytváření datasetů. Zvolili jsme čistírnu odpadních vod, protože stále více čistíren (pro domácnosti, firmy, obce nebo větší oblasti) je řízeno a monitorováno na dálku pomocí systémů SCADA. Tento testbed tedy slouží k výzkumu kybernetické bezpečnosti a možných vektorů útoků v této oblasti. Primárním cílem je pro nás sběr procesních dat, výzkum kybernetické bezpečnosti a výzkum v oblasti metod strojového učení pro detekci anomálií v průmyslových sítích. Účely testbedu:

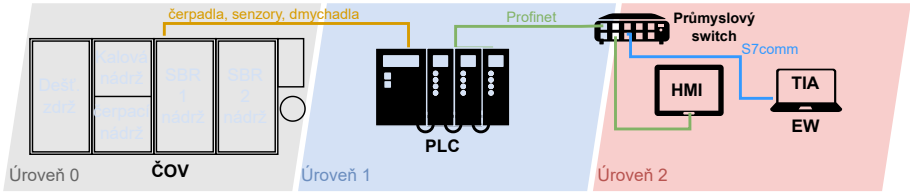
- Dlouhodobý sběr procesních i komunikačních dat z testbedu.
- Sběr dat z nestandardního provozu.
- Průzkum možných vektorů útoků.
- Demonstrace anomálií na fyzických zařízeních.
- Testování detekčních nástrojů.
- Výzkum v oblasti detekčních metod anomálií v průmyslových sítích.
- Zlepšení kybernetické bezpečnosti v ostrém provozu.
- Optimalizace reálných řešení.

Hlavním požadavkem je možnost sběru dat průmyslové síťové komunikace. Vzhledem k tomu je cíleno na fyzické testovací prostředí (testbed), který by takové generování dat mohl simulovat. Díky takovému generování dat je možné vytvářet detekční modely anomálií. Proto je důležité mít možnost testovat i nestandardní (anomální) provoz, což by v reálném prostředí nebylo možné. Z tohoto důvodu je třeba vytváření testovacích prostředí. Hlavní požadavky byly tedy:

- Vytvoření fyzického prostředí simulujícího ČOV.
- Komunikace musí obsahovat průmyslový komunikační protokol.
- Umístění fyzických komponent HMI a PLC.
- Možnost grafické vizualizace.
- Testovat nestandardní provoz (různé vektory kybernetických útoků).
- Dlouhodobý sběr dat standardní a nestandardní komunikace.
- Vytvořit virtualizované řešení.
- Vytvářet datasety pro detekční nástroje anomálií.

3.2.2 Technický popis

V rámci testbedu je možné detekovat maximální a minimální hladiny v ČOV. Dále je možné využít přečerpávání z nádrží a využít aerace a sedimentace. Je možné simulovat přítok vody a odtok vyčištěné vody. Celý testbed pracuje v cyklu samostatně, ale je možné do něj zasahovat a upravovat provoz tak jako v reálných čističkách. V rámci procesu je simulován přítok vody do čerpací stanice, dále přítok vody do dešťové zdrže a přečerpávání do čerpací stanice. Je zde simulován také proces aerace a sedimentace, tedy čištění vody pomocí dvou nádrží SBR. Celkově může být testbed ovládán pomocí HMI kde lze vypustit celou ČOV, popřípadě měnit parametry aerace a sedimentace nebo sledovat vizualizované hladiny vody. Na obrázku 3.4 je uvedeno obecné schéma testbedu ČOV, které je rozděleno dle průmyslové pyramidy (purdue modelu ANSI/ISA-99). Na úrovni 0 je fyzická ČOV. Fungují zde jednotlivá čerpadla nezbytná pro provoz čistírny, následují snímače hladiny, snímače kalu, snímače čerpání, snímače dešťové vody a dmychadla. Na úrovni 1 pracuje PLC od společnosti Siemens, které řídí celý proces čištění odpadních vod. Na vrstvě 2 pracuje inženýrské pracoviště, z něhož lze upravovat program ČOV nebo dohlížet na její provoz. Na této vrstvě je také HMI, které umožňuje obsluze ovládat jednotlivé procesy ČOV a je určeno také pro vizualizaci současného stavu. Jednotlivé komponenty propojuje průmyslový přepínač.

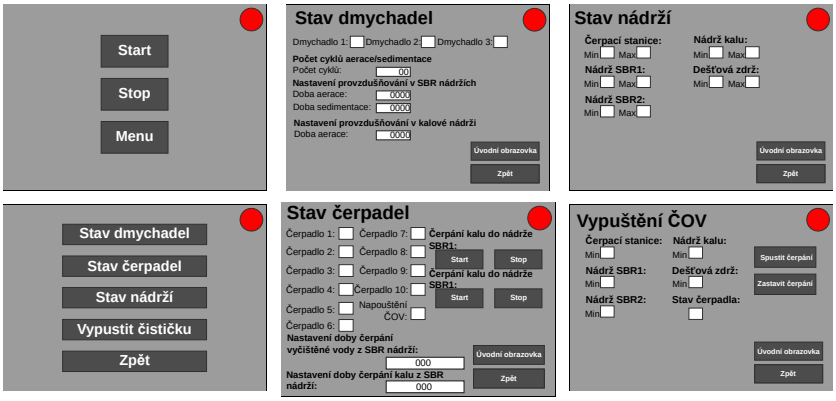


Obr. 3.4: Logická architektura ČOV.

Hlavním řídicím prvkem celé komunikace je PLC S7-300 (6ES7314-6EH04-0AB0) od firmy Siemens, které řídí provoz celého testbedu. Jako digitální vstupy jsou zde 5x plovákové senzory pro detekci maximální hladiny, 5x bezkontaktní senzory pro detekci minimální hladiny, Bezpečnostní tlačítko a tlačítko přítoku vody. Jako digitální výstupy jsou zde 11x čerpadla, 3x dmychadla a dioda indikace přítoku vody. Dále PLC komunikuje s HMI a inženýrskou stanicí, na které běží TIA portal pomocí rozhraní profinet a přímo pomocí proprietárního protokolu firmy Siemenes S7comm. Pro komunikaci v rámci SCADA systému OpenMUC je použit taktéž protokol S7comm. Na obrázku 3.5 lze vidět vzhled testovacího prostředí.

