VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

BRNO UNIVERSITY OF TECHNOLOGY

FAKULTA ELEKTROTECHNIKY A KOMUNIKAČNÍCH TECHNOLOGIÍ

FACULTY OF ELECTRICAL ENGINEERING AND COMMUNICATION

ÚSTAV TELEKOMUNIKACÍ

DEPARTMENT OF TELECOMMUNICATIONS

ANALÝZA PROTOKOLU S7 A VYTVOŘENÍ VIRTUALIZOVANÉHO PRŮMYSLOVÉHO SCÉNÁŘE

ANALYZING THE S7 PROTOCOL AND CREATING A VIRTUALIZED INDUSTRIAL SCENARIO

BAKALÁŘSKÁ PRÁCE

BACHELOR'S THESIS

AUTOR PRÁCE — Dominik Srovnal

AUTHOR

VEDOUCÍ PRÁCE — Ing. Ondřej Pospíšil

SUPERVISOR

BRNO 2022

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
FAKULTA ELEKTROTECHNIKY A KOMUNIKAČNÍCH TECHNOLOGIÍ

Bakalářská práce

bakalářský studijní program **Informační bezpečnost**

Ústav telekomunikací

Student: Dominik Srovnal ***ID:*** 214091

Ročník: 3 ***Akademický rok:*** 2021/22

NÁZEV TÉMATU:

Analýza protokolu S7 a vytvoření virtualizovaného průmyslového scénáře

POKYNY PRO VYPRACOVÁNÍ:

Student nastuduje a popíše problematiku průmyslových sítí. Zaměří se především na kybernetickou bezpečnost a komunikační průmyslové protokoly a to jmenovitě na protokol Profinet a proprietární protokol firmy Siemens s7comm. Student detailně popíše protokol S7comm a možnosti knihovny SNAP7. Dále se student zaměří na bezpečnost protokolu S7comm (bezpečnost jednotlivých verzí, kryptografické zabezpečení, možné útoky atd.). Na základě těchto znalostí student v praktické části vytvoří virtualizované prostředí simulující provoz čistírny odpadních vod za pomocí průmyslového protokolu a využití knihovny SNAP7. Dále v praktické části provede zachycení, rozbor a analýzu protokolu S7 se zaměřením na jeho bezpečnostní aspekty a také rozbor komunikace vlastního řešení.

DOPORUČENÁ LITERATURA:

[1] LEI, Cheng; DONGHONG, Li; LIANG, Ma. The spear to break the security wall of S7CommPlus. Blackhat USA, 2017.

[2] STOUFFER, Keith; FALCO, Joe; SCARFONE, Karen. Guide to industrial control systems (ICS) security. NIST special publication, 2011, 800.82: 16-16

Termín zadání: 7.2.2022 ***Termín odevzdání:*** 31.5.2022

Vedoucí práce: Ing. Ondřej Pospíšil

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

UPOZORNĚNÍ:

Autor bakalářské práce nesmí při vytváření bakalářské práce porušit autorská práva třetích osob, zejména nesmí zasahovat nedovoleným způsobem do cizích autorských práv osobnostních a musí si být plně vědom následků porušení ustanovení § 11 a následujících autorského zákona č. 121/2000 Sb., včetně možných trestněprávních důsledků vyplývajících z ustanovení části druhé, hlavy VI. díl 4 Trestního zákoníku č.40/2009 Sb.

ABSTRAKT

Průmyslové sítě jsou častým terčem útoků sloužícím k poškození výroby a narušení kritické infrastruktury v dnešní době. Ty je nutné zachytit a umět na ně správně reagovat. Právě proto je nutné se zabývat problematikou od samého počátku po konečný prvek. Tím se má na mysli prevence před možnými útoky a předpoklady pro předcházení takovým útokům na komunikaci v síti. Aby bylo možné odhalit potenciální slabiny, je třeba provést analýzy a simulace komunikace. Toho je možné dosáhnout pomocí softwarů k tomu určených. Takto se vytvořily dva programy určené k simulaci průmyslového scénáře a analýza protokolu S7. Data takové komunikace byly analyzovány a následně rozebrány.

KLÍČOVÁ SLOVA

Průmyslové řídící systémy, PLC, komunikační protokoly, Profinet, S7comm, SNAP7

ABSTRACT

Industrial network is frequent target of attacks used to damage production and disrupt today infrasctructure. It is necessary to capture such attacks and be able to react correctly to them. That is the reason, why it is necessary to deal with the problematics from the very beginning to the final element. Meaning of this is a prevention of possible attacks and the prerequisite for preventing such attacks on network communication. In order to detect potential weaknesses, communication analyzes and simulations need to be performed. This can be achieved using sofware designed specificly for such situations. Thus two programs were created to simulate the industrial scenario and analyze the S7 protocol. The data received from this communication were analyzed and subsequently scrutinized.

KEYWORDS

Industrial Control Systems, PLC, communication protocols, Profinet, S7comm, SNAP7

Vysázeno pomocí balíčku `thesis` verze 4.07; `http://latex.feec.vutbr.cz`

SROVNAL, Dominik. *Analýza protokolu S7 a vytvoření virtualizovaného průmyslového scénáře*. Brno: Vysoké učení technické v Brně, Fakulta elektrotechniky a komunikačních technologií, Ústav telekomunikací, 2022, 81 s. Bakalářská práce. Vedoucí práce: Ing. Ondřej Pospíšil

Prohlášení autora o původnosti díla

Jméno a příjmení autora:	Dominik Srovnal
VUT ID autora:	214091
Typ práce:	Bakalářská práce
Akademický rok:	2021/22
Téma závěrečné práce:	Analýza protokolu S7 a vytvoření virtualizovaného průmyslového scénáře

Prohlašuji, že svou závěrečnou práci jsem vypracoval samostatně pod vedením vedoucí/ho závěrečné práce a s použitím odborné literatury a dalších informačních zdrojů, které jsou všechny citovány v práci a uvedeny v seznamu literatury na konci práce.

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

Brno ....

podpis autora*

*Autor podepisuje pouze v tištěné verzi.

PODĚKOVÁNÍ

Rád bych poděkoval vedoucímu bakalářské práce panu Ing. Ondřeji Pospíšilovi za odborné vedení, konzultace, trpělivost a podnětné návrhy k práci.

Obsah

Seznam obrázků

Seznam tabulek

Seznam výpisů

Úvod

Automatizace funguje na bázi mechanizace. Mechanizace poskytuje zařízení lidem k usnadnění její práce. Automatizace snižuje potřebnou přítomnost člověka při vykonávání činnosti a tím zvyšuje efektivitu, přesnost a možnost rozvoje v průmyslu a jiných odvětvích.

Bakalářská práce se zabývá problematikou průmyslových sítí a jejich komunikačních protokolů, zejména jde o protokoly Profinet a proprietární protokol společnost Siemens S7comm. Kvůli velmi rychlému vývoji moderních technologií v průmyslu i mimo něj, je v dnešní době třeba využívát simulací k detekcí nových potenciálních slabin a anomálií, které mohou narušit jejich funkčnost a chod.

Cílem bakalářské práce je vytvoření průmyslového scénáře, pomocí kterého můžeme sledovat komunikaci mezi PLC a HMI. První část se bude zabývat průmyslovými zařízeními a výběrem jejich komunikačních protokolů. V druhé části budou rozebrány dva konkrétní komunikační protokoly. V třetí části bakalářské práce bude rozebrána knihovna Snap7. Čtvrtá část bude zaměřená na praktickou stránku bakalářské práce, tedy vymyšlení průmyslového scénáře. Poslední část se bude zabývat analýzou a rozborem protokolu S7.

1 Průmyslové řídící systémy (ICS)

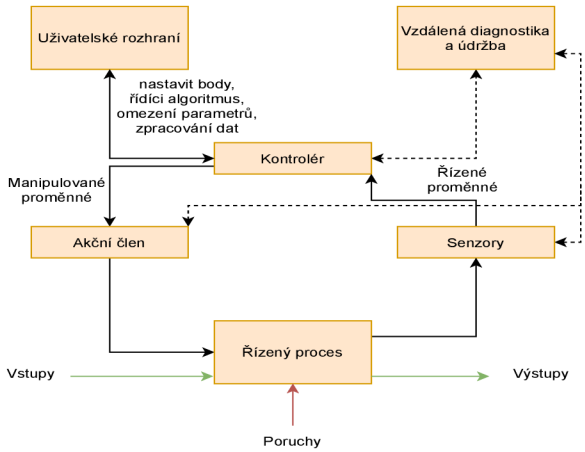
Průmyslové řídící systémy, anglicky Industrial Control Systems (ICS), je obecné pojmenování struktury, jež zahrnuje několik typů řídících systémů. Mezi hojně využívané systémy se řadí dispečerské řízení a sběr dat (Supervisory Control And Data Acquisition - SCADA), distribuované řídící systémy (Distributed Control Systems - DCS) a také programovatelné logické automaty (Programmable Logic Controller - PLC) se kterými se nejčastěji setkáme v průmyslových odvětvích a kritické infrastruktuře.[10] Tyto systémy spadají, společně s dalšími prvky, do takzvané průmyslové automatizační pyramidy jež se dělí na [35]:

- Field level - úroveň akčního členu či technologická úroveň
- Control level - kontrolní úroveň
- Process control level - nadřazená kontrolní úroveň
- Planning level - úroveň plánování výroby
- Enterprise level - podniková úroveň

Základem této pyramidy jsou mimo jiné ovládací komponenty, jejichž nejdůležitější členění je dle druhu zpracovávané energie (např. elektrické, mechanické, hydraulické, pneumatické) a dle vykonávané funkce (např. akční člen, měřící člen), které mohou působit společně k dosáhnutí průmyslových cílů (např. výroba či přenos energie).[10]

Proces je jednou z klíčových částí systému, jehož primární úkol je vytvoření výstupu. Řídící část systému obsahuje specifikaci požadovaného výstupu nebo výkonu. Řízení může být plně automatizované nebo může být ovládáno člověkem. Systémy lze nakonfigurovat tak, aby fungovaly v režimu s otevřenou smyčkou, s uzavřenou smyčkou a v manuálním režimu. V systémech řízení s otevřenou smyčkou je výstup řízen podle zavedených nastavení. V řídicích systémech s uzavřenou smyčkou má výstup vliv na vstup takovým způsobem, aby byl zachován požadovaný cíl. V manuálním režimu je systém plně ovládán člověkem. Část systému, která se primárně zabývá udržováním shody se specifikacemi, se nazývá regulátor, který funguje na principu zpětné vazby. Skvělým jednoduchým příkladem regulátoru je termostat, jenž na základě snímače teploty neustále vyhodnocuje informace dle kterých vydává pokyny k ohřevu. Dalším a posledním druhem řízení je ovládání, pro které je charakteristická nemožnost zpětné vazby. Typické ICS může obsahovat mnohé řídicí smyčky, uživatelské rozhraní (Human-Machine Interface - HMI) a nástroje pro vzdálenou diagnostiku a údržbu vytvořené pomocí řady síťových protokolů, jenž jsou spadají do další pozice v pyramidovém schématu. ICS se typicky používají
v elektrotechnickém, vodním a odpadním, ropném a zemním plynu, chemickém, do-

pravním, farmaceutickém, celulózovém a papírenském, potravinářském a nápojovém průmyslu a v diskrétní výrobě (např. automobilový průmysl, letecký průmysl a zboží dlouhodobé spotřeby). Jak vypadá taková ICS operace lze vidět na obr. 1.1.[10]



Obr. 1.1: Operace ICS

Při navrhování síťové architektury pro nasazení ICS se obvykle doporučuje oddělit síť ICS od podnikové sítě.[10]

Povaha síťového provozu v těchto dvou sítích je odlišná: přístup k Internetu, protokol k přenosu souborů (File Transfer Protocol - FTP), e-mail a vzdálený přístup budou obvykle povoleny v podnikové síti, ale neměly by být povoleny v síti ICS.[10]

V podnikové síti nemusí být zavedeny přísné postupy řízení změn pro síťové vybavení, konfiguraci a změny softwaru. Pokud je provoz sítě ICS přenášen v podnikové síti, mohl by být zachycen nebo vystaven útoku DoS (Denial of Service - znemožnění přístupu služby). Díky odděleným sítím by problémy se zabezpečením a výkonem v podnikové síti neměly mít vliv na síť ICS.[10]

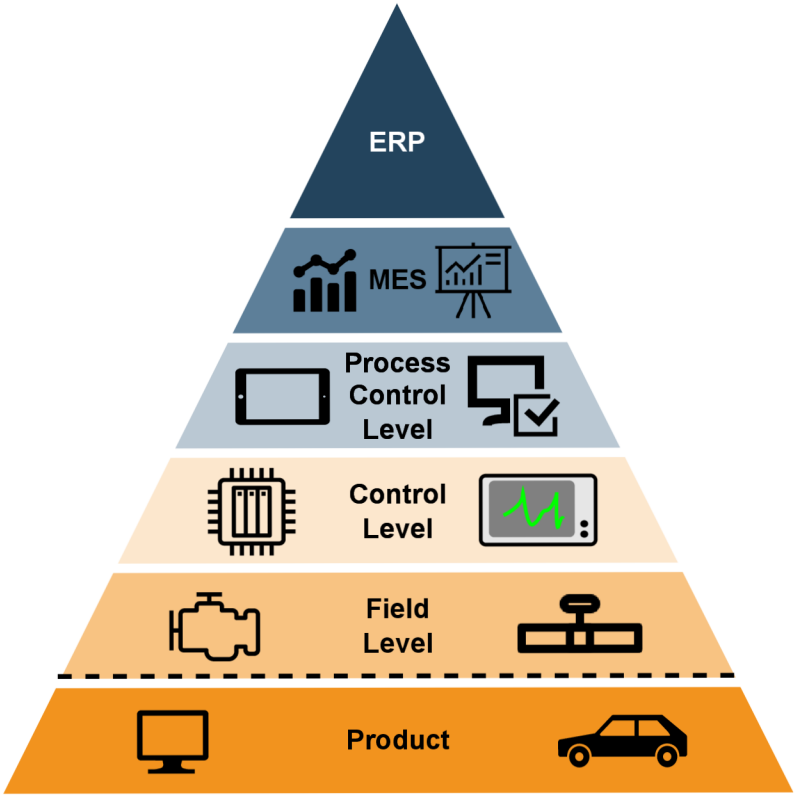
Většinou se vyžaduje spojení mezi ICS a podnikovými sítěmi. Toto spojení představuje významné bezpečnostní riziko a mělo by být chráněno ochrannými zařízeními. [10]

Pokud musí být sítě propojeny, důrazně se doporučuje, aby byla povolena pouze minimální (pokud možno jediná) připojení a aby připojení probíhalo přes firewall a DMZ.[10]

DMZ je samostatný síťový segment, který se připojuje přímo k firewallu. Do tohoto segmentu sítě jsou umístěny servery obsahující data z ICS, ke kterým je potřeba přistupovat z podnikové sítě. Pouze tyto systémy by měly být přístupné z podnikové sítě. U všech externích připojení by měl být povolen minimální přístup přes bránu firewall, včetně otevření pouze portů požadovaných pro konkrétní komunikaci.[10]

1.1 Automatizační pyramida

Do automatizační pyramidy spadají sekce, které na sebe technologicky navazují viz. úvod do kapitoly 1. Taková pyramida je zobrazena na obr 1.2.



Obr. 1.2: Automatizační pyramida

1.1.1 Field level

V úrovni akčního členu, tzv. Field level, se nachází prvky vykonávající aktivní a měřící činnost. [35] Tato úroveň je naprostým základem pyramidy dle standardu IEC 62264. Akční členy jsou primárně rozdělovány dle fyzikálního působení a to na:

- Elektromechanické akční členy
  - Asynchronní motory
  - Synchronní motory
  - Stejnosměrné motory
  - Lineární motory
- Hydraulické akční členy
  - Hydromotory
  - Ventily

- Pneumatické akční členy
  - Ventily
- Optické akční členy
  - Laser
- Topné a chladící akční členy
  - Topné těleso
  - Chladič

Mezi měřící členy se mimo jiné řadí následující:

- Senzor
- Detektor
- Čítač
- Časovač
- Analyzátor fyzikálních veličin

Uvedené akční a měřící členy umožňují výrobu, užívání běžných zařízení a jiné. Měřící zařízení a akční členy po zpracování požadavku odesílají data zpět do nadřazeného PLC, který vyhodnocuje získaná data.[8] Příkladem může být vodní čerpadlo - je li ponořené vodní čerpadlo s plovákem na hladině, kde plovák je měřící člen a vodní čerpadlo členem akčním, můžeme odčerpávat vodu. Podmínkou však je, aby byl plovák umístěn nad úrovní středu čerpadla, a to z důvodu zamezení poškození zadřením, tzv. během na sucho. V případě, že plovák klesne pod úroveň středu čerpadla, zastaví se proces odčerpávání.

Komunikace mezi field levelem a control levelem probíhá pomocí tzv. fieldbusů. Ty jsou normalizované dle standardu IEC 61158. Existuje mnoho fieldbusů - mezi nejznámější se řadí Modbus, Profibus, FIP - Factory Instrumentation Protocol a CAN - Controller Area Network.

1.1.2 Control level

Programovatelný logický automat (PLC)

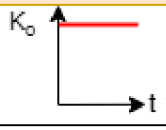
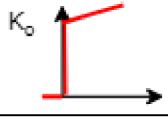
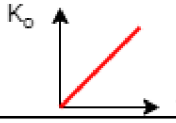
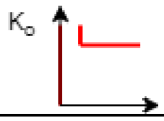
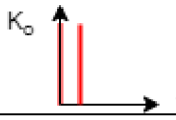
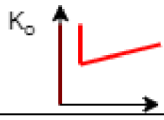
Jsou to průmyslové počítače používané k řízení různých elektromechanických procesů pro použití ve výrobě, výrobních závodech nebo jiných automatizačních prostředích.[31] Hlavními výhodami pro hojné zastoupení PLC v průmyslu jsou nízké provozní náklady, snadná programovatelnost a možnost libovolného rozšíření o potřebné moduly.

Každý PLC systém se skládá ze dvou hlavních komponentů. Těmi jsou centrální procesorová jednotka (CPU) a digitální či analogové I/O moduly. Dalšími důležitými komponenty programovatelného automatu jsou systémová a uživatelská paměť.[31]

PLC jsou zpravidla menších rozměrů, což je jednou z jejich charakteristických vlastností. V průmyslu se také vyskytují PLC systémy větších rozměrů, ať už se jedná

o celek či automat napěchovaný externími moduly.[33] Existuje široké spektrum modulů, které se zpravidla využívají pro rozšíření možností využití PLC. Mezi ně patří různé diagnostické, vizualizační či komunikační moduly nebo PID regulátory.

PID regulátory, celým názvem Proporciálně-Integračně-Derivační regulátory, se dělí na přímé a nepřímé. Přímé regulátory odebírají energii z regulované soustavy načež nepřímé regulátory vyžadují externí zdroj energie. PID regulátory jsou univerzální, můžeme se však setkat pouze s proporcionálními (P) regulátory. Integrační (I) regulátory existují za účelem eliminace odchylky vzniklé P regulátorem a nejdou použít samostatně. Jelikož derivační regulátor (D) pouze urychluje danou regulaci, tak jej též nelze využít samostatně. Dále existují jejich kombinace, a to proporciálně-integrační (PI), proporciálně-derivační (PD). Na obrázku 1.3 graficky znázorněné charakteristiky chování zmíněných regulací. [23]

Regulátory	Ideální Charakteristika	Regulátory	Ideální Charakteristika
Regulátor P		Regulátor PI	
Regulátor I		Regulátor PD	
Regulátor D		PID	

Obr. 1.3: Charakteristika PID

PLC jsou široce používány v různých průmyslových odvětvích (např. strojní výroba či farmaceutický průmysl). Je to zejména, mimo výše uvedené, kvůli intuitivní obsluze na bázi logiky. Logika je stavební kámen programování automatů a lze je programovat několika způsoby[33]:

- Graficky
  - Ladder Diagram - reléové schéma
  - Function Block Diagram (FBD) - logické schéma
  - Sequential Function Chart (SFC) - sekvenční schéma
- Algebraicky
  - Instruction List (IL) - Instrukční list
  - Structured Text (ST) - Strukturovaný text

Z grafických programovacích způsobů vyčnívá FBD. Nejrozšířenějším softwarem pro programování metodou FBD je Logo!Soft Comfort od firmy Siemens.

PLC můžeme řadit podle modularity do dvou skupin: První skupinou jsou kompaktní PLC. Tyto PLC obsahují všechny komponenty v jednom zařízení (CPU, I/O moduly, napájecí jednotka). Mají ale velmi omezené možnosti pro další rozšíření.[6] Druhou skupinou jsou modulární PLC. Jedná se o systém, který se skládá ze samostatných modulů, které lze kombinovat nebo doplňovat. Tyto PLC mají neomezené možnosti dalšího rozšiřování.[6]

PLC jsou základním hardwarovým prvkem pro systémy SCADA, které jsou navržené přímo pro sběr dat. Tato data můžeme v jisté míře využít za pomocí HMI a případně v tomto pokročilém uživatelském rozhraní řídící vstupy a výstupy ovládat.[10]

Uživatelské rozhraní (HMI)

HMI bylo vytvořeno k co nejsnazšímu a efektivnímu řízení. Operátoři linek, manažeři a supervizoři v průmyslu spoléhají na HMI při převodu složitých dat na užitečné informace.[32]

HMI se používá například k monitorování strojů, aby byla zajištěna jejich správná funkčnost. Snadno srozumitelné vizuální displeje dávají význam a kontext téměř v reálném čase. Nabízejí informace o hladinách v nádrži, měření tlaku a vibrací, stavu motoru a ventilu a dalších proměnných.[32]

Pokročilé možnosti dnešních HMI umožňují manažerům a supervizorům dělat mnohem víc než jen procesy kontroly. Pomocí historických a trendových dat nabízejí obrovské nové příležitosti ke zlepšení kvality produktů a zefektivnění systémů.[32]

Ze všech těchto důvodů hrají HMI klíčovou roli v hladkém a efektivním chodu továren a výrobních operací.[32]

Inženýrská pracovní stanice

Inženýrská pracovní stanice je obvykle velmi výkonná a spolehlivá výpočetní platforma určená pro konfiguraci, údržbu a diagnostiku aplikací řídicího systému a dalších zařízení řídicích systémů.[7]

Systém se obvykle skládá z redundantních pevných disků, vysokorychlostního síťového rozhraní, spolehlivých CPU, výkonného grafického hardwaru a aplikací, které poskytují konfigurační a monitorovací nástroje pro provádění vývoje aplikací řídicího systému, kompilace a distribuce systémových modifikací.[7]

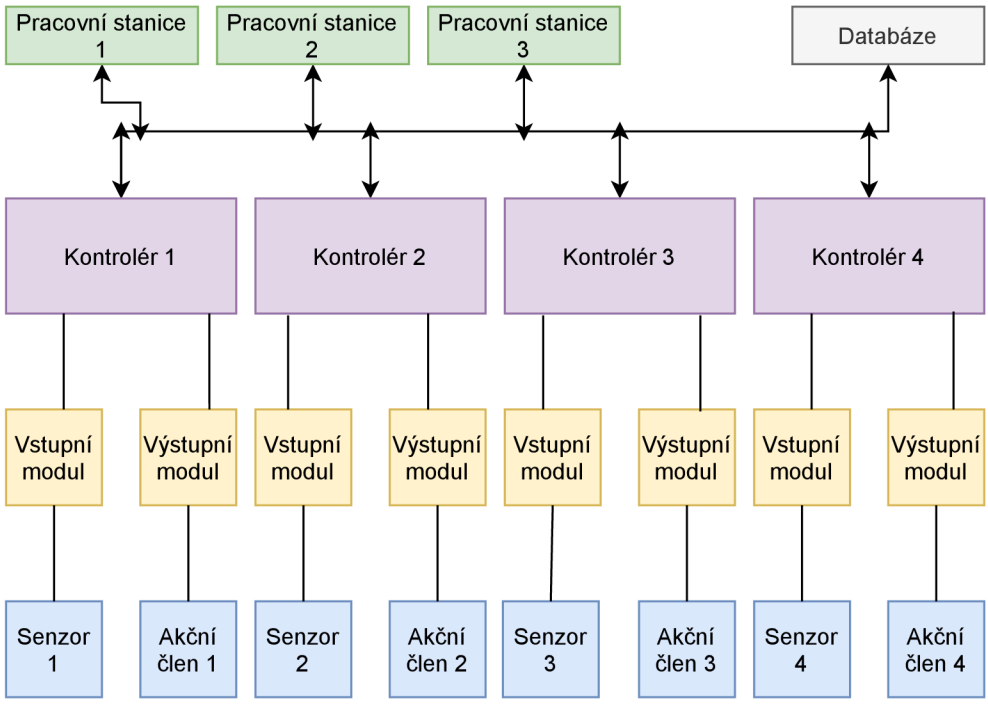
Distribuované řídící systémy (DCS)

DCS se používají k řízení výrobních systémů ve stejné geografické lokalitě pro průmyslová odvětví, jako jsou ropné rafinérie, čištění vody a odpadních vod, závody na výrobu elektrické energie, chemické výrobní závody, automobilová výroba a zařízení

na zpracování farmaceutických výrobků. Tyto systémy jsou obvykle systémy řízení procesů nebo systémů řízení diskrétních částí.[10]

DCS jsou integrovány jako řídicí architektura obsahující dohledovou úroveň řízení dohlížející na více integrovaných subsystémů, které jsou odpovědné za řízení detailů lokalizovaného procesu.[10]

DCS využívá centralizovanou kontrolní smyčku ke zprostředkování skupiny lokalizovaných kontrolérů, které sdílejí celkové úkoly provádění celého výrobního procesu. Řízení produktu a procesu se obvykle dosahuje nasazením zpětné vazby nebo dopředných regulačních smyček, přičemž klíčové podmínky produktu a procesu jsou automaticky udržovány kolem požadované nastavené hodnoty. Aby se dosáhlo požadované tolerance produktu a procesu kolem specifikované nastavené hodnoty, jsou v terénu použity specifické procesní regulátory nebo schopnější PLC, které jsou vyladěny tak, aby poskytovaly požadovanou toleranci a také míru samočinné korekce během poruch procesu. Modularizací výrobního systému snižuje DCS dopad jediné chyby na celý systém. V mnoha moderních systémech je DCS propojen s podnikovou sítí, aby obchodní operace měly přehled o výrobě.[10]



Obr. 1.4: Architektura DCS

Obrázek 1.4 zobrazuje architekturu DCS. Pracovní stanice řídí a komunikují s Kontroléry, které mají za úkol dohlížet na chod a správu zařízení, jako jsou například senzory. Pracovní stanice i kontroléry komunikují s databází. Kontrolní úrovně komunikují s field levely vybranými fieldbusy, např. Profibus či

Modbus. V případě komunikace s vyššími úrovněmi se začíná vyskytovat ethernet TCP/IP.

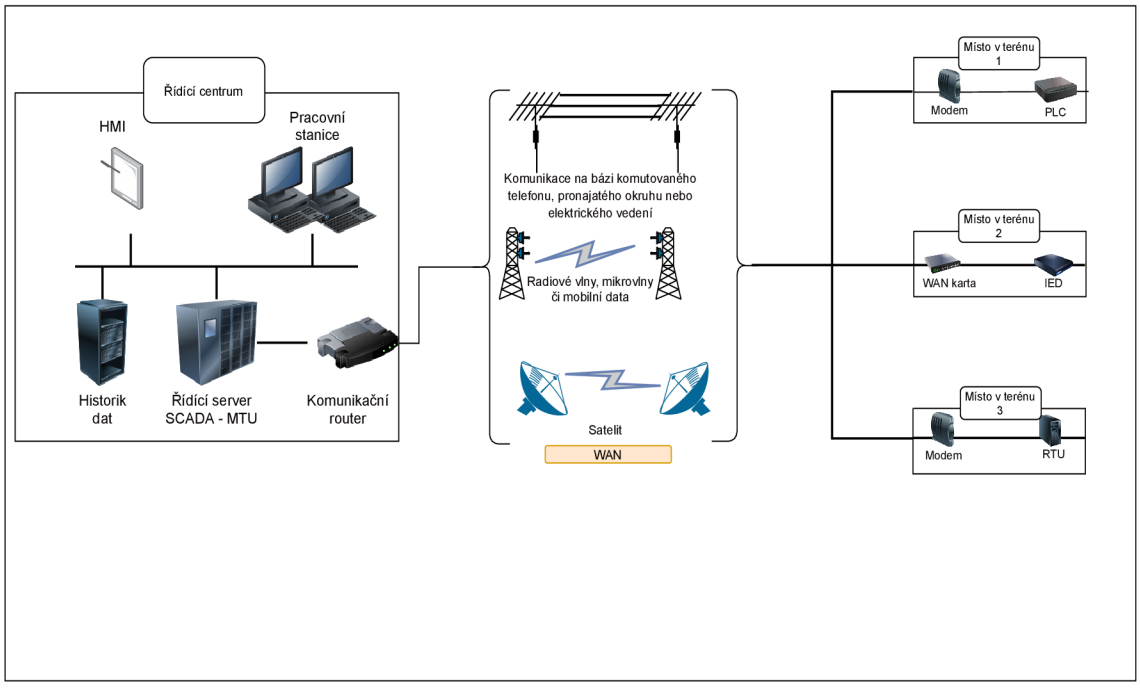
1.1.3 Process control level

SCADA Systémy

Systémy SCADA se používají k řízení rozptýlených aktiv, kde je centralizovaný sběr dat stejně důležitý jako řízení. Tyto systémy se používají v distribučních systémech, jako jsou rozvody vody a systémy sběru odpadních vod, potrubí na ropu a zemní plyn, přenosové a distribuční systémy elektrické energie, železniční a jiné systémy veřejné dopravy.[10]

SCADA systémy integrují systémy sběru dat se systémy přenosu dat a softwarem HMI, aby poskytovaly centralizovaný monitorovací a řídicí systém pro četné procesní vstupy a výstupy.[10]

SCADA systémy jsou navrženy tak, aby shromažďovaly informace o terénu, přenášely je do centrálního počítačového zařízení a zobrazovaly informace operátorovi graficky nebo textově, což operátorovi umožňuje monitorovat nebo ovládat celý systém z centrálního místa téměř v reálném čase. Na základě propracovanosti a nastavení jednotlivého systému může být řízení libovolného jednotlivého systému, operace nebo úkolu automatické nebo může být prováděno příkazy operátora.[10]



Obr. 1.5: Obecná konfigurace systému SCADA

Obrázek 1.5 ukazuje součásti a obecnou konfiguraci systému SCADA. V řídicím centru je umístěn řídicí server a komunikační směrovače. Mezi další součásti řídicího centra patří HMI, inženýrské pracovní stanice a datový historik, které jsou všechny propojeny sítí LAN.[10]

Řídicí centrum shromažďuje a zaznamenává informace shromážděné v terénu, zobrazuje informace HMI a může generovat akce na základě zjištěných událostí.[10]

Řídicí centrum je také zodpovědné za centralizované alarmování, analýzy trendů a hlášení. Místo v terénu provádí místní ovládání akčních členů a monitoruje senzory. Pracoviště jsou často vybavena funkcí vzdáleného přístupu, která operátorům umožňuje provádět vzdálenou diagnostiku a opravy obvykle přes samostatný vytáčený modem nebo připojení WAN. Standardní a proprietární komunikační protokoly běžící přes sériovou a síťovou komunikaci se používají k přenosu informací mezi řídicím střediskem a provozními místy pomocí telemetrických technik, jako je telefonní linka, kabel, vlákno a rádiové frekvence, jako je vysílání, mikrovlnná trouba a satelit.[10]

1.1.4 Planning a Enterprise level

Podniková úroveň společně s plánováním výroby spadají do nejvyšších vrstev pyramidy, kde podnik je nadřazený plánování. Zkratka MES z anglického Manufacturing Execution Systems (výrobní realizační systém) je v dnešní době používána častěji oproti označení planning level. MES se skládá z řízení výroby a kontrolních funkcí jako například plánování, kvalita výroby, kontrola výrobních nákladů atp. MES je základním stavebním kamenem pro tzv. čtvrtou průmyslovou revoluci (I4.0), což je termín používaný po celém světě k popisu konvergence technologiích založených na IoT (Internet of Things - Internet věcí), širším spektru rozhodování a pokročilé automatizaci. Jinými slovy, I4.0 pomáhá spravovat a optimalizovat veškeré aspekty výrobního procesu a dodávek materiálu.[35]

Podniková úroveň, nově označovaná jako tzv. Plánování podnikových zdrojů z anglického Enterprise Resource Planning (ERP), koordinuje kompletní proces výroby a shromažďuje data analyzovaná a spravovaná v různých oblastech výroby. ERP, stejně jako MES, je důležité pro I4.0 implementace, zejména pro[35]:

- Monitorování a zkoumání dat v reálném čase k odhalení atypických situací
- Začlenění souboru pravidel pro podnikání do systému ERP na základě kterého je vytvořen autonomní systém
- Nastavení komunikačního kanálu mezi manažerem a výrobními stroji, jelikož jsou přenosná zařízení integrována do ERP

ERP systém umožňuje správu transakcí pomocí sdílené robustní databáze se standardními postupy a výměnou dat mezi potřebnými sekcemi ve firmě. Ve velkém počtu výrobních společností jsou ERP systémy podporou pro produkci a distribuci. Ty jsou implementovány za účelem částečné integrace a automatizace finanční, manažerské, výrobní a prodejní funkce. Hojně používaným ERP software systémem je SAP ERP od společnosti SAP.

1.2 Konvergence Informační technologie (IT) a Operační technologie (OT)

Operační technologie (OT) označuje hardware a software používaný s automatizačními řídicími systémy v rámci infrastruktury. OT sítě a systémy včetně průmyslových řídicích systémů (ICS) nebo dohledového řízení a získávání dat (SCADA) se používají v mnoha průmyslových odvětvích, jako je energetika, ropa a plyn, úprava vody, doprava, obrana, řízení dopravy a dokonce i v rámci soukromých zařízení k monitorování a řízení funkcí, jako je vytápění a chlazení. Tato průmyslová odvětví tvoří součást našich národních kritických infrastruktur, bez nichž by společnost a ekonomika selhaly.[14]

Systémy OT byly navrženy tak, aby integrovaly systémy sběru dat, systémy přenosu dat a systémy rozhraní HMI za účelem vytvoření řešení centralizovaného řízení a monitorování. To umožňuje operátorovi vizuálně interpretovat stav závodu pro účely řízení a monitorování.[14]

Informační technologie (IT) je použití jakýchkoli počítačů, úložišť, sítí a dalších fyzických zařízení, infrastruktury a procesů k vytváření, zpracování, ukládání, zabezpečení a výměně všech forem elektronických dat.[14]

IT se obvykle používá v kontextu obchodních operací, na rozdíl od technologie používané pro osobní nebo zábavní účely. Komerční využití IT zahrnuje jak výpočetní techniku, tak telekomunikace.[14]

Obrázek 1.6 ukazuje trend v průmyslu konvergence IT a OT systémů za účelem přístupu k datům v reálném čase a propojování zařízení. Konvergence je řízena potřebou kvantitativního vykazování managementu, kterému pomáhá technologie „velkých dat“ a senzorů, umělá inteligence, fyzická automatizace, vzdálené operace, cloud, výpočetní technika, analytika. Všechny mají potenciál zvýšit produktivitu nebo výrobu. K usnadnění tohoto všeho je třeba, aby operátoři zvýšili síťovou konektivitu a přístup k IT i OT systémům pomocí standardů Ethernet, WI-FI a TCP/IP.