Obr. 3.5: Fotodokumentace experimentálního pracoviště (ČOV).

V rámci testovacího prostředí jsou dvě možnosti vizualizace. Prvním z nich je fyzické rozhraní člověk-stroj tedy HMI od firmy Siemens KTP-700 Basic. Pro toto HMI bylo nakonfigurováno několik obrazovek, kde jsou vizualizovány jednotlivé procesní prvky ČOV. Díky tomu lze na HMI tyto prvky sledovat a ovládat (senzory, čerpadla apod.). Pro tento testbed bylo vytvořeno šest obrazovek. Druhou možností je využití softwaru SCADA softwaru OpenMUC, který byl vytvořen speciálně pro polygon na VUT a jsou do něj zapojeny jednotlivá testovací prostředí. Grafická stránka je naprosto totožná s vizualizací na fyzickém HMI a tedy v rámci SCADA řešení je taktéž šest obrazovek, viz ukázka níže.



Obr. 3.6: Vizualizce OpenMUC pro ČOV.

3.2.3 Výsledky z testování a verifikace

V rámci testování bylo provedeno několik testovacích protokolů, které měly za účel ověřit finální vlastnosti testbedu. Jednalo se především o: generování dat standardního provozu (kvantifikovat možnosti generování a sběru dat), bezpečnostní cvičení (sběr dat standardního a nestandardního provozu), testování útoku na *ostrém* provozu (demonstrace útoku a možnost sběru dat z útoku). Všechny tyto testy proběhly úspěšně a demonstrovali možnosti testbedu, shrnutí dosažených výsledků, viz tabulka 3.4, kde lze vidět testované typy nestandardního provozu pro generování dat.

Tab. 3.4: Testované typy nestandardního provozu pro generování dat.

Typ anomálie	**Otestováno**
Útoky pomocí skriptů	Ano
Útoky pomocí externích aplikací	Ano
Získávání informací o zařízení pomocí externích aplikací	Ano
Získání programu PLC	Ano
Skenování v průmyslové síti a dopad skenování	Ano
DoS útoky na průmyslová zařízení	Ano

V tabulce 3.5 je pak již souhrn splněných požadavků pro vývoj testovacího prostředí ČOV. Všechny požadavky pro dané řešení byly splněny.

Tab. 3.5: Požadavky na testovací prostředí.

Požadavky na testovací prostředí	**Zajištěno**	**Poznámka**
Vytvoření fyzického prostředí simulujícího ČOV	Ano	
Komunikace musí obsahovat průmyslový komunikační protokol	Ano	S7comm protokol
Možnost grafické vizualizace	Ano	HMI, OpenMUC (SCADA)
Umístění fyzických komponent HMI a PLC	Ano	HW od firmy Siemens
Možnost testování nestandardního provozu	Ano	Otestovány různé vektory útoků
Virtualizované řešení	Ano	S7comm protokol
Vytváření datasetů	Ano	
Dlouhodobý sběr standardní a nestandardní komunikace	Ano	

3.3 Příklad III – Pivovar

3.3.1 Vstupní předpoklady

Detekce a analýza komunikačních dat je z velké míry závislá na zaznamenaných datech reálné komunikace. Struktura protokolu, jeho komunikační schéma a vzor komunikujícího zařízení je možné získat z dokumentace a virtuální simulací obrazu zařízení. Reálná komunikace je však ovlivněna dalšími faktory, které jsou buď těžko předvídatelné, nebo složitě simulovatelné. Také samotná simulace nestandardních stavů (útoky, nedostupnost zařízení, výpadky energie atd.) je v průmyslové datové komunikaci prakticky nerealizovatelné, jelikož by znamenala snížení produktivity, a tedy i finanční ztrátu pro podnik. Z tohoto důvodu jsou realizovány vývojová testovací prostředí (testbed) blížící se reálným scénářům, na kterých jsou tyto nestandardní stavy simulovány. V tomto dokumentu popsaný fyzický emulátor pivovaru je jedním z nich. V testbedu není cílem simulovat celý proces velkých pivovarů, ale různých stavů, které se při výrobě vyskytují. Díky automatizaci pomocí programovatelných logických automatů (PLC) je možné tyto stavy zpracovávat a přenášet pomocí síťových protokolů do ovládacích jednotek. Analýza této komunikace umožňuje vytvářet vzory, které slouží klasifikaci standardních i nestandardních stavů a procesů. Z výše uvedeného textu lze vyvodit kritéria a předpoklady, které by dané testovací prostředí mělo splňovat, aby adekvátně simulovalo reálné provoz. Předpoklady pro fyzickou realizaci testovacího prostředí:

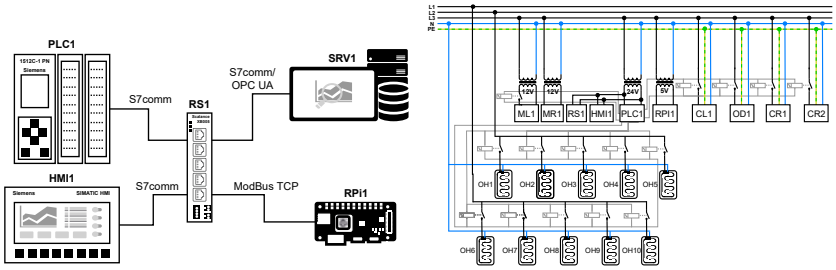
- PLC komunikující průmyslovým protokolem.
  - V rámci průmyslu jsou jedněmi z nejvyužívanějšími aplikační protokoly (ModbusTCP, Profinet, OPC UA, EthernetIP a S7comm).
- Další síťové prvky vyskytující se průmyslové komunikaci.
  - Pro lokální ovládání zařízení a vizualizaci se v průmyslu využívají HMI, které je k PLC připojeno buď přes sériovou komunikaci nebo pomocí jednoho z výše uvedených síťových protokolů. Pro vzdálený přístup a dohled slouží rozhraní SCADA, které je stejně jako HMI připojeno pomocí jednoho ze síťových protokolů.
- Rozhraní a stanice pro záznam a analýzu síťového provozu.
- Fyzické prvky jako jsou přepínače, ventily, senzory atd. nacházející se v reálném procesu pro výrobu piva.
- Úložiště pro dlouhodobý sběr dat.