Díky konvergenci IT a OT jsou systémy, které byly dříve v mnoha ohledech uzavřené, nyní propojeny a vystaveny všem rizikům, která v IT prostoru po léta existují. S tímto odhalením, a nikoli neočekávaně, se objevili jednotlivci nebo skupiny, které

Obr. 1.6: Trend v průmyslu konvergence IT a OT

chtějí využít tyto nově nalezené zranitelnosti. Konvergence sama o sobě není problém, ačkoli obrázek 1.6 zdůrazňuje některé zjevné rozdíly mezi IT a OT světem. Významným problémem jsou zcela odlišné priority mezi IT a OT, které způsobují diskontinuitu v bezpečnostním prostoru.[14]

1.3 Komunikační protokoly

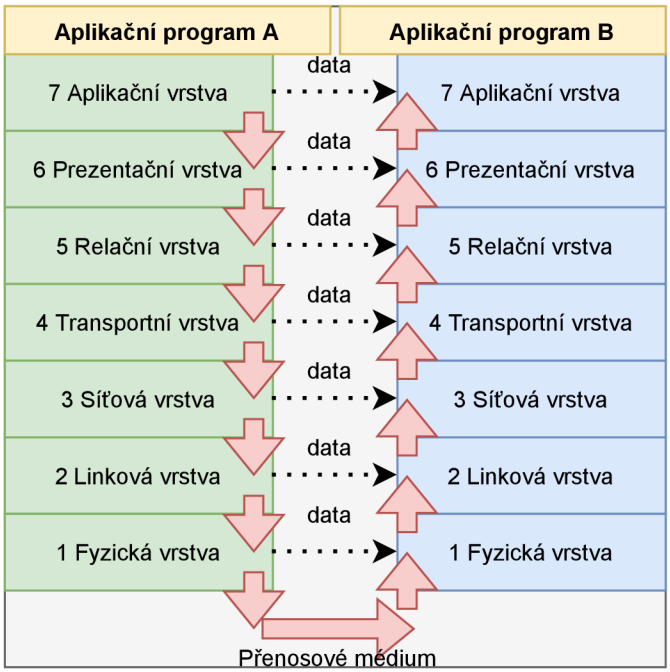
1.3.1 Průmyslový Ethernet

Ethernet

Ethernet je komunikační síť jako součást počítačové sítě. Pojem Ethernet se používá i pro pojmenování protokolů podle kterých se propojení mezi sítěmi uskutečňuje. Používá se zde sedmivrstvý referenční model ISO/OSI. Spodní vrstvy modelu se nazývají fyzická, linková, síťová a transportní a jsou to vrstvy orientované na vlastní komunikační síť. Vyšší vrstvy jsou relační, prezentační a aplikační. Tyto vrstvy jsou orientovány na aplikační použití.[22][20]

Obrázek 1.7 ukazuje referenční model ISO/OSI, ve kterém jsou vazby vyznačené šipkami a představují fyzický směr informačního toku mezi dvěma, nebo více účastníky. Čárkované spoje značí spojení mezi účastníky.

Fyzická vrstva je nejnižší vrstva referenčního modelu ISO/OSI a je určena pro nezabezpečovaný přenos dat ve formě modulovaného a kódovaného proudu bitů, jenž prochází přenosovým médiem. Linková vrstva zabezpečuje přenos bitů, které jsou seskupeny do bloků, umožňuje přístup ke přenosovému médiu komunikující stanici nebo účastníkovi. Síťová vrstva zodpovídá za směrování zpráv mezi více než dvěma účastníky a segmenty sítě. Transportní vrstva vytváří rozhraní mezi spodními a vrchními vrstvami modelu ISO/OSI a zodpovídá za způsob adresování a formát adres.



Obr. 1.7: Referenční model ISO/OSI

Relační vrstva zodpovídá za navázání nebo zrušení spojení mezi účastníky a dohlíží nad tímto spojení. Prezentační vrstva je překladatelská vrstva mezi interpretacemi informace přicházející z aplikační vrstvy. Uskutečňují se v ní konverze syntaxe zpráv. Aplikační vrstva je nejvyšší vrstva referenčního modelu ISO/OSI a slouží k poskytování služby jednotlivým účastníkům k tomu, aby mohli předávat zprávy a zároveň je rozhraním mezi procesy přenosu a vlastního použití dat.[22][19]

Průmyslový Ethernet

Průmyslový Ethernet pramení ze standardu IEEE 802.3 v oblasti konektorů, přenosových médií a dalšího obvodového řešení viz Tab. 1.2. Tyto oblasti splňují požadavky na odolnost proti elektrickému šumu, mechanickým vibracím, vlivům teploty a má potřebnou životnost viz. Tab 1.1. Průmyslový Ethernet úspěšně realizuje komunikační protokoly, které řeší interoperabilitu, tedy schopnost různých vzájemné spolupracovat a poskytovat služby, inteligentních zařízení a přenosy dat mezi nimi, včetně jejich řízení.[22][2]

Třídy kabelů do průmyslového prostředí a jejich vybrané charakteristiky		
Třída	**Light Duty**	**Heavy Duty**
Krytí	IP20 podle IEC 60529, EN 60529	IP67 podle IEC 60529, EN60529
Provozní teplota	0 až +55°C	-20 až +65°C
Rázy	15g/11 ms (IEC60068-2-27, EN 60068-2-27)	
Vibrace	5g při 10 až 150 Hz (IEC 60068-2-27, EN 60068-2-27, krit. A)	

Tab. 1.1: Třídy kabelů[20]

Metalické kabely podle specifikace IAONA		
Určení	**Kabely pro instalace**	**Spojovací kabely**
Průřez jádra	AWG 24/1 až AWG 22/1	AWG 26/7 až AWG 24/7
Norma	EN 50288-2-1	EN 50288-2-2
Počet párů	2 nebo 4	
Frekvenční rozsah	kategorie 5 (100 MHz)	
Průměr kabelu (čtyři páry)	6 až 8,5 mm (Light duty), 7 až 9,5 mm (Heavy duty)	5 až 6 mm (Light duty), 6 až 7 mm (Heavy duty)
Materiál pláště	nespecifikován	
Stínění	společné měděné stínění nebo fólie plus měděné stínění	
Maximální délka kabelu	100 m	60 m, popř. 50m pro spolehlivý přenos
Hořlavost	IEC 60332-1 (jednoduchá zkouška hořlavosti)	
Tvorba solí	dle normy IEC60754-2	

Tab. 1.2: Metalické kabely[20]

Průmyslový ethernet je ethernet vhodně modifikovaný do výrobního prostředí. Základ přebírá z IEEE 802.3 a díky modifikacím si získává následující kvality[20]:

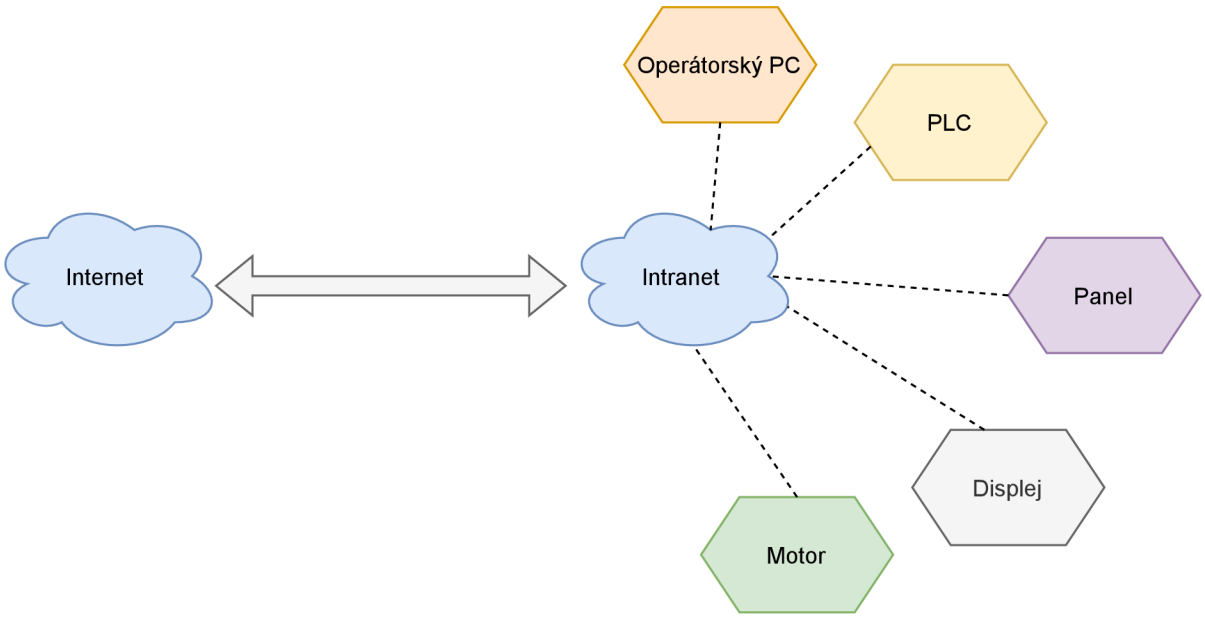
- Lze přizpůsobit pro více funkcí
- Kvalitnější konektory a jejich systém spojení viz. Tab. 1.3
- Umožňuje rychlou redundanci sítě v případě odpojení kabelu - přesměrování dat
- Determinismus a reálný čas

Ethernetové konektory do průmyslového prostředí		
Typ	**Standard**	**Podporováno**
M12-4	IEC 61076-2-101-A1	ODVA, PNO
RJ45-IP67	IEC 61076-3-106 (varianta 01)	ODVA, PNO
RRJ45-IP67	IEC 61076-3-106 (varianta 06)	IDA, Interbus-Club

Tab. 1.3: Ethernetové konektory[20]

Protokolů, které spadají pod průmyslový Ethernet je mnoho, mezi nejpoužívanější patří Profinet, EtherNet/IP, EtherCAT, Modbus-TCP, POWERLINK nebo třeba CC-Link IE Field.[22]

Na obrázku 1.8 můžeme vidět využití Ethernetu v průmyslu. Ethernet zde propojuje navzájem odloučené jednotky I/O, které zajišťují sběr dat a přenos řídících signálů, PLC, řídící PC, systémy CNC, průmyslové roboty, dohledové video systémy, skenery, ovládací displeje, průmyslové regulátory, elektronické systémy pneumatických, hydraulických, elektrických pohonů a dalších zařízení.



Obr. 1.8: Využití Ethernetu v průmyslu

Determinismus a reálný čas

Determinismus je důležitou součástí Průmyslového Ethernetu a prakticky jej separuje od Ethernetu. Standardní Ethernet není sám o sobě deterministický kdežto výrobní prostředí determinismus vyžaduje. Výrobní prostředí potřebuje pakety dat odeslané a přijaté v konkrétních časech s garancí, že bude každý paket vždy doručen. Tato podmínka je nutná, jelikož ztráta nebo zpoždění dat mezi zařízeními v průmyslu může skončit katastrofou, např. kritickou chybou ve výrobním procesu. Determinismus je nezbytným předpokladem pro funkčnost reálného času v průmyslové komunikaci.[21]

Reálný čas v systémech je v dnešní době žádanějším než kdy dříve. Je to z důvodu snižování ceny výpočetních technologií a s tím související nárůst výpočetního výkonu, tzn. reálný čas umožňuje vyšší efektivitu. Reálný čas neznamená automaticky rychlejší provedení, ale spíše to, že proces je závislý na včasném provedení úlohy. Včasnost a současnost jsou požadavky pro vyřešení i náročnějších situací. Z toho vyplývá, že optimální vytíženost CPU zde není nejdůležitější. V tabulce 1.4 jsou vyjádřeny standardní požadavky na časy cyklů pro jednotlivé kontroly.[21][12]

Standardní časy cyklů pro kontrolní úroveň	
Kontrolní úroveň	Standardní čas cyklu
Nízkorychlostní senzory	Desítky milisekund
Řídící systémy pohonů	Milisekundy
Řízení pohybu	Stovky mikrosekund
Přesné řízení pohybu	Desítky mikrosekund
Vysokorychlostní zařízení	Mikrosekundy
Elektronický rozsah - detekce chyb	Stovky nanosekund

Tab. 1.4: Využití Ethernetu v průmyslu

Průmyslový Ethernet v reálném čase nabízí mnoho výhod v kontrolní úrovni vůči již existujícím řešením. V kontrolní síti Průmyslový Ethernet nabízí 10 Gbps, což je téměř tisíckrát více, než dnešní fieldbus sítě (např. 12 kbps u PROFIbusu).[33]

Existuje široké spektrum protokolů, jejich standardů, komunikačních profilů a přenosových rychlostí jednotlivých Průmyslových Ethernetů viz. jejich výběr v Tab. 1.5.

Tab. 1.5: Typy protokolů Průmyslového Ethernetu

Protokol	Standard	CPF - Komunikační profil	IEC/PAS NP	Přenosová rychlost	Open source
EtherCAT	IEC 61158, IEC 61784-2	CPF12	IEC/PAS 62407	100Mbit/s	ANO
EtherNet/IP	IEEE 802.3	CPF2	IEC/PAS 62413	100 Mbit/s	ANO
Ethernet Powerlink	IEEE 802.3 , IEC 61784-2	CPF13	IEC/PAS 62408	100 Mbit/s	ANO
Modbus-RTPS	-	CPF15	IEC/PAS 62030	1MB/s	ANO
P-net on IP	IEEE 802.3i	CPF4	IEC/PAS 62412	10 Mbit/s	ANO
Profinet	IEEE 802.3u, IEC 61158, IEC 61784-2	CPF3	IEC/PAS 62411	100 Mbit/s	ANO
SERCOS III	IEEE 802.3 & ISO/IEC 8802-3	CPF16	IEC/PAS 62410	100 Mbit/s	ANO
TCnet	IEC 61158-3	CPF11	IEC/PAS 62406	100 Mbit/s	ANO
Vnet/IP	IEEE802.3	CPF10	IEC/PAS 62405	1 Gbit/s	ANO

1.3.2 Profinet

Profinet je nejpokročilejší řešení průmyslového Ethernetu na světě. Jedná se o komunikační protokol pro výměnu dat mezi ovladači a zařízeními. Regulátory mohou být PLC, DCS nebo PAC. Zařízeními mohou být I/O bloky, systémy vidění, čtečky RFID, procesní nástroje, proxy nebo jiné řídicí jednotky.[18]

Profinet je plně kompatibilní s tzv. office Ethernetem a využívá všechny jeho funkce. Nicméně existují rozdíly, office Ethernet není schopen výkonu v reálném čase pro průmyslovou automatizaci. Office Ethernet také mnohem hůře odolává drsným průmyslovým prostředím. Protokolem Profinet se budeme detailně zabývat později.[18]

1.3.3 EtherNet/IP

EtherNet/IP je ethernetová komunikační síť, která uživatelům poskytuje nástroje pro nasazení standardní ethernetové technologie, jako je IEEE 802.3 v kombinaci se sadou TCP/IP Suite v aplikacích průmyslové automatizace a zároveň umožňuje připojení k internetu v podnikové konektivitě.[9]

EtherNet/IP nabízí různé možnosti topologie sítě, včetně hvězdicové nebo lineární se standardními zařízeními ethernetové infrastruktury nebo Device Level Ring (DLR) se speciálně aktivovanými zařízeními EtherNet/IP.[9]

Funkce QuickConnect umožňuje rychlou výměnu zařízení, zatímco síť běží. Shoda se standardy IEEE Ethernet poskytuje uživatelům výběr rychlostí síťového rozhraní, např. 10, 100 Mb/s a 1 Gb/s, a flexibilní síťovou architekturu kompatibilní s komerčně dostupnými možnostmi instalace Ethernetu, včetně metalických, optických a bezdrátových. Možnosti pro průmyslově hodnocená zařízení obsahující IP67 nebo lepší konektory s moduly a LED stavu sítě s označením zařízení umožňují snadné použití.[9]

EtherNet/IP pro své vyšší vrstvy využívá Společný průmyslový protokol (CIP). CIP sítě se řídí modelem OSI, který definuje rámec pro implementaci síťových protokolů v sedmi vrstvách: fyzická, datová linka, síťová, transportní, relační, prezentační a aplikační. Sítě, které se řídí tímto modelem, definují kompletní sadu síťových funkcí od fyzické implementace přes aplikační vrstvu nebo vrstvu uživatelského rozhraní.[9]