Požadavky a předpoklady na datovou část testbedu:

- Záznam standardní i nestandardní komunikace.
- Analýza komunikace a klasifikace standardní komunikace i nestandardní.

3.3.2 Technický popis

Za účelem výzkumné činnosti bylo realizováno emulační vývojové prostředí (testbed) pro simulace a testování procesu v potravinářském průmyslu je založeno na konceptu automatizované procesu výroby piva. Komunikace v rámci testbedu je rozdělena na datovou a signálovou. Datová komunikace probíhá mezi zařízení PLC, HMI1, SRV1 a RPi1 propojené pomocí průmyslového Ethernetu přes síťový přepínač RS1 (viz obrázek 3.7). Napájení vývojového testbedu zajišťuje třífázová přípojka 400V/16A. Fáze L1 a L2 slouží pro připojení tištěných topných desek (OH1-OH10), které ohřívají nádoby VN1 a VN2. Poslední fáze L3 napájí zbylá zařízení na přímo nebo přes některý z transformátorů. Některé prvky mají také přeřazený relé modul řízený z PLC jednotky, aby je bylo možné spínat v požadované fázi procesu výroby (viz obrázek 3.7).

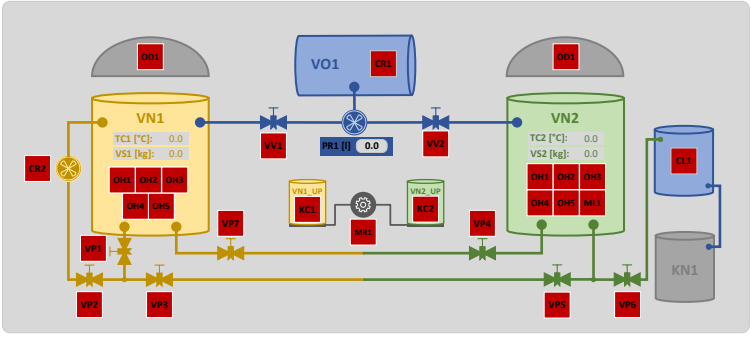


Obr. 3.7: Komunikační schéma (vlevo) a elektrické schéma napájení (vpravo).

Data jsou přenášena pomocí tří hlavních protokolů. První protokol S7comm zajišťuje výměnu dat mezi zařízeními PLC1, HMI1 a SCADA (SRV1) OpenMUC. Tento protokol je nativně používán u průmyslových zařízení společnosti Siemens, pod kterou spadají i obě zařízení. Druhým protokolem je Modbus TCP, který je implementován do jednodeskového počítače Raspberry Pi Zero W (RPi1). Na tento počítač jsou připojeny dva senzory teploty TC1 a TC2. Pomocí protokolu Modbus jsou následně přenášeny do PLC1 a SVR1. Třetí protokol OPC UA slouží pro komunikaci se vzdáleným dohledovým centrem SCADA OpenMUC. Tento protokol byl zvolen pro jeho podpory ze strany PLC1, poměrně velkému zastoupení na trhu a modulárnosti z pohledu objektové strukturalizace dat. Signálová komunikace je zprostředkována mezi koncovými prvky (senzory, ventily, přepínači) a vstupně výstupním rozhraním PLC1 jednotky. Fotodokumentace je na obrázku 3.8

Obr. 3.8: Fotodokumentace experimentálního pracoviště (balicí smyčka).

Vizuální zobrazení, které je viditelné operátorovi je uvedeno na obrázku 3.9. Hlavními prvky jsou nádoby VN1, VN2, které slouží k samotnému procesu vaření, doplněné nádobou na vodu VO1. Na tyto nádoby jsou připojeny čerpadla CR1 (čerpání vody do VN1 a VN2), CR2 (přečerpávání ve VN1) a ventily VV1, VV2 (napouštění vody) a VP1 až VP7 (kontrola průtoku mezi VN1 a VN2). Jelikož se jedná o kladkový spádový pivovar, tak motor MR1 zajišťuje změnu poloh nádob s koncovými spínači KC1 a KC2, které signalizují hraniční stav VN1 a VN2. V každé nádobě jsou uvedena snímaná data ze senzorů (TC1, TC2 – teplota, VS1, VS2 – váha), stav topných těles (OH1-OH10), koncový spínač proti přetečení vody (KC3, KC4, KC5) a časomíra (TVN1, TVN2) pro měření cyklů při procesu vaření. Posledními prvky jsou průtokoměr (PR1) pro měření přečerpané vody ze zásobníku VO1, odsávání nečistot a vlhkosti při vařené (OD1), chlazení po ukončení vaření (CL1) a kvasná nádoba (KN1) pro uložení vařeného produktu.



Obr. 3.9: Grafický panel ve SCADA OpenMUC – Hlavní obrazovka.

3.3.3 Výsledky testování

Jedním z klíčových požadavků při návrhu testovacího prostředí Pivovar bylo, aby prostředí mohlo sloužit pro generování, záznam a analýzu síťového provozu průmyslových protokolů. Testování bylo rozděleno na dva testovací protokoly. **Testovací protokol 1** byl proveden za účelem generování, záznamu a analýzy standardního provozu. Během celého procesu bylo zaznamenáno 200 568 paketů, kde 36,8 % bylo protokolu S7comm, 18,4 % Modbus TCP a zbytek byla komunikace síťových protokolu TCP, UDP atd. Po zaokrouhlení jde o 9,28 paketů za sekundu. Z toho je 3,42 paketů pro protokol S7comm a 1,71 pro Modbus. Průměrně mají zprávy velikost 187 bajtů pro S7comm a 173 bajtů pro Modbus TCP. Při standardním provozu testbed generuje přibližné 923 bajtů za sekundu komunikace S7comm a Modbus. **Testovací protokol 2** byl naopak zaměřen na generování, záznam a analýzu nestandardního provozu. Bylo ověřeno, že z pohledu vlivu na proces vaření jsou kritické stanice PLC1 a RPi1, které přímo ovládají některé z koncových prvků; HMI1 a SRV1 jsou klíčové pro spuštění procesu a pro jeho případné ukončení, ale během vaření má jejich případný výpadek minimální dopad na proces; z pohledu komunikace nevnáší výpadky téměř žádnou nadbytečnou komunikaci např. z pohledu opakovaných dotazů (mimo výpadek RPi1). V tabulce 3.6 je pak provedeno shrnutí stanovených požadavků. Veškeré stanovené kritéria a požadavky byly splněny.