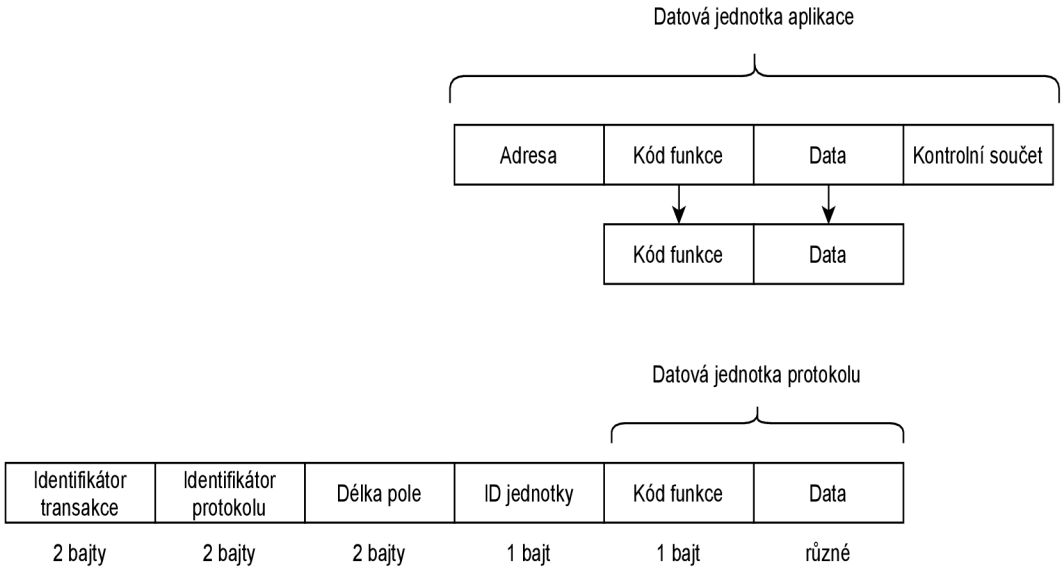
CIP zahrnuje komplexní sadu zpráv a služeb pro různé aplikace automatizace výroby, včetně řízení, bezpečnosti, zabezpečení, energie, synchronizace a pohybu, správy informací a sítě. Jako skutečně na médiích nezávislý protokol, který podporují stovky prodejců po celém světě, poskytuje CIP uživatelům jednotnou komunikační architekturu v celém výrobním podniku.[9]

1.3.4 Modbus-TCP

Modbus TCP/IP (také Modbus-TCP) je protokol Modbus RTU s rozhraním TCP, který běží na Ethernetu. Struktura zpráv Modbus je aplikační protokol, který definuje pravidla pro organizaci a interpretaci dat nezávisle na médiu pro přenos dat.[13]

TCP/IP odkazuje na Transmission Control Protocol a Internet Protocol, které poskytují přenosové médium pro zasílání zpráv Modbus TCP/IP. TCP/IP umožňuje výměnu bloků binárních dat mezi počítači. Je to také celosvětový standard, který slouží jako základ pro World Wide Web. Primární funkcí TCP je zajistit, aby byly všechny pakety dat přijímány správně, zatímco IP zajišťuje, že zprávy jsou správně adresovány a směrovány. Kombinace TCP/IP je pouze přenosový protokol a nedefinuje, co data znamenají nebo jak mají být data interpretována, to je úkolem aplikačního protokolu, v tomto případě Modbus.[13]

Modbus TCP/IP používá TCP/IP a Ethernet k přenosu dat struktury zpráv Modbus mezi kompatibilními zařízeními. To znamená, že Modbus TCP/IP kombinuje fyzickou síť (Ethernet) se síťovým standardem (TCP/IP) a standardní metodu reprezentace dat (Modbus jako aplikační protokol). Zpráva Modbus TCP/IP je v podstatě komunikace Modbus zapouzdřená v ethernetovém obalu TCP/IP.[13]



Obr. 1.9: Struktura Modbus-TCP

Z obrázku 1.9 vidíme, že kód funkce a datová pole jsou absorbována ve své původní podobě. Proto Modbus TCP/IP Application Data Unit (ADU) má podobu 7 bajtové hlavičky (Identifikátor transakce + Identifikátor protokolu + pole délky + Unit ID) a datové jednotky protokolu (kód funkce + data). Záhlaví MBAP je dlouhé 7 bajtů a obsahuje následující pole:

Identifikátor transakce (2 bajty): Tato identifikace pole se používá pro párování transakcí v případě více zpráv odeslané po stejném TCP spojení klientem bez čekání předchozí odpověď.[13]

Identifikátor protokolu (2 bajty): Toto pole je vždy 0 pro Modbus služby a další hodnoty jsou vyhrazeny pro budoucí rozšíření.[13]

Délka pole (2 bajty): Toto pole představuje počet bajtů zbývajících polí a zahrnuje bajt Unit ID, bajt kódu funkce a data pole.[13]

ID jenotky (1 bajt): Toto pole se používá k identifikaci vzdáleného serveru umístěného v síti bez TCP/IP (pro sériové přemostění). V typické serverové aplikaci Modbus TCP/IP je unit ID nastaveno na 00 nebo FF, server je ignoruje a jednoduše se vrátí zpět do odpovědi.[13]

1.3.5 POWERLINK

POWERLINK používá kombinaci timeslotu a dotazování dosáhnout izochronního přenosu dat. Aby byla zajištěna koordinace, PLC nebo průmyslové PC je označeno jako tzv. řídící uzel (MN). Tento uzel vynucuje časování cyklu, které slouží k synchronizaci všech zařízení a řídí cyklickou datovou komunikaci. Všechna ostatní zařízení fungují jako řízené uzly (CN). V průběhu jednoho hodinového cyklu MN zasílá tzv. „Poll Requests“ do jedné CN za druhou v pevném pořadí. Každý CN na tento požadavek okamžitě odpoví „Poll Response“, kterému mohou naslouchat všechny ostatní uzly.[11]

Cyklus POWERLINK se skládá ze tří period. Během „Start Period“ MN odešle rámec „Start of Cycle“ (SoC) do všech CN pro synchronizaci zařízení. Jitter je asi 20 nanosekund. Cyklická izochronní výměna dat probíhá během druhého periody („cyklická perioda“). Multiplexování umožňuje v této fázi optimalizované využití šířky pásma. Třetí perioda označuje začátek asynchronní fáze, která umožňuje přenos velkých, časově kritických datových paketů. Takové údaje, např. uživatelská data nebo TCP/IP rámce, je rozptýlena mezi asynchronními fázemi několika cyklů.[11]

POWERLINK rozlišuje mezi doménami v reálném čase a mimo ně. Vzhledem k tomu, že přenos dat v asynchronní periodě podporuje standardní IP rámce, routery oddělují data bezpečně a transparentně od domén reálného času. POWERLINK se velmi dobře hodí pro všechny druhy automatizačních aplikací včetně I/O, Motion Control, robotických úloh, PLC-to-PLC komunikace a vizualizace.[11]

1.3.6 CC-Link IE Field

CC-Link IE Field je vysokorychlostní a velkokapacitní síť, která poskytuje jak synchronní deterministickou (cyklickou) komunikaci, tak asynchronní komunikaci na

vyžádání (přechodnou). I/O ovládání, řízení pohybu a bezpečnostní funkce lze kombinovat. Gigabitový přenos a protokol v reálném čase umožňuje snadnou a spolehlivou datovou komunikaci a vzdálenou I/O komunikaci nezávislou na zpoždění přenosu. Vysokorychlostní komunikace pro informace o správě zařízení a informace o sledování a také pro přenos řídicích dat. Flexibilní topologie sítě. Síťová sdílená paměť umožňuje komunikaci mezi řídicími jednotkami a provozními zařízeními. Snadná konfigurace a diagnostika sítě umožňuje celkové snížení nákladů na inženýrství od spuštění systému až po údržbu.[5]

CC-Link IE Field může přistupovat k zařízením přímo pomocí nástrojů vzdáleného inženýrství v celé hierarchii sítě. Zařízení lze monitorovat nebo konfigurovat odkudkoli v síti, což zvyšuje efektivitu inženýrství díky vzdálené správě. Vzhledem k tomu, že fyzické vrstvy a linkové vrstvy CC-Link IE Field Network využívají standardní technologii Ethernet, lze použít běžné kabely, přepínače a rozbočovače.[5]

2 Vybrané komunikační protokoly Profinet a S7comm

2.1 Profinet

Profinet byl vyvinut Profibus International a firmou Siemens v roce 2004. Tento protokol je založen na průmyslovém Ethernetu. Ethernet funguje na bázi instalační technologie, komunikace v reálném čase, správy sítě a funkce pro webovou integraci. Optimální podpory pro různé typy aplikací dosáhne pomocí dvou možností: Profinetu IO pro integraci distribuovaných I/O a Profinetu CBA pro vytváření modulárních závodů v distribuované automatizaci. Bezproblémová integrace systémů fieldbus se zajišťuje prostřednictvím konceptu proxy. To je důležitá funkce umožňující jednoduché rozšíření zařízení. Profinet je optimálním komunikačním systém pro automatizační techniku na bázi průmyslového Ethernetu.[17]

Profinet je komplexní standard, který splňuje všechny požadavky na použití Ethernetu v průmyslové automatizaci, od komunikace na úrovni kontroléru, standardní automatizace s I/O systémy až po výkonné aplikace pro řízení pohybu. Profinet je proto vhodný pro všechny automatizační aplikace.[17]

Referenční model ISO/OSI				
Vrstva	**Úloha**	**Standardní komunikace**		**Komunikace v reálném čase**
7b	zpracování	Profinet IO služby a protokol	Profinet CBA	-
7a	zpracování	RPC bez připojení	DCOM, RPC orientovaný na připojení	-
6	zobrazení	-	-	-
5	komunikace	Rozhraní soket	-	-
4	přenos	UDP	TCP	-
3	přepínání	IP	-	-
2	zabezpečení	Plný Duplex, rozšíření reálného času	-	Protokol v reálném čase Isochronní protokol v reálném čase
1	bitový přenos	100Base-TX, 100Base-FX	-	Adapter síťového ethernetu

Obr. 2.1: Profinet v referenčním modelu ISO/OSI

Vývoj Profinetu stále pokračuje. Probíhají práce na definicích pro témata zabezpečení a bezpečnosti, stejně jako na převodu profilu Profidrive na Profinet, aby bylo

možné používat aplikace pro řízení pohybu. Téma operací údržby bylo také zahájeno jako první krok k rozhraní na úroveň MES. V oblasti automatizace procesů se v současné době definují požadavky na využití Profinetu. [17]

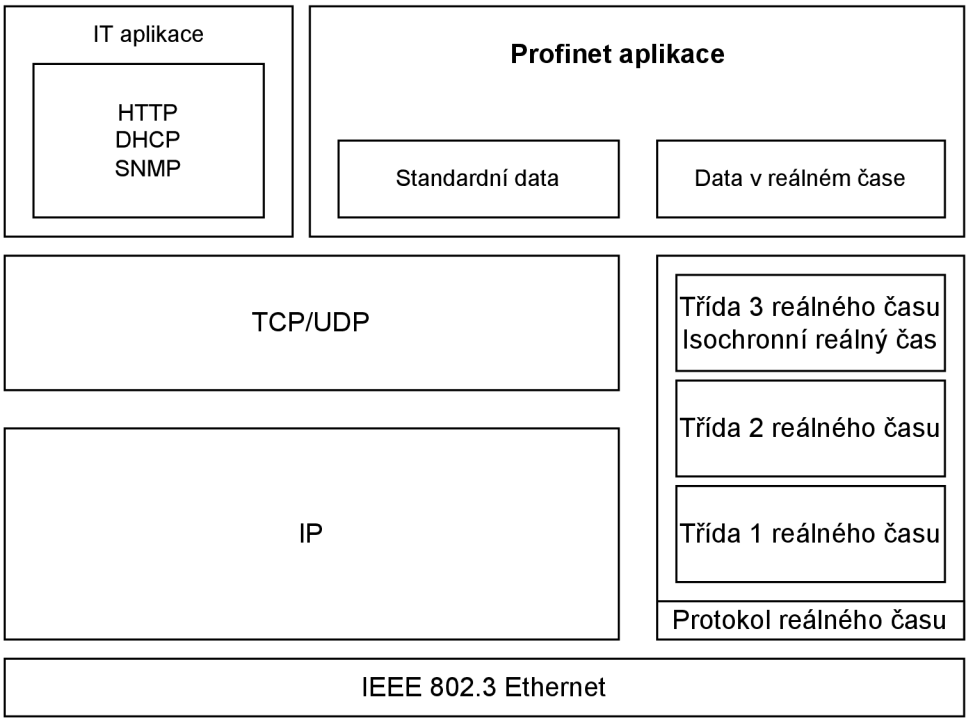
Pro Profinet bylo navíc velmi důležité brzké zavedení produktové certifikace. Jde o opatření doprovázející technologický vývoj, jehož prostřednictvím vysoký standard kvality produktů Profinet je zaručen hned od začátku.[17]

2.1.1 Použití Profinetu

Profinet slouží jako komunikační protokol mezi řídícími systémy a zařízeními v automatizovaném provozu. Musí zajistit přenos s dostatečnou rychlostí a vhodným determinismem. Profinet je jednoduchý k použití, jelikož neklade vysoké nároky na náklady instalaci a uvedení do provozu. Je kompatibilní s Ethernetem díky IEEE standardům a dle standardů IEC 61158 je schopný propojení v již existujícím provozu bez jakéhokoliv problému. To je hlavním důvodem volby Profinetu oproti S7Comm protokolu. Ten je hojně užívaný ve výrobě používající primárně ICS od firmy Siemens.

2.1.2 Komunikace Profinet

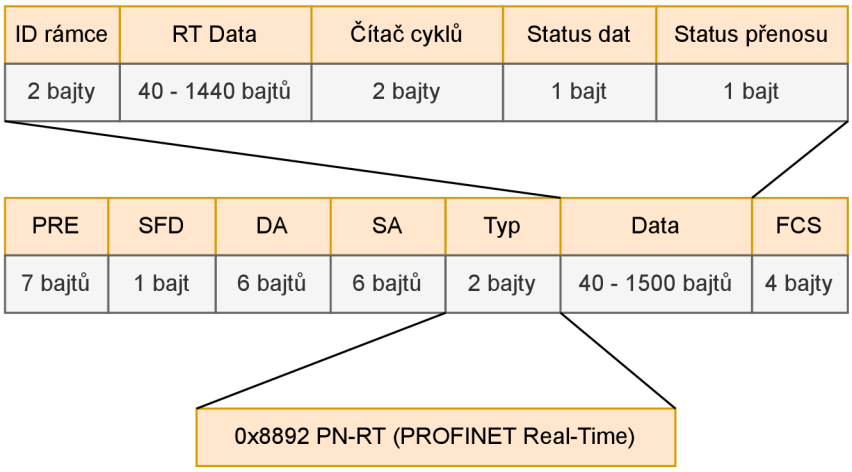
Pro komunikaci Profinet jsou k dispozici různé úrovně výkonu. Parametry, konfigurační data a informace o propojení, které nejsou z hlediska času kritické, jsou přenášeny v Profinet standardním kanálem založeným na TCP/UDP a IP. To splňuje předpoklady pro propojení úrovní automatizace s jinými sítěmi (manufacturing execution systems (MES), enterprise resource planning (ERP)).[28] Celá komunikace v Profinetu funguje na bázi vrstev v blokovém diagramu viz. obr. 2.2



Obr. 2.2: Blokové schéma vrstev Profinetu

Pro přenos časově kritických procesních dat v rámci výrobního závodu je k dispozici kanál reálného času známý jako soft real time (SRT). Tento kanál je implementován jako software na základě stávajících regulátorů. Rámcová struktura protokolu pro reálný čas viz. obr. 2.3.[28]

Pro izochronní aplikace je k dispozici izochronní komunikace v reálném čase (IRT), která umožňuje frekvenci hodinových impulzů menší než 1 ms a přesnost jitteru 1 μs.[28]



Obr. 2.3: Struktura rámce Profinetu

2.1.3 Síťová a IT instalace

Instalace sítě Profinet jsou orientovány na specifické požadavky na sítě Ethernet v průmyslovém prostředí. *Profinet Installation Guideline* poskytuje konstruktérům zařízení a provozovatelům zařízení jednoduchá pravidla pro instalaci ethernetových sítí a související kabeláže. Tato směrnice poskytuje výrobcům zařízení jasné specifikace rozhraní zařízení.[28]

Správa sítě zahrnuje funkce pro správu zařízení Profinet v sítích Ethernet. To zahrnuje konfiguraci zařízení, konfiguraci sítě a diagnostiku sítě. V případě webové integrace využívá Profinet základní technologie Ethernet a umožňuje přístup ke komponentě Profinet pomocí standardních internetových technologií. Aby bylo zachováno otevřené spojení s jinými typy systémů, Profinet podporuje OPC DA (přístup k datům) a DX (výměna dat).[28]

2.1.4 Fieldbus integrace

Důležitým aspektem Profinet je bezproblémový přechod ze stávajících fieldbus řešení, jako je Profibus DP, na Profinet na bázi Ethernetu. To významně přispívá k ochraně investic ze strany výrobce zařízení, konstruktéra zařízení/strojního systémového inženýra a koncového uživatele.[28]

Profinet nabízí dvě alternativy pro integraci fieldbus systémů:

Integrace fieldbus zařízení pomocí proxy. Proxy je zástupcem polních zařízení nižší úrovně na Ethernetu. Prostřednictvím principu proxy nabízí Profinet zcela transparentní přechod ze stávajících na nově instalované jednotky závodu.[28]

Integrace celých aplikací fieldbus. Segment fieldbus představuje samostatnou komponentu. Představitelem této komponenty je zařízení Profinet, které provozuje

fieldbus, jako je PROFIBUS DP na nižší úrovni. Celá funkčnost nižší úrovně fieldbus je tak implementována ve formě komponenty v proxy, která je k dispozici na Ethernetu.[28]