Tab. 3.6: Tabulka požadavků a jejich realizace v testovacím prostředí.

Požadavek	Zajištěno	**Realizace v rámci testbedu**
Průmyslový protokol	Ano	S7comm, Modbus TCP.
PLC	Ano	Automatizační jednotka Siemens SIMATIC S7-1500.
HMI	Ano	Rozhraní člověk-stroj Siemens SIMATIC KTP-700.
SCADA	Ano	Open-source softwarové verze OpenMUC.
Datové úložiště	Ano	QNAP NAS s více než 15 TB úložného prostoru.
Fyzické prvky	Ano	El.mag. ventily, relé , senzory – teploty váhy, průtoku.
Záznamové zařízení	Ano	Síťová sonda Profishark 1G, VUT síťová sonda.
Analýza a simulace	Ano	Stolní a rackové počítače se softwarem jako je Kali linux, Debian, Tenzorflow, Wireshark, TIA portál atd.
Virtualizovaná verze	Ano	Virtualizovaná verze s protokolem Modbus.

4 Závěr

Tato práce představila aktuální výzvy a příležitosti, které přináší digitalizace průmyslu i nové trendy jako Průmysl 4.0, IoT, IIoT a další. Jeden z hlavních přínosů práce je ucelená terminologie, která napomáhá k chápaní vývoji celého OT odvětví, spojování jednotlivých odvětví včetně jejich slučování a oddělování, jako např. v případě kybernetické bezpečnosti. Byly také představeny základní normy, předpisy a standardy, které se tykají návrhu a vývoje v prostředí OT. V rámci práce byly dále vysvětleny základní komponenty OT včetně názorných příkladů z praxe včetně jejich možné simulace a matematického popisu. Byly přiblíženy jednotlivé modely komponent i jejich vzájemná návaznost a propojenost. Ucelený přehled tak jasným způsobem ukazuje složitost těchto systémů a nutnost precizního návrhu i samotné implementace. V neposlední řadě tato práce přibližuje výzkum a vývoj v rámci návrhu, implementace, testování, optimalizace i finalizace tří vybraných ukázek - případových studií (průmyslová balicí smyčka, čistička a pivovar). Tyto ukázky názorným způsobem popisují postup od vzniku myšlenky, návrhu funkčních a užitných parametrů až po jejich naplnění. Tímto práce uzavírá komplexní pohledu na dnešní OT svět. Závěrem jsou již uvedeny stručně odpovědi na stanovené stěžejní otázky:

- **Jaké výzvy a příležitosti přináší digitalizace průmyslu?**
  - Digitalizace přináší příležitosti, jako je zvýšení efektivity, produktivity a flexibility ve výrobním procesu. Umožňuje také využití pokročilých technologií, jako je umělá inteligence, analytika velkých dat a internet věcí (IoT). Přináší však také výzvy, jako jsou rizika kybernetické bezpečnosti, potřeba nových dovedností a náklady na implementaci nových technologií. V rámci práce byly všechny kladné i záporné stránky digitalizace blíže vysvětleny.
- **Jak měnící se prostředí ovlivňuje přijetí a implementaci OT?**
  - Měnící se prostředí, jako jsou nové předpisy, technologický pokrok a ekonomické faktory, mohou ovlivnit přijetí a implementaci OT. Společnosti mohou čelit problémům při zavádění nových technologií kvůli starším systémům, nedostatku odborných znalostí nebo odporu vůči změnám. Práce představila aktuální situaci v rámci dnešních OT.
- **Jaká je současná úroveň jednotnosti terminologie používané v rámci OT a jak ji lze standardizovat?**
  - Současná úroveň jednotnosti v terminologii používané v OT se může lišit v závislosti na odvětví a společnosti. Standardizace lze dosáhnout použitím mezinárodních norem a osvědčených postupů, jakož i iniciativ specifických pro odvětví za účelem vytvoření společné terminologie. Nicméně aktuálně chybí celistvá terminologie a značná část odvětví používá a je zvyklá na vlastní metodiku. Práce přiblížila hlavní rozdíly včetně možného ucelení terminologie.

- **Jakou roli hrají normy, předpisy a normy při utváření vývoje a implementace systémů OT?**
  - Normy, předpisy a normy hrají důležitou roli při utváření vývoje a implementace systémů OT. Poskytují pokyny pro návrh, provoz a údržbu systémů OT a také zajišťují interoperabilitu a shodu s právními a bezpečnostními požadavky. Práce představila hlavní standardy, normy a další legislativní nařízení v rámci kontextu s OT.
- **Jaké jsou základní komponenty v rámci OT sítí a jak jsou napojeny na dnešní chápání průmyslových sítí?**
  - Mezi základní komponenty OT sítí patří senzory, akční členy, ovladače a komunikační protokoly. Tyto komponenty jsou vzájemně propojeny a tvoří síť, která umožňuje sběr, zpracování a přenos dat. Dnešní chápání průmyslových sítí zahrnuje pojmy jako interoperabilita, kybernetická bezpečnost a používání standardních komunikačních protokolů. Všechny základní komponenty včetně architektury OT jsou v práci představeny.
- **Jaký je současný stav konvergence IT a OT a jaký je její dopad na průmysl?**
  - Konvergence mezi IT a OT je rostoucí trend v tomto odvětví, kde se hranice mezi těmito dvěma doménami stále více stírají. Tento trend umožňuje větší integraci mezi obchodními systémy a produkčními systémy, stejně jako použití pokročilých technologií ke zlepšení efektivity a produktivity. V rámci práce je konvergence diskutována s názornou ukázkou jednotlivých překážek i přínosů.
- **Jak lze moderní OT technologie, jako je Průmysl 4.0 a IoT, využít k efektivnímu provozu průmyslových sítí?**
  - Moderní OT technologie lze použít k monitorování a řízení průmyslových sítí v reálném čase, sběru a analýze dat a optimalizaci výrobních procesů. Průmysl 4.0 a IoT umožňují využití pokročilých technologií, jako je prediktivní údržba, vzdálené monitorování a strojové učení, ke zlepšení efektivity a snížení prostojů. Práce přibližuje moderní trendy v OT a dává jim kontext v rámci současných průmyslových sítí.
- **Jaké překážky a řešení představuje implementace OT v průmyslových aplikací?**
  - Překážky implementace OT v průmyslových aplikacích zahrnují náklady na implementaci, starší systémy, rizika kybernetické bezpečnosti a potřebu nových dovedností. Mezi řešení těchto překážek patří vytvoření jasného obchodního případu, upřednostnění kybernetické bezpečnosti, investice do školení a vzdělávání a spolupráce se zkušenými partnery. Práce představuje tři vybrané případové studie a ukazuje možnosti od návrhu, přes implementaci až po finalizaci průmyslové aplikace.

Autorovy publikace

[APub1] Benedikt, J.; Vrtal, M.; Fujdiak, R.; aj.: Virtualization platform for urban infrastructure. In *2022 22nd International Scientific Conference on Electric Power Engineering (EPE)*, IEEE, 2022, s. 1–5.

[APub2] Blazek, P.; Fujdiak, R.; Hodon, M.; aj.: Communication Anomaly Detection in Cyber-physical Systems. In *SEIA'2019 Conference Proceedings*, Lulu. com, 2020, str. 311.

[APub3] Blazek, P.; Fujdiak, R.; Mlynek, P.; aj.: Development of cyber-physical security testbed based on IEC 61850 architecture. *Elektronika ir Elektrotechnika*, ročník 25, č. 5, 2019: s. 82–87.

[APub4] Fujdiak, R.; Blazek, 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)*, IEEE, 2019, s. 1–6.

[APub5] Fujdiak, R.; Blazek, P.; Chmelar, P.; aj.: Communication Model of Smart Substation for Cyber-Detection Systems. In *International Conference on Computer Networks*, Springer, 2019, s. 256–271.

[APub6] Fujdiak, R.; Blazek, P.; Mikhaylov, K.; aj.: On track of sigfox confidentiality with end-to-end encryption. In *Proceedings of the 13th International Conference on Availability, Reliability and Security*, 2018, s. 1–6.

[APub7] Fujdiak, R.; Blazek, P.; Mlynek, P.; aj.: Developing Battery of Vulnerability Tests for Industrial Control Systems. In *2019 10th IFIP International Conference on New Technologies, Mobility and Security (NTMS)*, IEEE, 2019, s. 1–5.

[APub8] Fujdiak, R.; Mikhaylov, K.; Pospisil, J.; aj.: Insights into the issue of deploying a private LoRaWAN. *Sensors*, ročník 22, č. 5, 2022: str. 2042.

[APub9] Fujdiak, R.; Mikhaylov, K.; Stusek, M.; aj.: Security in low-power wide-area networks: State-of-the-art and development toward the 5G. In *LPWAN Technologies for IoT and M2M Applications*, Elsevier, 2020, s. 373–396.

[APub10] Fujdiak, R.; Mlynek, P.; Blazek, P.; aj.: Seeking the relation between performance and security in modern systems: metrics and measures. In *2018 41st International Conference on Telecommunications and Signal Processing (TSP)*, IEEE, 2018, s. 1–5.

[APub11] Fujdiak, R.; Mlynek, P.; Malina, L.; aj.: Development of IQRF technology: Analysis, simulations and experimental measurements. *Elektronika ir Elektrotechnika*, ročník 25, č. 2, 2019: s. 72–79.

[APub12] Fujdiak, R.; Mlynek, P.; Misurec, J.; aj.: Simulated coverage estimation of single gateway LoRaWAN network. In *2018 25th International Conference on Systems, Signals and Image Processing (IWSSIP)*, IEEE, 2018, s. 1–4.

[APub13] Fujdiak, R.; Mlynek, P.; Mrnustik, P.; aj.: Managing the secure software development. In *2019 10th IFIP International Conference on New Technologies, Mobility and Security (NTMS)*, IEEE, 2019, s. 1–4.

[APub14] Fujdiak, R.; Mlynek, P.; Slacik, J.; aj.: Investigating the Suitability of Blockchain for Smart Grid. In *2019 20th International Scientific Conference on Electric Power Engineering (EPE)*, IEEE, 2019, s. 1–6.

[APub15] Fujdiak, R.; Orgon, M.; Hallon, J.; aj.: Radiation of an Electromagnetic Field from the Power Line Communication Adapters. In *2018 41st International Conference on Telecommunications and Signal Processing (TSP)*, IEEE, 2018, s. 1–4.

[APub16] Fujdiak, R.; Pokorny, J.; Zobal, L.; aj.: Security and Performance Trade-offs for Data Distribution Service in Flying Ad-Hoc Networks. In *2019 11th International Congress on Ultra Modern Telecommunications and Control Systems and Workshops (ICUMT)*, IEEE, 2019, s. 1–5.

[APub17] Fujdiak, R.; Slacik, J.; Orgon, M.; aj.: Investigation of power line communication and wi-fi co-existence in smart home. In *2018 10th International Congress on Ultra Modern Telecommunications and Control Systems and Workshops (ICUMT)*, IEEE, 2018, s. 1–4.

[APub18] Fujdiak, R.; Uher, V.; Mlynek, P.; aj.: IP Traffic Generator Using Container Virtualization Technology. In *2018 10th International Congress on Ultra Modern Telecommunications and Control Systems and Workshops (ICUMT)*, IEEE, 2018, s. 1–6.

[APub19] Gadala, M.; Strigini, L.; Fujdiak, R.: Authentication for Operators of Critical Medical Devices: A Contribution to Analysis of Design Trade-offs. In *Proceedings of the 17th International Conference on Availability, Reliability and Security*, ACM, 2022.