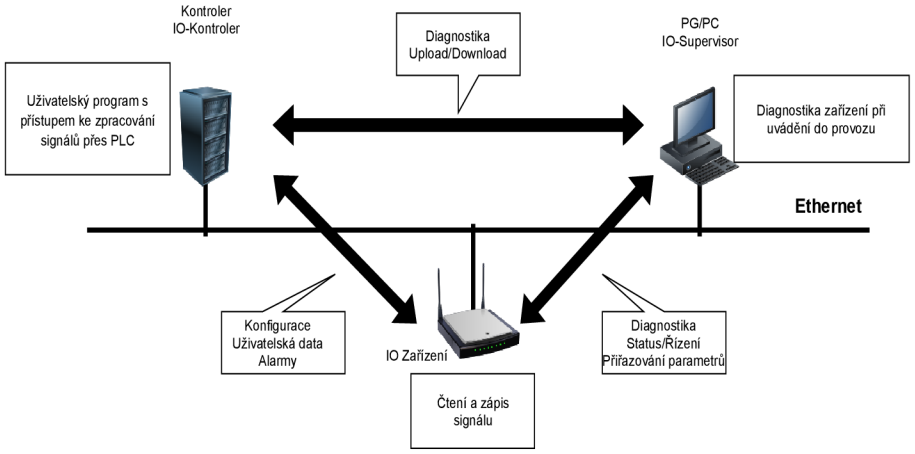
2.1.5 Profinet komponenty

Představitelem technologického modulu při projektování závodu je tzv. komponenta Profinet. Každá komponenta Profinet má rozhraní, které obsahuje technologické proměnné, které se mají vyměňovat s ostatními komponentami.[28]

Komponenty Profinet jsou modelovány pomocí technologie standardizovaného objektového modelu komponent (COM). COM je pokročilá objektová orientace, která umožňuje vývoj aplikací na základě předem sestavených komponent. Komponenty se vyznačují tvorbou úplných jednotek, které mohou být ve vztahu s jinými komponentami. Stejně jako bloky lze komponenty flexibilně kombinovat a snadno znovu použít, bez ohledu na to, jak jsou interně implementovány. Přístupové mechanismy k rozhraním komponent jsou v Profinet jednotně definovány.[28]

2.1.6 Profinet IO

Profinet IO umožňuje přímé propojení distribuovaných polních zařízení na Ethernetu. Všechna používaná zařízení jsou propojena v jednotné síťové struktuře, a proto nabízejí jednotnou komunikaci v celém výrobním závodě. Uživatelský pohled na Profibus DP byl z velké části aplikován na konfiguraci, programování a diagnostiku.[4]



Obr. 2.4: Typy zařízení v Profinet IO

Profinet IO specifikuje kompletní výměnu dat mezi IO Controllery a IO zařízeními, jakož i jejich parametrizaci a diagnostiku. Je navržen pro rychlou výměnu dat s dobou cyklu sběrnice několik milisekund a je založen na modelu provider/consumer. Polní zařízení v podřízeném segmentu Profibus lze integrovat do Profinet IO-System pomocí proxy.[17]

V kontextu Profinet je Profinet IO komunikační koncept pro implementaci modulárních, distribuovaných aplikací na průmyslovém Ethernetu. Distribuované I/O a provozní zařízení jsou integrována do ethernetové komunikace pomocí Profinet IO. Vzhled a ovládání Profinet IO inženýrství je orientováno podle Profibus DP. Programování uživatelského programu pro IO-Controller je ekvivalentní postupu s Profibus DP. Kromě toho jsou pro Profinet IO k dispozici nové bloky a seznamy stavů systému. Protože se vyměňuje pouze rozhraní k přenosovému médiu, lze již dříve nainstalované I/O Profibus dále používat. Pohled I/O známý z Profibus DP je zachován. Uživatelská data z provozních zařízení jsou cyklicky přenášena v reálném čase do procesního obrazu automatizačního systému.[27]

Koncept Profinet IO

Distribuovaná polní zařízení, tzv. Profinet IO-Devices, jsou při konfiguraci přiřazena k programovatelnému kontroléru, Profinet IO-Controller. Pokud má Profinet IO-Controller také rozhraní Profibus, může být současně DP masterem podřízeného

Profibusu. Pokud má navíc funkcionalitu Profinet CBA, lze ji použít k implementaci technologických modulů v rámci distribuovaného automatizačního systému. S Profinet IO byl princip master/slave známý z Profibus DP převeden na model provider/-consumer. Z hlediska komunikace mají všechna zařízení Profinet stejná oprávnění na Ethernetu. Každému zařízení je však při konfiguraci přiřazen typ a ten definuje typ a způsob komunikace podle modelu provider/consumer.[17]

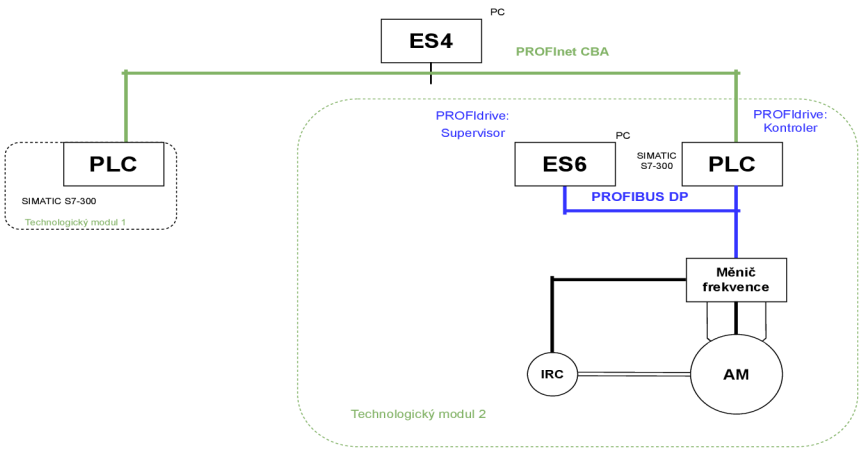
Datový tok Profinet IO

Výměna dat mezi komunikačními stanicemi Profinet IO probíhá prostřednictvím standardního kanálu založeného na UDP/IP a kanálu v reálném čase. V rámci těchto kanálů jsou data opět přenášena různými protokoly.[17]

2.1.7 Profinet CBA

Profinet CBA je nový koncept automatizace, který se objevil jako výsledek trendu v automatizační technice směrem k modulárním, opakovaně použitelným strojům (mechatronickým komponentům) a závodům s distribuovanou inteligencí. Se svým komplexním designem (jednotný model pro inženýrskou, komunikační a migrační architekturu na jiné komunikační systémy, jako je Profibus a OPC), Profinet CBA splňuje všechny klíčové požadavky automatizační techniky pro:

Konzistentní komunikace od úrovně pole až po úroveň podnikového řízení, jako je plánování podnikových zdrojů (ERP) a systémy řízení výroby (MES) využívající Ethernet. Inženýrský model celého závodu nezávislý na dodavateli pro celé prostředí automatizace. Otevřenost vůči jiným systémům. Implementace IT standardů. Schopnost integrace segmentů Profibus beze změn.[28]



Obr. 2.5: Komunikační struktura systému Profinet CBA

2.2 S7comm

S7comm (S7 Communication) je proprietární protokol společnosti Siemens, který běží mezi programovatelnými logickými automaty (PLC).[24]

Používá se jako komunikační pro dorozumívání se s PLC, výměnu dat mezi PLC, přístup k PLC datům ze systémů SCADA (dohledové řízení a získávání dat) a pro diagnostické účely. [24]

OSI Vrstva	Protokol
7 Aplikační vrstva	S7comm
6 Prezentační vrstva	S7comm
5 Relační vrstva	S7comm
4 Transportní vrstva	ISO-on-TCP
3 Síťová vrstva	IP
2 Linková vrstva	Ethernet
1 Fyzická vrstva	Ethernet

Obr. 2.6: S7comm na referenčním modelu ISO/OSI

2.2.1 Použití a rozdělení protokolu S7comm

Protokol S7comm se ve všech jeho verzích používá ke komunikaci Siemens PLC mezi sebou a TIA portálem. Všechny verze protokolů využívají TPKT a transportního protokolu dle ISO8073 včetně portu 102/TCP.[29]

- S7Comm protokol
- Early S7CommPlus protokol
- S7CommPlus protokol

S7Comm protokol se využívá je komunikaci mezi PLC S7-200, S7-300 a S7-400. Tento protokol nezahrnuje žádný mechanismus proti útokům a je snadno zneužitelný. Early S7CommPlus protokol se používá při komunikaci mezi PLC S7-1200v3.0 a je komplikovanější než S7Comm protokol, avšak je snadno prolomitelný. S7 protokol má následující výhody[29]:

- Nezávislost na sběrnici (Profibus, Industrial Ethernet)
- Lze použít ve všech oblastech S7
- Možnost přenosu až 64kB

- Automatické potvrzení datových záznamů
- Nízké zatížení procesoru a sběrnice při přenosu velkých objemů dat

2.2.2 Komunikace S7comm

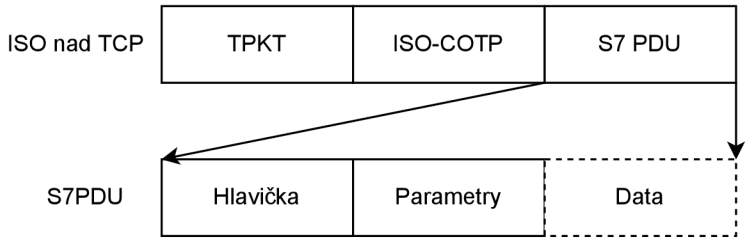
Při komunikaci se zařízeními S7 existuje celá rodina protokolů, které lze použít. Obecně je lze rozdělit na protokoly Profinet a protokoly S7 Comm. Protokoly S7 Comm mají mnohem jednodušší strukturu, ale také jsou mnohem méně zdokumentované.[3] [29]

S7-PDU

Protokol S7 se skládá z bloků. Každý blok se jmenuje PDU (Protocol Data Unit), jeho maximální délka závisí na komunikačních procesorech (CP) a je vytvářena během spojení. Protokol S7 je funkčně nebo příkazově orientovaný, to znamená, že každý přenos obsahuje příkaz nebo odpověď. Pokud se velikost příkazu nevejde do PDU, musí být rozdělena mezi další následující PDU.[25]

Každý příkaz se skládá ze záhlaví, sady parametrů, data o parametrech a datovém bloku viz. obrázek 2.7, kde[16]:

- Záhlaví (hlavička): obsahuje délkovou informaci, PDU reference a konstantu typu zprávy
- Parametry: Obsah a struktura parametrů se liší v závislosti na typu zprávy a funkci PDU
- Data: Volitelné pole k přenosu dat, pokud nějaká existují, např. hodnoty pamětí, kódy bloků, data firmwaru



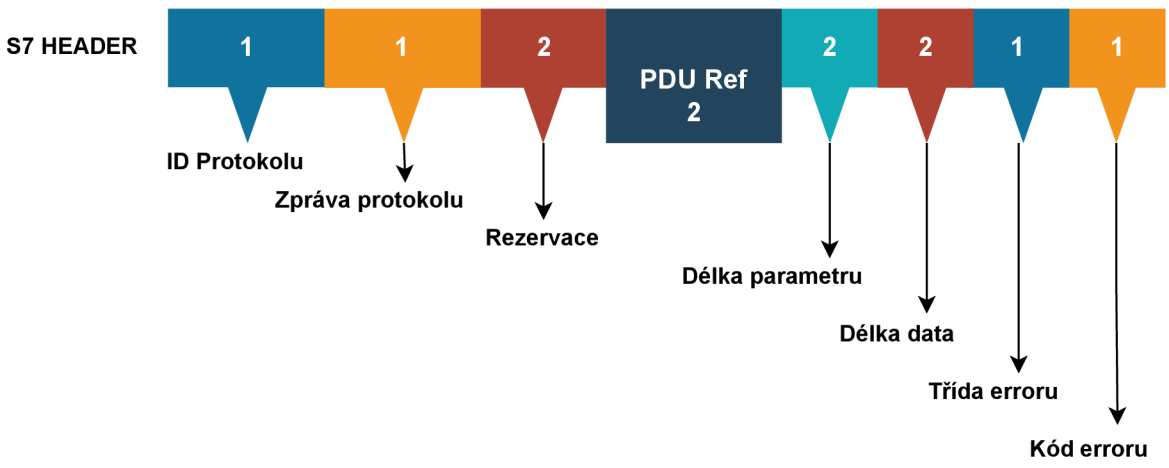
Obr. 2.7: S7-PDU

Záhlaví S7 HEADER

Hlavička se sestává z 10-12 bajtů, potvrzovací zprávy obsahují dva extra errorové bajty viz. obr. 2.8. Mimo to je formát záhlaví stejný pro všechna PDU.[16]

- ID protokolu: [1B] konstanta protokolu je vždy 0x32

- Zpráva protokolu: [1B] obecný typ zprávy
  - 0x01 - Požadavek: zaslaný tzv. masterem (nadřazeným) zařízením, jedná se např. o čtení/zápis paměti, čtení/zápis bloků, start/stop zařízení, nastavení komunikace
  - 0x02 - Ack: Potvrzení zaslané tzv. slave (podřízeným) zařízením bez datového pole
  - 0x03 - Ack-Data: Potvrzení s volitelným datovým polem, obsahuje zpětnou vazbu na požadavek
  - 0x07 - Uživatelská data: Rozšíření původního protokolu, pole parametru obsahuje ID požadavku/zpětné vazby - využívá se pro debugging (ladění programu), bezpečnostní funkce či nastavení času
- Rezervace: [2B] vždy nastavena jako 0x0000
- PDU reference: [2B] generovaný masterem, navýšený s každým novým přenosem, používané pro propojení zpetné vazby a požadavků
  - Little-endian - druh endianity, jedná se o chování SIMATIC WinCC, Step7 a dalších Siemens programů
- Délka parametru: [2B] Délka pole parametru
  - Big-endian - druh endianity
- Datová délka: [2B] Délka datového pole
  - Big-endian - druh endianity
- Třída erroru: [1B] Vyskytuje se pouze v Ack-data, možné errory viz. tabulka 2.1.
- Kód erroru: [1B] Vyskytuje se pouze v Ack-data, výběr errorů viz. tabulka 2.2



Obr. 2.8: Header

Kód erroru	Popis
0x00	Žádná chyba
0x81	Chyba vztahu aplikace
0x82	Chyba definice objektu
0x83	Chyba - k dispozici nejsou žádné zdroje
0x84	Chyba při zpracování služby
0x85	Chyba na zásobách
0x87	Chyba přístupu

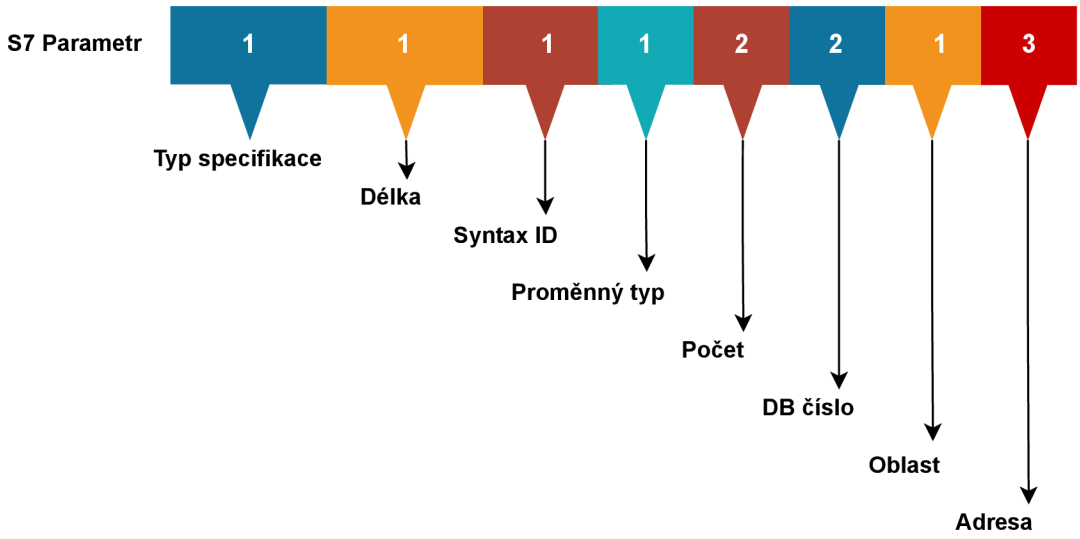
Tab. 2.1: Errory záhlaví

Kód erroru	Popis
0x0000	Žádná chyba
0x0110	Neplatné číslo typu bloku
0x0112	Neplatný parametr
0x011A	Chyba zdroje PG
0x011B	Chyba zdroje PLC
0x011C	Chyba protokolu
0x011F	Uživatelská vyrovnávací paměť je příliš krátká
0x0141	Chyba požadavku
0x01C0	Neshoda verzí
0x01F0	Neimplementováno

Tab. 2.2: Errory parametru

S7 Parametr

V následujícím obrázku 2.9 je vyobrazena struktura parametru S7. [15]



Obr. 2.9: Struktura parametru S7

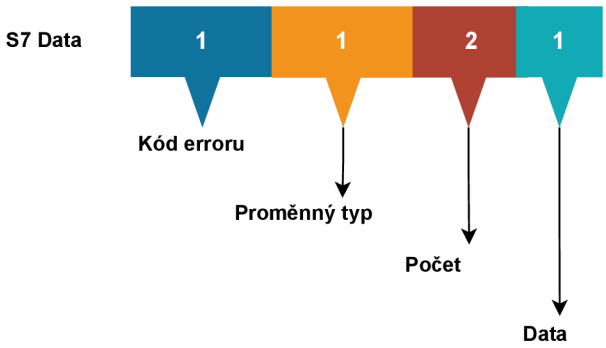
- Typ specifikace: [1B] Vyjadřuje hlavní typ struktury parametru, pro čtení/zápis se využívá hodnota 0x12 což znamená *Proměnná specifikace*
- Délka: [1B] Délka parametru
- Syntax ID: [1B] Vyjadřuje režim adresování a formát zbytku struktury, adresování libovolného typu využívá hodnotu 0x10
- Proměnný typ: [1B] Využívá se při určení typu a délky proměnné
- Počet: [2B] Vyjadřuje možnost zvolení celého pole podobných proměnných pomocí jediné struktury. Tyto proměnné musí mít stejný typ a musí být po sobě jdoucí v paměti a pole určuje velikost. Zpravidla je nastaveno na 1 pro čtení/zápis jedné proměnné.
- DB číslo: [2B] adresa databáze
- Oblast: [1B] Vybírá oblast paměti v adresované proměnné, výběr konstant viz tabulka 2.3
- Adresa: [3B] Obsahuje offset adresované proměnné ve vybrané oblasti paměti. Adresy jsou v podstatě přeloženy na bitové offsety a zakódovány na 3 bajty v síťovém pořadí bajtů (big endian)

Konstanty oblasti paměti	Popis
0x03	Informace o systému rodiny S200
0x05	Systémové příznaky rodiny S200
0x06	Analogové vstupy řady S200
0x07	Analogové výstupy rodiny S200
0x1C	Čítače S7 (C)
0x1D	Časovače S7 (T)
0x1E	IEC čítače (rodina 200)
0x1F	IEC časovače (rodina 200)
0x80	Přímý periferní přístup (P)
0x81	Vstupy (I)
0x82	Výstupy (Q)
0x83	Vlajky (M)
0x84	Datové bloky (DB)
0x85	bloky dat instance (DI)
0x86	Místní data (L)
0x87	Dosud neznámé (V)

Tab. 2.3: Oblasti paměti

S7 Data

Níže je vyobrazena struktura S7 dat viz obr. 2.10. [15]



Obr. 2.10: Struktura dat S7

- Kód erroru: [1B] vrací hodnotu operace, 0xff značí úspěch
- Proměnný typ a počet: [1B 2B] Stejné jako v parametru
- Data: toto pole obsahuje reálnou hodnotu adresované proměnné

2.2.3 Zabezpečení protokolu S7comm

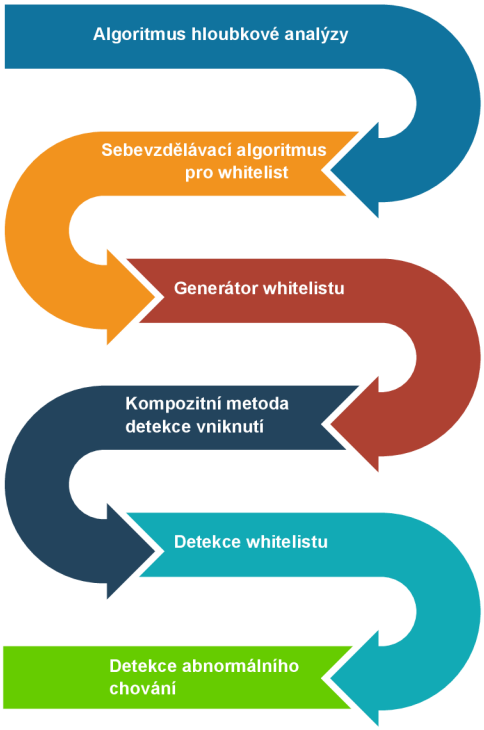
Zabezpečením protokolu S7 se zabývají dvě studie zaměřené na odchycení jakéhokoliv narušení v komunikaci. Protokol S7 je díky jeho vlastnostem, konkrétně jeho proprietaritě a prvotním zapouzdření dat do COTP (Connection-Oriented Transport Protocol - transportní protokol orientovaný na připojení) protokolu, následném zapouzdření do TPKT protokolu a posléze umožnění PDU odeslání dat skrze TCP/IP. Dále se využívá tzv. honeypotu s vysokou interakcí, který chrání komunikaci.

Model detekce vniknutí

Základními síťovými bezpečnostními prvky jsou výrobní firewally a detekční metody. Bezpečnostní prvky jsou spíše pasivní obranou načež detekční metody jsou obranou aktivní. Detekční metody, jak z názvu plyne, aktivně sledují výrobní síť a v případě zjištění jakékoliv abnormality o ní informuje.

Ve své podstatě se dělí na dvě metody - metoda detekce zneužití a metoda detekce anomálií. První zmíněná metoda funguje na principu tzv. blacklistu, což je protokol, který má zabezpečení nastavené na zákazu konkrétních entit, které potenciálně mohou být nebezpečné. Charakteristickým znakem je zaměření na konkrétní hrozby, tzn. je třeba znalost takových hrozeb. Druhá metoda funguje na opačném principu a to na tzv. whitelistu, což je opakem blacklistu. Umožňuje přístup pouze vybraným entitám, které nejsou považované za hrozbu. Z toho vyplývá, že charakteristickým znakem whitelistu je zaměření na důvěryhodné přístupy. Mimo whitelist se metoda detekce abnormality věnuje chování komunikace v systému a opět v případě abnormálního komunikačního chování informuje o takové skutečnosti.

Metoda detekce vniknutí, jak je uvedeno výše, funguje na bázi blacklistů a whitelistů, bohužel i tyto metody mají své nedostatky. Z toho důvodu se využívá výhod obou listů. ICS systémy často využívají statické metody k tvorbě whitelistů. Jsou náročné k nastavení, nejsou dynamické a jsou těžce přenositelné, tzn. v případě přemístění ICS, je třeba vytvořil nový whitelist. Aby se eliminovala náročnost statického whitelistu, studie využila dynamického whitelistu, který se umí sám učit. Díky tomu dokáže vytvářet aktuální whitelisty a přizpůsobovat se změnám. Díky hloubkové analýze umožněné protokolem S7, předchozím algoritmům a metodám vznikne navrhovaný BPID (Based-Protocol Intrusion Detection - Detekce vniknutí založeného na protokol) model viz. obr. 2.11. [30]



Obr. 2.11: Architektura modelu BPID

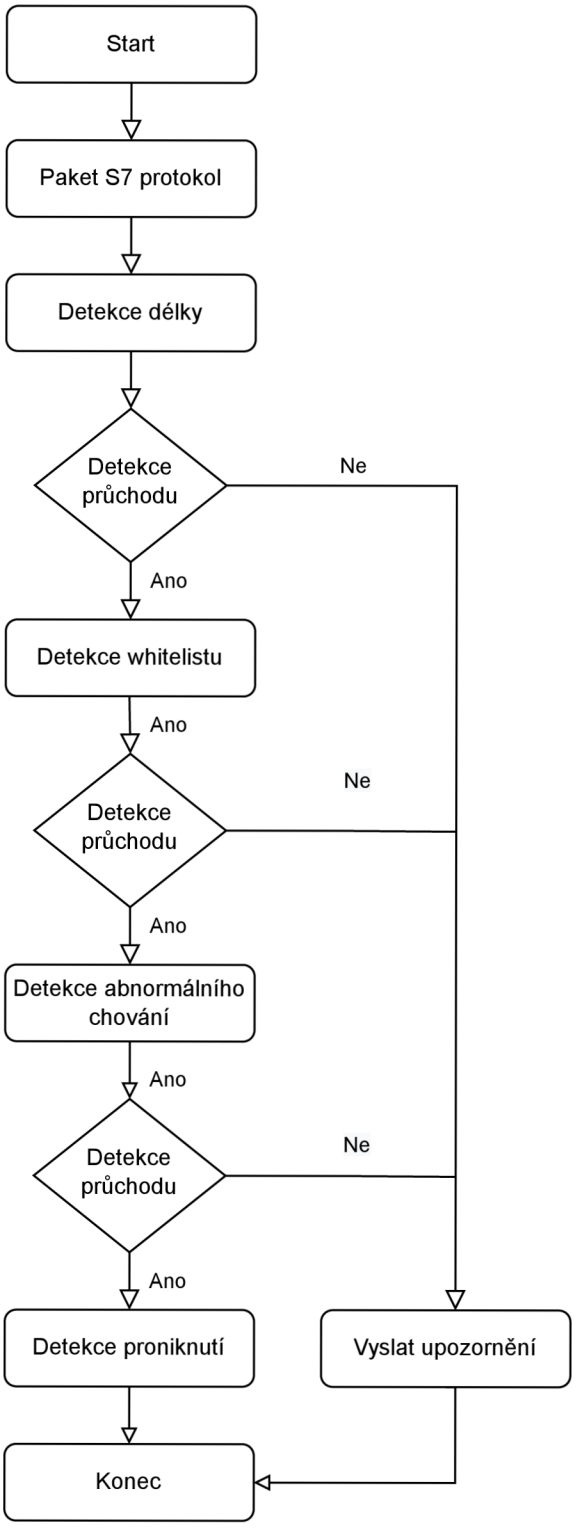
Algoritmus hlubokého učení a jeho obecné techniky rozlišení protokolů se používají k řešení běžných veřejných protokolů, jako je linková vrstva a MAC adres, rozlišení zdrojů a cílů IP adres v síťové vrstvě IP protokolů, rozlišení čísel zdrojového a cílového portu transportních vrstev TCP protokolu a analýzy aplikační vrstvy HTTP protokolu. Co se týče ICS sítě, využívají se spíše soukromé protokoly konkrétního výrobce, jako například S7 ve společnosti Siemens, kde jsou platná data zapouzdřena a přenesena v protokolu aplikační vrstvy.[30]

Algoritmus učení bez učitele referuje na sbírku datových paketů s předpokládaným komunikačním chováním v ICS. V ICS je možnost kontroly stylem, kde se nahraje chování datových paketů a utvoří dočasný whitelist, který se porovná s aktuálním whitelistem, kde v případě nesrovnalosti upozorní na chybu. Z důvodu správné funkce, je nutné aby algoritmus měl svůj časový cyklus k sebevzdělání, následně se naučí normální komunikační datové pakety v ICS (pořád za tohoto cyklu) a na konec utvoří whitelist. Ve stejnou chvíli algoritmus vydává maximální a minimální paketovou délku pro následnou detekci abnormálního paketu. Prvně je datový paket S7 protokolu hluboce analyzován k získání analyzované n-tice pro kontrolu délkových informací paketů.[30]

Kompozitní metoda detekce vniknutí je vyobrazena ve vývojovém diagramu na obr. 2.12. Metoda prvně provádí hloubkovou analýzu na datovém paketu k získání analyzování informací, jako je délka datového paketu, IP adresa síťové vrstvy, číslo

portu pro transportní vrstvu, protokol aplikační vrstvy, funkční pole, adresní pole, datové pole a pole názvu souboru protokolu S7. Následně probíhá detekce správnosti délky paketu aby bylo zabráněno případnému útoku, který by byl konstruován k zablokování kanálu vysíláním příliš dlouhých škodlivých paketů. V případě, že je délka paketu správná, provede whitelist kontrolu. Pokud paket úspěšně projde skrze whitelist kontrolu, znamená to, že formát paketu je správný a následuje detekce abnormálního chování. Jestliže se nepřijde na žádné abnormální chování paketu, vše je v pořádku a není třeba vysílat upozornění. Za situace, kdy by v jedné z kontrolních částí paket neprošel, upozornění je vysláno.[30]

Závěr studie hodnotí výsledky experimentu, které jsou velmi uspokojivé. Detekce vniknutí škodlivého paketu má přesnost zachycení 100 % do 3000 paketů/s. S narůstajícím počtem paketů se zvyšuje riziko průniku skrze detekci (4000 paketů/s - 99,2 %, 4500 paketů/s - 98,5 %, 5000 paketů/s - 98,3 %). Autoři studie podotýkají, že BPID model má určité nedostatky počínaje nemožností model používat univerzálně, jelikož je vázaný k S7 protokolu. [30]



Obr. 2.12: Vývojový diagram kompozitní metody detekce vniknutí

Honeypot s vysokou interakcí

Vzhledem k narůstajícím útokům na ICS se začaly hojně využívat tzv. honeypoty - systémy, které se chovají jako návnada a dokáží přitahovat hrozby. V tomto výzkumu je využit Conpot, který má nizkou interaktivnost, ale poskytuje jednoduchou implementaci ICP (Industrial Control Protocols - Průmyslové Řídící Protokoly), která je výchozí pro simulaci PLC SIEMENS SIMATIC S7 s připojením Modbus a S7comm. Vzhledem k tomu, že Conpot je pouze základním honeypotem, je třeba jej modifikovat a zdokonalit ve třech aspektech, a to v řídících protokolech, HMI a vybavení pro simulaci Siemens S7 PLC. Vylepšením uvedených aspektů zlepšujeme interakci honeypotů pro simulaci PLC a usnadňujeme jejich konfiguraci. Vylepšení Conpotu ve třech aspektech umožňuje simulovat komplexní ICS.[34]

Dynamická interakce HMI zlepšuje přehlednost a dostupnost ke kritickým informacím, které jsou nutné pro konfiguraci a zjištění aktuálního stavu honeypotu. Takový HMI modul je vyobrazen v tabulce 2.4.[34]

Navigace	**Popis a obsah**
Úvod	Vstup na standardní webovou stránku
Úvodní stránka	Obecné informace o CPU
Identifikace	Detailní informace o CPU
Informace o modulu	Modulové informace o místním nosiči
Komunikace	Fyzické charakteristiky a statistické informace síťové adresy a komunikačního rozhraní
Diagnostická vyrovnávací paměť	Vyjímky a diagnostické informace o zařízeních
Proměnný stav	Proměnné CPU a I/O
Datové záznamy	Soubory se záznamy v paměti
Aktualizace firmwaru	Odkaz na aktualizaci firmwaru v CPU

Tab. 2.4: Šablona HMI modulu

Zdokonalení ICS protokolů závisí na analýze S7comm komunikačních paketů za pomocí programu Wireshark. Jak je ve výzkumu zmíněno, principem této analýzy je odeslání datového obsahu COTP balíčku s 0x32 identifikátorem v prvním bajtu. Celá komunikace odpovídá podkapitole 2.2.2 Komunikace S7. Díky odeslání tohoto balíčku bylo možné zlepšit analytickou metodu a zpětnou vazbu S7comm protokolu pro různé funkční struktury Conpotu.[34]

Výsledky studie na základě simulace, která probíhala čtyřicet tři dní, bylo porovnané stejné množství žádostí o identifikaci. Na základě vylepšení jednotlivých aspektů se úspěšnost honeypotu Conpot zvýšila z 81,77% na 98,01% při využití S7-300 PLC. Závěrem výzkumu bylo zhodnoceno, že zlepšení zřetelné, avšak je stále třeba zabezpečení zdokonalovat.[34]

2.2.4 S7comm Plus

Tato nová verze protokolu je vysoce šifrovaná, což znemožňuje analýzu paketů. Neexistuje žádná oficiální dokumentace protokolu a málo nebo žádné informace o něm online.[**?**]

Siemens S7-1200v4.0 a S7-1500 používají tento nový protokol S7CommPlus včetně paketů S7CommPlus Connection a paketů S7CommPlu Function. Všechny pakety používané protokolem S7CommPlus mají podobnou strukturu a má komplexní šifrování vůči opakovanému útoku.[29] S7CommPlus se indentifikuje číslem protokolu 0x72. Existují tři verze S7CommPlus, a to S7CommPlusV1, S7CommPlusV2 a S7CommPlusV3, kde poslední verze se považuje za nejzabezpečenější vůči dvěma předchozím. Třetí verze se využívá výhradně u TIA portálu V13 a výše.