[APub20] Holasova, E.; Fujdiak, R.: Deep Neural Networks for Industrial Protocol Recognition and Cipher Suite Used. In *2022 IEEE International Carnahan Conference on Security Technology (ICCST)*, IEEE, 2022, s. 1–7.

[APub21] Holasova, E.; Fujdiak, R.; Kuchar, K.: Specific Anomaly Detection Method in Wireless Communication Networks. In *2020 4th Cyber Security in Networking Conference (CSNet)*, IEEE, 2020, s. 1–3.

[APub22] Holasova, E.; Kuchar, K.; Fujdiak, R.; aj.: Security modules for securing industrial networks. In *2021 2nd International Conference on Electronics, Communications and Information Technology (CECIT)*, IEEE, 2021, s. 1125–1132.

[APub23] Ilgner, P.; Fujdiak, R.: Fuzzing Framework for IEC 60870-5-104 Protocol. In *Proceedings of the 5th International Conference on Computer Science and Software Engineering*, 2022, s. 190–194.

[APub24] Ilgner, P.; Fujdiak, R.: Fuzzing ICS Protocols: Modbus Fuzzer Framework. In *2022 IEEE International Carnahan Conference on Security Technology (ICCST)*, IEEE, 2022, s. 1–6.

[APub25] Kuchar, K.; Fujdiak, R.; Blazek, P.; aj.: Simplified Method for Fast and Efficient Incident Detection in Industrial Networks. In *2020 4th Cyber Security in Networking Conference (CSNet)*, IEEE, 2020, s. 1–3.

[APub26] Kuchar, K.; Holasova, E.; Fujdiak, R.; aj.: Incident Detection System for Industrial Networks. In *Big Data Privacy and Security in Smart Cities*, Springer, 2022, s. 83–102.

[APub27] Malina, L.; Srivastava, G.; Dzurenda, P.; aj.: A secure publish/subscribe protocol for internet of things. In *Proceedings of the 14th International Conference on Availability, Reliability and Security*, 2019, s. 1–10.

[APub28] Masek, P.; Younesian, E.; Bahna, M.; aj.: Performance Analysis of Different LoRaWAN Frequency Bands for mMTC Scenarios. In *2022 45th International Conference on Telecommunications and Signal Processing (TSP)*, IEEE, 2022, s. 417–420.

[APub29] Mikhaylov, K.; Fujdiak, R.; Pouttu, A.; aj.: Energy attack in LoRaWAN: experimental validation. In *Proceedings of the 14th International Conference on Availability, Reliability and Security*, 2019, s. 1–6.

[APub30] Mikhaylov, K.; Stusek, M.; Masek, P.; aj.: Communication performance of a real-life wide-area low-power network based on Sigfox technology. In *ICC 2020-2020 IEEE International Conference on Communications (ICC)*, IEEE, 2020, s. 1–6.

[APub31] Mikhaylov, K.; Stusek, M.; Masek, P.; aj.: On the Performance of Multi-Gateway LoRaWAN Deployments: An Experimental Study. In *2020 IEEE Wireless Communications and Networking Conference (WCNC)*, IEEE, 2020, s. 1–6.

[APub32] Mlynek, P.; Misurec, J.; Silhavy, P.; aj.: Simulation of achievable data rates of broadband power line communication for smart metering. *Applied Sciences*, ročník 9, č. 8, 2019: str. 1527.

[APub33] Mlynek, P.; Misurec, J.; Toman, P.; aj.: Performance testing and methodology for evaluation of power line communication. *Elektronika ir Elektrotechnika*, ročník 24, č. 3, 2018: s. 88–95.

[APub34] Mlynek, P.; Slacik, J.; Fujdiak, R.: Experimental Measurements of Communication Technologies for Mesh Distribution Networks of Low Voltage. In *2018 41st International Conference on Telecommunications and Signal Processing (TSP)*, IEEE, 2018, s. 1–5.

[APub35] Pokorny, J.; Fujdiak, R.; Kovanda, M.; aj.: Traffic Analysis of IEEE 802.11 on Physical Layer by using Software Defined Radio. In *2020 12th International Congress on Ultra Modern Telecommunications and Control Systems and Workshops (ICUMT)*, IEEE, 2020, s. 78–81.

[APub36] Pospisil, J.; Fujdiak, R.; Mikhaylov, K.: Investigation of the performance of TDoA-based localization over LoRaWAN in theory and practice. *Sensors*, ročník 20, č. 19, 2020: str. 5464.

[APub37] Pospisil, O.; Blazek, P.; Fujdiak, R.; aj.: Active Scanning in the Industrial Control Systems. In *2021 International Symposium on Computer Science and Intelligent Controls (ISCSIC)*, IEEE, 2021, s. 227–232.

[APub38] Pospisil, O.; Blazek, P.; Kuchar, K.; aj.: Application perspective on cybersecurity testbed for industrial control systems. *Sensors*, ročník 21, č. 23, 2021: str. 8119.

[APub39] Pospisil, O.; Fujdiak, R.; Mikhaylov, K.; aj.: Testbed for lorawan security: Design and validation through man-in-the-middle attacks study. *Applied Sciences*, ročník 11, č. 16, 2021: str. 7642.

[APub40] Potisk, L.; Hallon, J.; Orgon, M.; aj.: Electromagnetic compatibility of PLC adapters for in-home/domestic networks. *Journal of Electrical Engineering*, ročník 69, č. 1, 2018: s. 79–84.

[APub41] Róka, R.; Fujdiak, R.; Holasova, E.; aj.: Protection Schemes in HPON Networks Based on the PWFBA Algorithm. *Sensors*, ročník 22, č. 24, 2022: str. 9885.

[APub42] Ruotsalainen, H.; Shen, G.; Zhang, J.; aj.: LoRaWAN Physical Layer-Based Attacks and Countermeasures, A Review. *Sensors*, ročník 22, č. 9, 2022: str. 3127.

[APub43] Sikora, M.; Fujdiak, R.; Kuchar, K.; aj.: Generator of slow denial-of-service cyber attacks. *Sensors*, ročník 21, č. 16, 2021: str. 5473.

[APub44] Sikora, M.; Fujdiak, R.; Misurec, J.: Analysis and detection of application-independent slow Denial of Service cyber attacks. In *2021 IEEE International Conference on Intelligence and Security Informatics (ISI)*, IEEE, 2021, s. 1–6.

[APub45] Sikora, M.; Krivulcik, A.; Fujdiak, R.; aj.: Design of Advanced Slow Denial of Service Attack Generator. In *2020 12th International Congress on Ultra Modern Telecommunications and Control Systems and Workshops (ICUMT)*, IEEE, 2020, s. 99–104.

[APub46] Slacik, J.; Mlynek, P.; Fujdiak, R.: Broadband Power-line Devices Comparison and HomePlug AV2 Experimental Measurement. In *2018 41st International Conference on Telecommunications and Signal Processing (TSP)*, IEEE, 2018, s. 1–4.

[APub47] Slacik, J.; Mlynek, P.; Fujdiak, R.; aj.: Capabilities and Visions of Broadband Power-Line in Smart Grids Applications. In *2019 20th International Scientific Conference on Electric Power Engineering (EPE)*, IEEE, 2019, s. 1–5.

[APub48] Tin, P. T.; Vozriak, M.; Fujdiak, R.; aj.: Secrecy Performances of Wireless Relay Systems Affected by Hardware Impairments. In *2019 PhotonIcs & Electromagnetics Research Symposium-Spring (PIERS-Spring)*, IEEE, 2019, s. 1522–1529.

[APub49] Voznak, M.; Hendrych, J.; Orcik, J.; aj.: Population Mobility Data Retrieval from Wireless Cellular Networks. In *Proceedings of the 2019 Progress in Electromagnetics Research Symposium (PIERS-Rome)*, ročník 2019, 2019, ISBN 978-4-88552-316-8, s. 1–9.

[APub50] Vrtal, M.; Benedikt, J.; Fujdiak, R.; aj.: Investigating the Possibilities for Simulation of the Interconnected Electric Power and Communication Infrastructures. *Processes*, ročník 10, č. 12, 2022: str. 2504.

[APub51] Vrtal, M.; Benedikt, J.; Topolánek, D.; aj.: Power grid and data network simulator. In *2022 22nd International Scientific Conference on Electric Power Engineering (EPE)*, IEEE, 2022, s. 1–4.

[APub52] Zobal, L.; Kolář, D.; Fujdiak, R.: Current State of Honeypots and Deception Strategies in Cybersecurity. In *2019 11th International Congress on Ultra Modern Telecommunications and Control Systems and Workshops (ICUMT)*, IEEE, 2019, s. 1–9.

Autorovy pedagogické materiály

[APed1] Fujdiak, R.: Základy kryptografie a kryptografických algoritmů. 2015, (*skripta pro předmět MKRI*).

[APed2] Fujdiak, R.: Datová komunikace: Internet of Things IoT a Sigfox. 2017, (*laboratorní úloha pro předmět BDAK*).

[APed3] Fujdiak, R.: Datová komunikace: Technologie LoRaWAN. 2017, (*laboratorní úloha pro předmět BDAK*).

[APed4] Fujdiak, R.: Foundations of Cryptography: Random Numbers. 2018, (*přednáška pro předmět CZKR*).

[APed5] Fujdiak, R.: Vysokorychlostní komunikační systémy: LPWA Komunikační technologie - LoRaWAN. 2019, (*přednáška pro předmět BVKS a KVKS*).

[APed6] Fujdiak, R.: Vysokorychlostní komunikační systémy: LPWA Komunikační technologie - Sigfox. 2019, (*přednáška pro předmět BVKS a KVKS*).

[APed7] Fujdiak, R.; Jiří, M.: Počítačem podporovaná řešení inženýrských problémů (P1–P13). 2014, (*audiovizuální tvorba pro předmět MPPR*).

[APed8] Fujdiak, R.; Jiří, M.: Číslicové zpracování signálů (P1–P12). 2014, (*audiovizuální tvorba pro předmět BCZS*).

[APed9] Fujdiak, R.; Jiří, M.: Vyšší techniky datových přenosů: Technologie LPWAN a jejich místo mezi ostatními bezdrátovými technologiemi. 2016, (*přednáška pro předmět MVDP a LVDP*).

[APed10] Mašek, P.; Štůsek, M.; Fujdiak, R.; aj.: Komunikační systémy pro IoT. 2019, (*skripta pro předmět BVKS a KVKS*).

[APed11] Stodůlka, T.; Fujdiak, R.: *Budování Cyber Range platformy s technologií cloud computingu*. Vysoké učení technické v Brně, 2022, ISBN 9788021460645.

Autorova účast na projektech

[APro1] 731198: Rotterdam, Umea and Glasgow: Generating Exemplar Districts In Sustainable Energy Deployment (RUGGEDISED). 01.11.2016–31.10.2021, H2020-EU (*člen řešitelského týmu*).

[APro2] 737475: Aggregated Quality Assurance for Systems (AQUAS). 01.05.2017–30.06.2020, H2020-EU (*člen řešitelského týmu*).

[APro3] FAST/FEKT-J-16-3344: Agregační brána pro zabezpečený přenos dat z okamžitých měření fyzikálních veličin. 01.01.2016–31.12.2016, FEKT - interní (*spoluřešitel*).

[APro4] FEKT-S-14-2352: Výzkum elektronických komunikačních a informačních systémů. 01.01.2014–31.12.2016, FEKT - interní (*člen řešitelského týmu*).

[APro5] FEKT-S-17-4184: Výzkum informačních a komunikačních systémů a jejich bezpečnost. 01.01.2017–31.12.2019, FEKT - interní (*člen řešitelského týmu*).

[APro6] FEKT-S-20-6312: Výzkum elektronických komunikačních a informačních a systémů a jejich využití pro zabezpečení kritických infrastruktur. 01.01.2020–31.12.2022, FEKT - interní (*člen řešitelského týmu*).

[APro7] FEKT/FIT-J-18-5434: Výzkum efektivních kryptografických metod pro zvýšení bezpečnosti nastupujících komunikačních technologií v oblasti Internetu věcí. 01.01.2018–31.12.2018, FEKT - interní (*člen řešitelského týmu*).