S7comm Plus komunikace

K navázání spojení mezi TIA Portalem a PLC bylo použito třícestné handshake TCP spojení. Po připojení COTP (Connection Oriented Transport Protocol) odešle TIA Portal požadavek na připojení S7CommPlus. První paket S7CommPlus Connection Response obsahuje ID objektu a pole hodnot, které generuje PLC. Při obdržení ID objektu a pole hodnot vypočítá TIA Portal ID relace a blok klíče. Poté se do PLC odešle druhý paket s požadavkem na připojení S7CommPlus obsahující ID relace a blok klíče. Pokud jsou ID relace a blok klíče správné, po ověření PLC bude odeslán paket s odpovědí, aby bylo spojení S7CommPlus dokončeno. Každý paket požadavku funkce S7CommPlus obsahuje část integrity. Část integrity vypočítá TIA Portal pomocí ID relace a pevné hodnoty pole jako vstupního parametru. Když PLC přijme paket S7CommPlus Function Request, bude ověřena integrita části. Paket S7CommPlus Function Response může být odeslán pouze v případě, že ověření bylo správné.[29]

2.2.5 Zabezpečení protokolu S7comm Plus

Nejbezpečnějším dnešním protokolem je S7CommPlusV3 který je používán pouze na nejnovějších TIA portálech a S7-1500 PLC. Podporuje různé operace, které jsou zpracované softwarem TIA portálu, jimiž jsou[1]:

- Start/Stop aktuálně načteného ovládacího programu v paměti PLC
- Stažení řídícího programu do PLC
- Nahrání aktuálního řídícho programu z PLC do TIA portálu
- Čtení hodnoty řídící proměnné
- Upravení hodnoty řídící proměnné

Výše uvedené operace překládá software TIA portálu do S7CommPlus zpráv před tím, než jsou vysílané do PLC. PLC se následně chová dle zpráv, které obdrží, zpracuje řídící operace a provede zpětnou vazbu do TIA portálu. Zprávy jsou přenášeny v relaci, kde každá relace má ID které volí PLC. Relace začíná tzv. handshakem čtyř zpráv, které se používá k výběru kryptografických atributů relace včetně verze protokolu a klíčů. Po handshaku jsou všechny zprávy chráněny integritou využívající kryptografický ochranný mechanismus.[1]

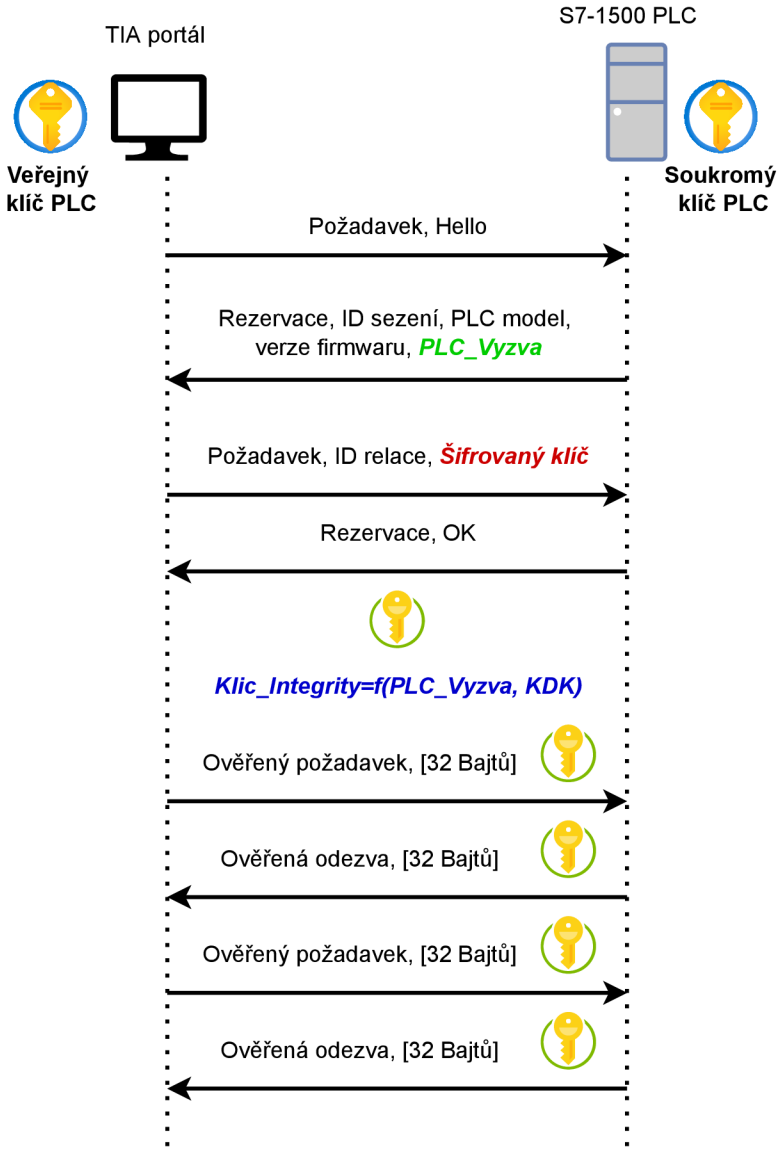
S7 mechanismus ochrany integrity

Siemens integroval kryptografickou ochranu v nejnovějším S7 proprietárním protokolu aby zajistil ochranu PLC před neautorizovanými přístupy. Tento nový mechanismus využívá dva hlavní moduly[1]:

- Protokol výměny klíčů relace, které využívají obě strany (PLC a TIA portál) k zajištění tajného sdíleného klíče pro každé sezení (session).
- Fragmentová ochrana zpráv, která vypočítá hodnotu Message Authentication Code (MAC).

Protokol výměny klíčů

Protokol výměny klíčů byl vylepšen nahrazením procesu generování klíče v předchozí verzi, tj. S7CommPlusV2, složitějším procesem pro novější verze S7CommPlusV3. Tento nový mechanismus zahrnuje novou techniku výměny klíčů na základě veřejného klíče s metodou šifrování založeném na kryptografii nad eliptickými křivkami jak je znázorněno na obr. 2.13.[1]



Obr. 2.13: Mechanismus vzniku relačního klíče S7

První požadavek je tzv. Hello zpráva, kterou TIA portál inicializuje novou relaci. Poté PLC odpoví a sdílí firmware verzi, model, ID relace a konkrétních 20 bajtů známých jako ***PLC_Vyzva***. Verze PLC firmwaru určuje eliptickou křivku při výměně veřejných klíčů. Poté, co TIA portál obdrží druhou zprávu z PLC, aktivuje derivační algoritmus k náhodnému vybrání KDK (key derivation key - klíčový derivační klíč) a generuje klíč relace z ***PLC_Vyzva*** a vybraného KDK. Následně TIA portál vysílá šifrovaný klíč pomocí kryptografické eliptické křivky do PLC skrze třetí zprávu. Třetí zpráva, mimo jiné, obsahuje dvě hlavní části[1]:

- Datová struktura obsahující vybrané šifrované klíče s veřejným klíčem PLC
- Dva osmi bajtové klíčový otisk (přídavný klíč) ID veřejného klíče PLC a vybraného klíče.

Posléze PLC zkontroluje třetí zprávu a v případě, že je kontrola úspěšná, vrátí informaci OK skrze čtvrtou zprávu a odsud veškeré následující zprávy v relaci jsou chráněné integritou s derivačním klíčem relace.[1]

Fragmentová ochrana zpráv

Když TIA portál stáhne/nahraje řídící logický program do/z S7-1500 PLC, přiřazené S7CommPlus zprávy jsou fragmentované do vícero menších fragmentů odeslané skrce TCP/IP pakety. Všechny zprávy zaslané mezi oběma stranami jsou chráněny integritou HMAC-SHA256, což je kryptografický algoritmus hash klíčovaného klíče. Taková ochrana integrity je aplikována na úrovni fragmentace, tzn. nahrazuje hodnotu signálu MAC na konci každé zprávy a kryptografický obsah je umístěn
v každém fragmentu mezi jeho záhlaví a data. Ačkoliv fragmentace S7 zpráv je pro útočníky výzvou, tak tenhle ochranný mechanismus byl prolomen. Útočníci mohli implementovat tzv. man-in-the-middle (prostředníka) přístup a úspěšně zvládli modifikovat síťový provoz na portu 102/TCP kvůli určitým vlastnostem v kalkulaci pro tuto ochranu integrity.[1]

Stahování S7CommPlus zpráv - objekty a atributy

S7 je protokol na bázi odpovědi na požadavek. Každý požadavek zprávy se skládá ze záhlaví požadavku a sady požadavku. Záhlaví obsahuje funkční kód který identifikuje žádanou operaci (např. 0x31 pro stažení zprávy). Jedna S7CommPlus zpráva může obsahovat vícero objektů, kde každý může obsahovat vícero atributů. Všechny objekty a atributy mají unikátní identifikátor třídy. Nicméně požadavek 0x04 (Vytvoření objektu) staví nový objekt v paměti PLC s unikátním ID. Program po stažení zprávy vytvoří objekt třídy tzv. *ProgramCycleObjectBlock*. Tento objekt obsahuje vícero atributů, kde každý z nich má hodnoty určené ke specifickému účelu.

Z pohledu zabezpečení jsou tyto atributy kritické data, která jsou vysílány přes S7CommPlusV3 protokol. Z toho vyplývá, že pokud útočník zachytí S7 pakety obsahující tyto atributy, může je jednotlivě modifikovat a v případě správné modifikace je schopen způsobit zdrojově-binární nesoudržnosti.[1]

3 Knihovna SNAP7

Snap7 je open source, 32bitová nebo 64bitová, multiplatformní ethernetová komunikační sada pro nativní propojení s PLC Siemens S7. Knihovna podporuje částečně i nové CPU 1200/1500, staré S7200, malé LOGO 0BA7/0BA8 a SINAMICS Drives.[26]

Přestože byla navržena tak, aby překonala omezení OPC serverů při přenosu velkého množství vysokorychlostních dat v průmyslových zařízeních, lze ji škálovat i na malé linuxové základní desky nebo mips desky, jako jsou Raspberry PI (1 a 2), BeagleBone Black, pcDuino. , CubieBoard, UDOO a ARDUINO YUN.[26]

Jsou zde tři specializované komponenty, Client, Server a Partner, díky kterým je umožněna definitivní integrace PC systémů do automatizačního řetězce PLC.[26]

Mezi hlavní rysy patří například již výše zmíněný nativní multi-architekturní design, tedy 32bitový nebo 64bitový. Podpora více CPU, jako je Intel a AMD i386/x86(64), ARM, Sun Sparc, Mips. Platformově nezávislý, aktuálně jsou podporovány operační systémy Windows (od NT 4.0 až po Windows 8), Linux, BSD, Oracle Solaris 11, Apple OSX. Plně škálovatelné, počínaje blade servery až po desku Raspberry PI. Žádná závislost na knihovnách třetích stran, není nutná instalace, nulová konfigurace. Tři různé modely nativních vláken pro optimalizaci výkonu: vlákna Win32 / vlákna Posix / vlákna Solaris 11. Dva modely přenosu dat: klasický synchronní a asynchronní. Dva modely toku dat: dotazování a nevyžádané (PLC přenáší data, když chce). Dva specializované porty: Settimino a Moka7, které umožňují komunikovat s PLC S7 s Arduino nebo telefony s operačním systémem Android.[26]

3.1 Snap7 Client

Snap7Client je klient, který splňuje téměř kompletně protokol S7, lze číst/zapisovat celou paměť PLC (In/Out/DB/Merkers/Timers/Counters), provádět blokové operace (upload/download), ovládat PLC (Run/Stop/Compress. .), splňuje bezpečnostní úroveň (Set Password/Clear Password) a téměř všechny funkce, které Simatic Manager nebo Tia Portal umožňuje.[26]

Knihovna Snap7 je navržena s ohledem na velké průmyslové časově kritické datové přenosy zahrnující sítě s desítkami PLC. Snap7Client obnáší tři zajímavé funkce: nezávislost PDU, SmartConnect a asynchronní přenos dat.[26]

3.1.1 Nezávislost PDU

Každý datový paket vyměňovaný s PLC se musí vejít do jednotky PDU, jejíž velikost je pevná a pohybuje se od 240 do 960 bajtů.[26]

Všechny funkce Snap7 tento koncept zcela skrývají, data, která lze přenést v jediném přenosu, závisí pouze na velikosti dostupných dat.[26]

Pokud tato velikost dat překročí velikost PDU, paket se automaticky rozdělí na více přenosů.[26]

3.1.2 SmartConnect

Při připojování k serveru musí být splněny v zásadě dva požadavky.[26]

1. Hardware musí být zapnutý.[26]

2. Musí být spuštěn serverový software naslouchající danému připojení.[26]

Pokud lze „pingnout“ PLC, tak je téměř jisté, že připojení bude úspěšné. Funkce SmartConnect spoléhá na tento princip, aby se zabránilo vypršení časového limitu připojení TCP, když je PLC vypnuto nebo je odpojen síťový kabel. Na rozdíl od časového limitu připojení TCP je doba pingu pevná a lze ji nastavit.[26]

Když je zavolána funkce CliConnectTo() (funkce připojení klienta k PLC), nebo když se aktivní Snap7Partner potřebuje připojit, nejprve je PLC „pingnuto“, a pokud byl výsledek pingu v pořádku, je provedeno TCP spojení.[26]

Snap7 k tomu používá dva různé způsoby v závislosti na platformě:

Windows – Je použita systémová knihovna iphlpapi.dll, která se načítá dynamicky, protože není oficiálně podporována společností Microsoft (i když je přítomna na všech platformách a je plně zdokumentována MSDN). Pokud selže jeho načtení (velmi vzácný případ), vytvoří se ICMP soket pro provedení pingu. Používá se jako plán B, protože potřebujeme oprávnění správce k vytváření soketů RAW ve Windows Vista/Windows 7/Windows 8.[26]

Unix (Linux, BSD, Solaris) - Od verze 1.3.0 se používá asynchronní (s časovým limitem) připojení TCP, takže práva root nejsou potřeba.[26]

Během inicializace knihovna zkontroluje, zda lze ping provést pomocí výše uvedených metod. Pokud všechny selžou, SmartConnect je deaktivován a všichni vytvoření klienti (nebo aktivní partneři) se pokusí připojit přímo.[26]

Výpis 3.1: Příklad SmartConnect

```
while (!TerminateCondition())
{
    if (Client->Connected())
    {
        PerformDataExchange())
        sleep(TimeRate);
    }
    else
        if (Client->Connect()!=0)
            sleep(10);
}
```

Na výpisu 3.1 lze vidět příklad SmartConnect. sleep(TimeRate) značí interval doby výměny dat. sleep(10) značí dobu zotavení, v Unixu se místo sleep používá nanosleep(). Předpokládá se, že TerminateCondition() je funkce typu boolean, která vrátí hodnotu true, když je třeba vlákno ukončit.[26]

3.1.3 Asynchronní přenost dat

Synchronní funkce se provádí ve stejném vláknu přenosu, tj. ukončí se pouze po dokončení úlohy. Synchronní funkce se často nazývají blokovací funkce, protože blokují provádění programu volajícího.[26]

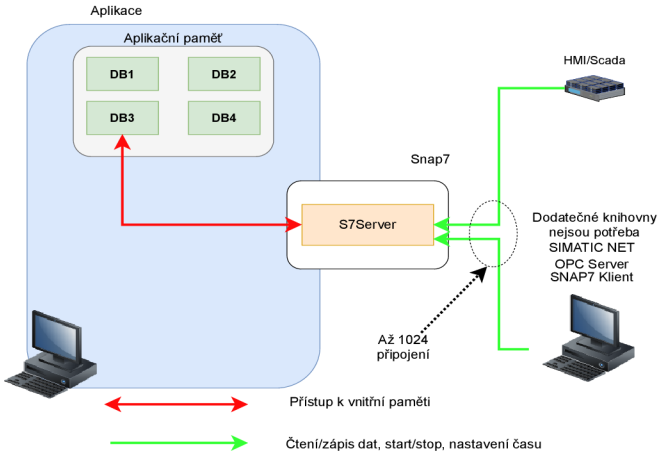
Asynchronní funkce naproti tomu se skládá ze dvou částí, z nichž první část se provádí ve stejném vlákně přenosu, který připravuje data (pokud existují), spouští druhou část a okamžitě se ukončí. Druhá část se provádí v samostatném vláknu a provádí tělo požadované úlohy současně s prováděním volajícího programu. Tato funkce se také nazývá neblokování.[26]

Volba použití jednoho nebo druhého modelu v podstatě závisí na dvou faktorech:

1. Jak moc je paralelní úloha granulární, než aktivita CPU.[26]
2. O kolik je doba provádění úlohy větší než režie způsobená synchronizací.[26]

3.2 Snap7 Server

Snap7Server je jednodušší objekt k použití. Snap7Server není ani druh OPC serveru ani program, který sbírá data z PLC a prezentuje výsledky. Snap7Server, stejně jako komunikační procesor (CP), přijímá připojení S7 externími klienty a odpovídá na jejich požadavky.[26]



Obr. 3.1: Příklad Snap7 Serveru

Mechanismus je velmi jednoduchý. Program přidělí paměťový blok a řekne serveru „toto je DB3“. Pokaždé, když klient požaduje čtení/zápis nějakého bajtu z/do DB3, server tento blok použije. Pokud klient požaduje přístup k neexistujícímu bloku (tj. bloku, který nebyl sdílen), server odpoví chybou "zdroj nenalezen", stejně jako by to udělalo skutečné PLC.[26]

3.3 Snap7 Partner

Smart7Partner umožňuje vytvořit S7 peer-to-peer komunikaci.[26]

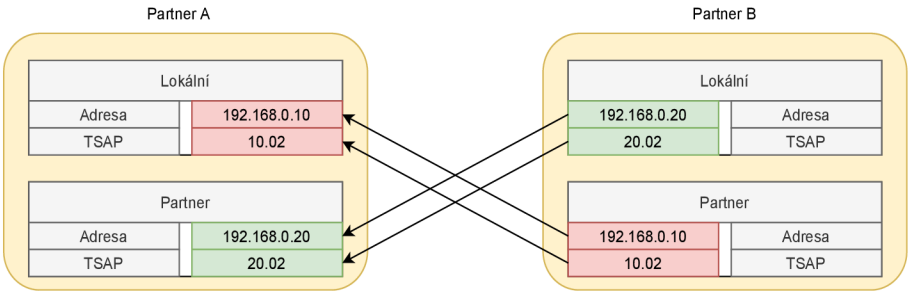
3.3.1 Siemens model

Na rozdíl od modelu klient-server, kde klient zadá požadavek a server na něj odpoví, model peer-to-peer vidí dvě komponenty se stejnými právy, z nichž každá může odesílat data asynchronně. Jediný rozdíl mezi nimi je ten, kdo o spojení žádá. [26]

Partner, který požaduje připojení, se nazývá aktivní. Partner, který připojení přijímá, se nazývá pasivní. Po navázání spojení mohou odesílat nevyžádaná data. Protokol S7 je příkazově orientovaný a příkazy jsou obvykle prováděny serverem. Partneři komunikují prostřednictvím protokolu S7, pomocí netypovaného telegramu „segmented data send“. Nejedná se striktně o příkaz, jedná se to přenos dat, který používá mechanismus potvrzení protokolu S7. Ve skutečnosti jej pár klient-server nerozpozná. [26]