[APro8] FEKT/FIT-J-19-5905: Experimentální prostředí pro výzkum, evaluaci a testování distribuovaných datových systémů. 01.01.2019–31.12.2019, FEKT - interní (*člen řešitelského týmu*).

[APro9] FEKT/FIT-J-19-5905: Pokročilé metody hluboké inspekce v aplikační vrstvě pro obranu proti dnešním hrozbám. 01.01.2019–31.12.2019, FEKT - interní (*člen řešitelského týmu*).

[APro10] FV20487: Inteligentní řešení pro zvýšení efektivity a automatizace pracovního procesu pro implementaci konceptu Průmysl 4.0. 01.09.2017–31.12.2019, MPO (*spoluřešitel*).

[APro11] FV40366: Datový monitoring pro zvýšení spolehlivosti procesů chytrých továren. 01.08.2019–31.12.2021, MPO (*spoluřešitel*).

[APro12] FW01010474: Analýza, detekce a mitigace hrozeb dostupnosti síťových služeb. 01.04.2020–31.12.2022, TA ČR (*spoluřešitel*).

[APro13] TJ01000381: Pokročilé behaviorální modely aplikační vrstvy pro efektivní analýzu provozu v podnikových sítích. 01.01.2018–30.06.2019, TA ČR (*spoluřešitel*).

[APro14] TJ02000332: Pokročilé metody monitorování provozu bezdrátových sítí. 01.06.2019–31.05.2021, TA ČR (*hlavní řešitel*).

[APro15] TK02030013: Kyber-fyzikální dvojče městské infrastruktury zítřka. 01.07.2019–30.06.2023, TA ČR (*spoluřešitel*).

[APro16] TK03010091: Dopady kybernetické bezpečnosti na regulované oblasti smart meteringu. 01.10.2020–31.12.2021, TA ČR (*člen řešitelského týmu*).

[APro17] VI20172019057: Monitoring a analýza komunikace pro bezpečnostní dohled kritických energetických infrastruktur. 01.01.2017–31.12.2019, MV ČR (*spoluřešitel*).

[APro18] VI20192022132: Kybernetická aréna pro výzkum, testování a edukaci v oblasti kyberbezpečnosti. 01.07.2019–30.06.2022, MV ČR (*spoluřešitel*).

Ostatní reference

[1] OpenMUC.
URL `https://www.openmuc.org/`

[2] BBraun: Operační technologie.

[3] Byres, E.: SCADA Security Basics: SCADA vs. ICS Terminology. *Tofino Security*, ročník 5, 2012.

[4] Control Engineering Česko: Propojení dat IT a OT. 2020.

[5] Cosman, E.: ICS, IACS, SCADA And So On: Do The Abbreviations Matter? 2021, (Industry trends category).

[6] Council of the European Union: Proposal for a Regulation of the European Parliament and of the Council laying down measures for a high common level of cybersecurity at the institutions, bodies, offices and agencies of the Union - General approach. 2022, (ST 14128 2022 INIT).

[7] Council of the European Union: Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/1020. 2022, (COM/2022/454 final).

[8] Council of the European Union: Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/1020. 2022, (ST 12429 2022 INIT).

[9] Emake, E. D.; Adeyanju, I. A.; Uzedhe, G. O.: Industrial Control Systems (ICS): Cyber attacks & Security Optimization. *International Journal of Computer Engineering and Information Technology*, ročník 12, č. 5, 2020: s. 31–41.

[10] IEC: Industrial communication networks – Network and system security – Part 1-1: Terminology, concepts and models. 2009.

[11] ISA, A.: ISA-99. 00. 01-2007 Security for Industrial Automation and Control Systems Part 1 Terminology, Concepts, and Models. *International Society for Automation*, ročník 10, 2007.

[12] Johnson, G.: Determinism in industrial ethernet: A technology overview-part 2. *Process Technology*, 2009.

[13] Lara, P.; Sánchez, M.; Villalobos, J.: Enterprise modeling and Operational Technologies (OT) application in the oil and gas industry. *Journal of Industrial Information Integration*, 2020: str. 100160.

[14] Michael, F.: Nejzranitelnějším článkem Průmyslu 4.0 jsou lidé. Rozhovor s Tomášem Froňkem (SIEMENS) o rizikách automatizace a digitalizace. 2021.

[15] Phinney, T.: IEC 62443: Industrial network and system security. *Last accessed July*, ročník 29, 2013.

[16] Stouffer, K.; Lightman, S.; Pillitteri, V.; aj.: Guide to industrial control systems (ics) security–nist special publication (sp) 800-82 revision 2. *NIST, Tech. Rep*, 2015.

[17] Sundararajan, A.; Chavan, A.; Saleem, D.; aj.: A survey of protocol-level challenges and solutions for distributed energy resource cyber-physical security. *Energies*, ročník 11, č. 9, 2018: str. 2360.

[18] Willis, M. J.; Tham, M. T.: Advanced process control. *Department of Chemical and Process Engineering, University of Newcastle Upon Tyne, UK*, 1994.

[19] Česká Republika: Zákon č. 240/2000 Sb.: Zákon o krizovém řízení a o změně některých zákonů (krizový zákon). *Sbírka zákonů České republiky*, 2000.

ABSTRAKT

Tato práce poskytuje komplexní přehled provozní techniky (OT) a jejích různých součástí a aplikací. Pokrývá podstatu OT, včetně základní terminologie, klíčových komponent, jako jsou procesy, senzory, akční členy, ovladače a rozhraní člověk-stroj, stejně jako komunikační techniky a technologie používané v OT. Práce se také zaměřuje na architekturu OT systémů a konvergenci IT a OT. Obsah je rozdělen do několika kapitol, z nichž každá se zaměřuje na jiný aspekt tématu, včetně případových studií a ukázek OT v různých průmyslových prostředích.

ABSTRACT

This work provides a comprehensive overview of operational technology (OT) and its various components and applications. It covers the essence of OT, including basic terminology, key components such as processes, sensors, actuators, controllers and human-machine interfaces, as well as communication techniques and technologies used in OT. The work also delves into the architecture of OT systems and the convergence of IT and OT. The content is divided into several chapters, each focusing on a different aspect of the topic, including case studies and OT demonstrations in various industrial settings.