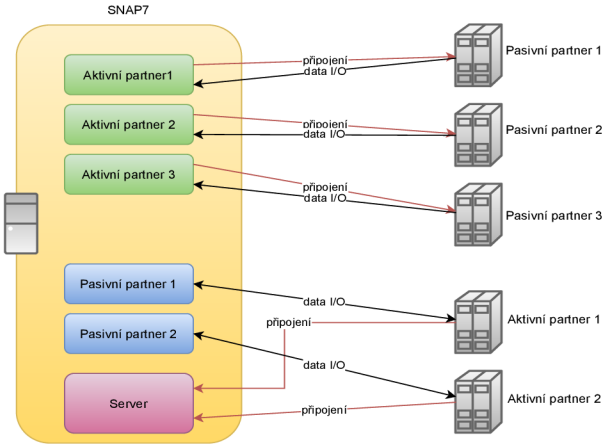
Komunikace není plně asynchronní, tj. neexistuje žádný mechanismus přerušení, který by příjemci řekl, že paket přichází: partner, který paket přijímá, musí naslouchat prostřednictvím funkce Block Recv. Pokud jsou dva PLC systémy umístěny ve stejném projektu, Simatic Manager může sledovat připojení, v opačném případě

budou mít oba blíže nespecifikovaného partnera. Ale z hlediska přenosu dat v tom není žádný rozdíl. Ke komunikaci potřebuje každý znát své vlastní souřadnice sítě S7 a souřadnice toho druhého: IP adresu a TSAP.[26]



Obr. 3.2: Siemens model Snap7 Partnera

3.3.2 Snap7 model



Obr. 3.3: Snap7 model Snap7 Partnera

Model Snap7 následuje model Siemens s některými výhodami. Není potřeba žádná konfigurace připojení. [26] Dva modely odesílání dat: Asynchronní se třemi modely dokončení. Synchronní - volající je blokován do odeslání dat.[26] Dva modely příjmu dat: Asynchronní - zpětné volání je vyvoláno při příchozím paketu. Synchronní - volání BRecv stejně jako pomocí FB13.[26] Když se vytváří partner, je nutné specifikovat jeho typ: Aktivní nebo Pasivní, jejich chování, jak je vysvětleno v modelu Siemens, je odlišné. Jakmile je typ partnera vytvořen, nelze žádným způsobem změnit.[26] Aktivní partner: Chová se jako klient. Požaduje připojení k pasivnímu partnerovi a čeká na potvrzení připojení. Lze vytvořit, kolik partnerů

je požadováno, a spojit je s jejich pasivním protějškem.[26] Pasivní partner: Chová se jako server. Čeká na žádost o připojení a naslouchá portu IsoTCP.[26]

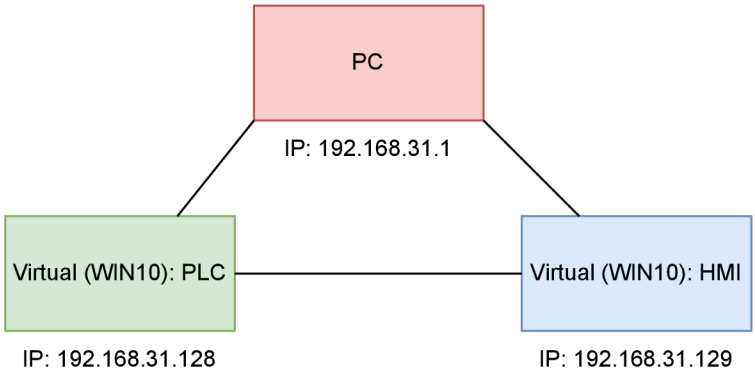
4 Komunikace pomocí knihovny SNAP7

Pracoviště pro komunikaci byly vytvořeny ve dvou verzích kde každá verze využívá různé operační systémy. Jedná se konkrétně o operační systém Windows a Linux. První verze běží ve virtualizovaném prostředí s operačním systémem Windows. Druhá verze emulace funguje na samostatném zařízení Raspberry Pi fungujícím na operačním systému Linux. Následně je řešen průběh komunikace mezi PLC a HMI.

4.1 Pracoviště

Obrázek 4.1. zobrazuje schéma zapojení komunikace mezi virtuálními stroji s operačním systémem Windows 10. Jeden stroj představuje PLC a druhý HMI.

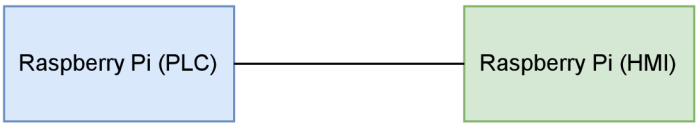
Virtuální stroje běží na fyzickém stolním PC. K virtualizaci operačních systému Windows 10 bylo využito programu VMWare. Na každém stroji byl potřeba nastavit Vnet, tedy síťové rozhraní VMWare. Po nastartování strojů a následném přihlášení bylo nainstalováno Visual Studio pro práci na HMI a PLC.



Obr. 4.1: Schéma zapojení virtuálních strojů.

Obrázek 4.2. zobrazuje schéma zapojení komunikace mezi dvěma Raspberry Pi. Jedno představuje PLC a druhé HMI.

Schéma zapojení Raspberry PI je oproti schématu zapojení virtuálních strojů odlišné. Komunikace zde probíhá striktně mezi sebou a tudíž nevyžadují žádného prostředníka, který by zpracovával tuto komunikaci, jak tomu bývá u virtuálních strojů. Pro sériovou komunikaci je použit RJ-45 kabel mezi zařízeními Raspberry Pi 3 Model B+ na typu OS Raspbian.



Obr. 4.2: Schéma zapojení Raspberry Pi.

4.2 Souhrn použitého hardwaru a softwaru

V tabulce 4.1 je vyobrazení specifikace použitého hardwaru pro jednotlivé zařízení, a to virtualizovaného stroje Win10 a Raspberry Pi. Pro virtualizovaný stroj byla vyčleněná paměť z RAM PC.

Specifikace	Virtualizovaný stroj Win10	Raspberry Pi
Procesor	AMD Ryzen 3700X	ARM Cortex-A53
Grafická karta	nVidia RTX 3080	-
Paměťové moduly	4 GB	1 GB

Tab. 4.1: Specifikace Hardwaru

V tabulce 4.2 je seznam softwaru použitý při vytvoření PLC a HMI. Kód byl napsán v programovacím jazyce C#, pro Windows byl zkompilován pomocí programu Visual Studio a pro Raspberry Pi přes software Mono.

Virtualizovaný stroj Win10	Raspberry Pi
Visual Studio 17.1	-
-	Mono 5.18
Wireshark 3.6.5	-
SNAP7 v1.4.2	SNAP7 v1.4.1
C#	C#

Tab. 4.2: Specifikace Softwaru

4.3 Průběh komunikace

4.3.1 Instalace

Komunikace v rámci virtuálních strojů probíhala skrze fyzický počítač. Nejdříve bylo potřeba nastavit vzájemný síťový dosah mezi oběma virtuálními stroji. Tedy nastavení výchozí brány a pevných adres IP.

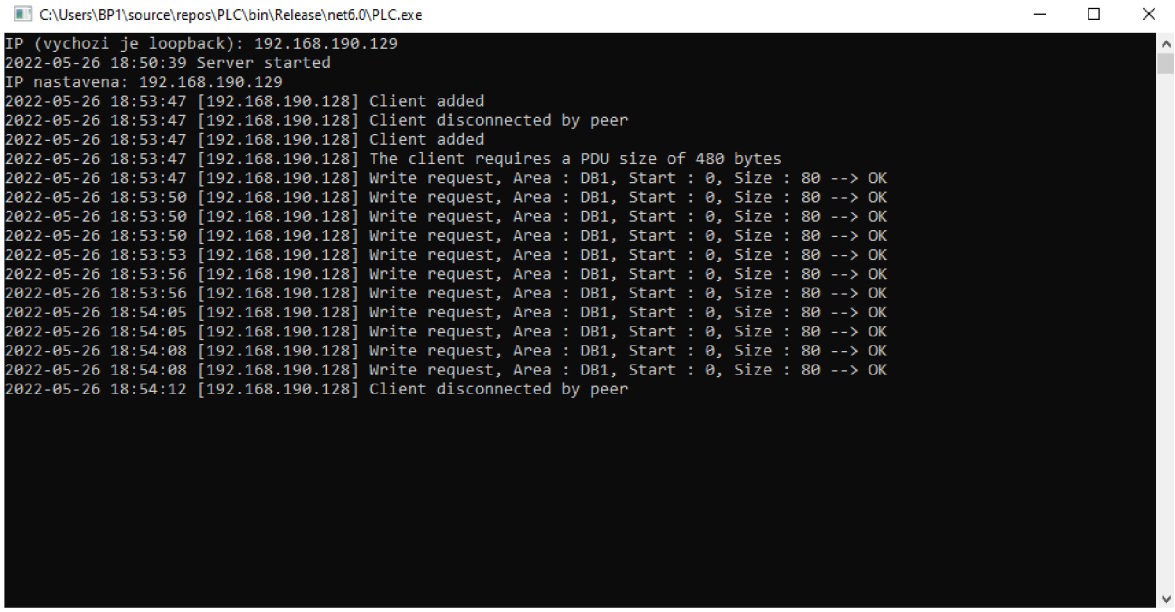
K samotnému vytvoření PLC bylo potřeba stáhnout Visual Studio ze stránek Microsoft, knihovnu Snap7 s rozšiřující knihovnou snap7.dll. Verze Snap7 knihovny je 1.4.2. Tyto knihovny zajišťují správnou funkčnost programu jakožto virtuální PLC. Program má podobu konzole, která oznamuje základní události PLC (připojení/odpojení klienta, zápis do data bloku a podobné).

Pro HMI bylo také využito Visual Studio a knihovna Sharp7. Tato knihovna představuje ekvivalent klienta SNAP7. U HMI nebylo potřeba využít žádné další rozšiřující knihovny.

V rámci komunikace mezi dvěma Raspberry Pi bylo potřeba dodatečně nainstalovat software Mono. Tento program zajišťuje spuštění aplikací vytvořených v programovacím jazyce `C#` a .NET pod unixovými operačními systémy. Místo rozšiřující knihovny snap7.dll muselo být použito ekvivalentu libsnap7.so, jelikož knihovny typu dll nejsou podporovány v jiných operačních systémech, než je Windows. Vzhledem k tomu, že Mono používá vlastní nástroj ke kompilaci kódu, tak bylo potřeba upravit určité části kódu. Jedna z úprav zahrnovala specifikovat použití knihoven, jako je System.Drawing. Visual Studio samo o sobě nepotřebuje některé knihovny definovat, protože při vytváření projektu lze specifikovat, jaký programovací jazyk a platforma bude použita. Podle těchto parametrů Visual Studio definuje základní knihovny automaticky. Další úpravou bylo sjednocení spouštěcí funkce Main do jednoho souboru společně s kódem HMI.

4.3.2 PLC

Po spuštění PLC je třeba zadat adresu IP, na které bude naslouchat. Ve výchozím nastavení je použita IP localhost, tedy 127.0.0.1. Při zadání špatné (např. neexistující) IP adresy dojde k chybě, kdy nelze spustit PLC. V takovém případě je třeba spustit program znovu a zadat správnou adresu. Po zadání adresy je PLC připraveno a není třeba na něm nic nastavovat. PLC, jak je výše zmíněno, oznamuje události, které se v něm dějí. Například přípojení a odpojení klienta, velikost PDU, zápis do data bloku, čtení z data bloku. Do PLC se nezapisují žádné příkazy, po zadání jakéhokoliv znaku dojde k vypnutí.



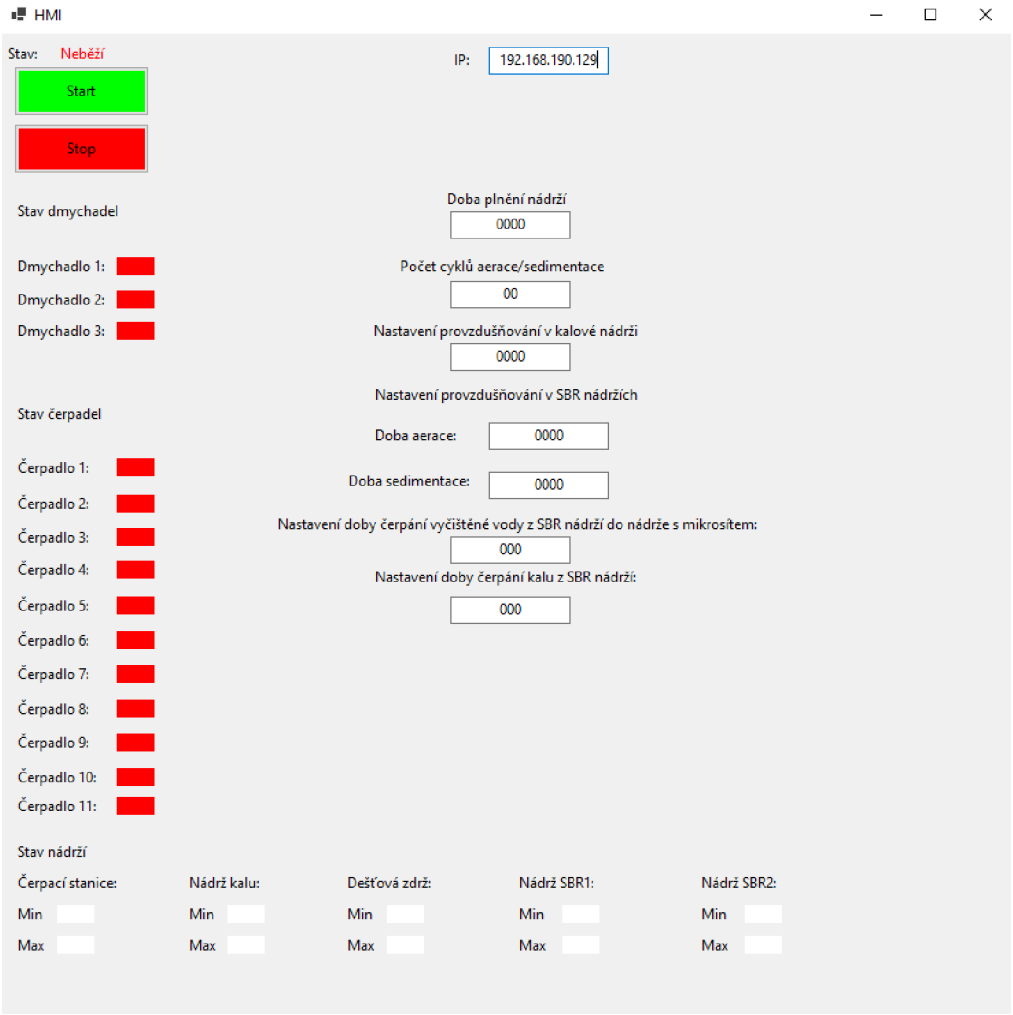
Obr. 4.3: Spuštěný program představující PLC naslouchající na IP adrese 192.168.190.129.

Na obrázku 4.3 je vidět program představující PLC, na němž je nastavena IP adresa 192.168.190.129. Lze si všimnout, že obrázek demonstruje připojení klienta a jak je vysvětleno v části 3.1.1, vyžaduje klient velikost PDU v rozmezí od 240 do 960 bajtů. V tomto případě je to 480 bajtů. Dále lze vidět určitou akci, která představuje zápis do data bloku. Tento akce vždy sdělí o jakou oblast, tedy data blok, se jedná. Dále počáteční bod a velikost zápisu. Veškerá komunikace s PLC probíhá zápisem do tzv. bufferu. Tento buffer představuje změny stavů senzorů, čerpadel. Jedná se tedy o číselný buffer o velikosti 80 míst. Hodnota je buď 0 (stav vypnuto) nebo 1 (stav zapnuto). Celý buffer se posílá vždy s každým zápisem do data bloku. Slouží tedy i jako aktualizace hodnot, v případě, kdyby se útočník pokusil data změnit.

4.3.3 HMI

Na obrázku 4.4 je vidět vizuálně celé HMI na platformě Windows. Stav zobrazuje, jestli je HMI připojení k PLC nebo není. Do kolonky IP se vloží adresa IP daného PLC, se kterým chceme navázat komunikace. Poté je nutné zadat parametry, jako je doba plnění nádrží, počet cyklů aerace a sedimentace, provzdušňování v kalové nádrží a SBR nádržích. Dále nastavení doby čerpání vyčištěné vody ze SBR nádrží do nádrže s mikrosítem a nastavení doby čerpání kalu ze SBR nádrží. Každý parametr má vlastní rozmezí. Po kliknutí na tlačítko Start se v případě správně nastavené IP adresy a všech parametrů, program spustí. V opačném případě dojde k chybě, která

vizuálně navede uživatele k opravě. Po spuštění dojde ke spuštění simulace, která je popsána v sekci Funkcionalita.



Obr. 4.4: HMI připraveno k simulaci.

Popis kódu

Nejdříve se v hlavní třídě definuje S7Client pomocí S7Client SNAP7 = new S7Client(). Tato funkce byla použita ze třídy Sharp7 a zajišťuje veškerou komunikaci s PLC. Klient je nastaven a je třeba si vytvořit proměnné, které představují nádrže. Při spuštění programu se spustí funkce Main, skrz kterou se spustí funkce Form1, která zajistí, že se zobrazí HMI. Po kliknutí na tlačítko Start se spustí funkce `button1_Click`, ve které je vložena celá struktura programu. Nejdříve dojde k získání číselných hodnot z parametrů z textových polí (textBox) přes int.Parse(textové pole). Dále dojde k definování podmínek pro rozmezí hodnot zadaných parametrů. Příklad takové podmínky zobrazuje výpis 4.1, kde t1 představuje získanou číselnou hodnotu z textového

pole a label5 představuje pole pro vložení popisků nebo různého textu.

Výpis 4.1: Podmínka pro rozmezí parametru

```
if (t1 <= 0 || t1 >= 6)
{
    label5.ForeColor = Color.Red;
    label5.Text = "Nastala␣chyba:␣Cykly␣aerace/sedimentace
␣␣␣␣může␣být␣v␣rozmezí␣1-5";
}
```

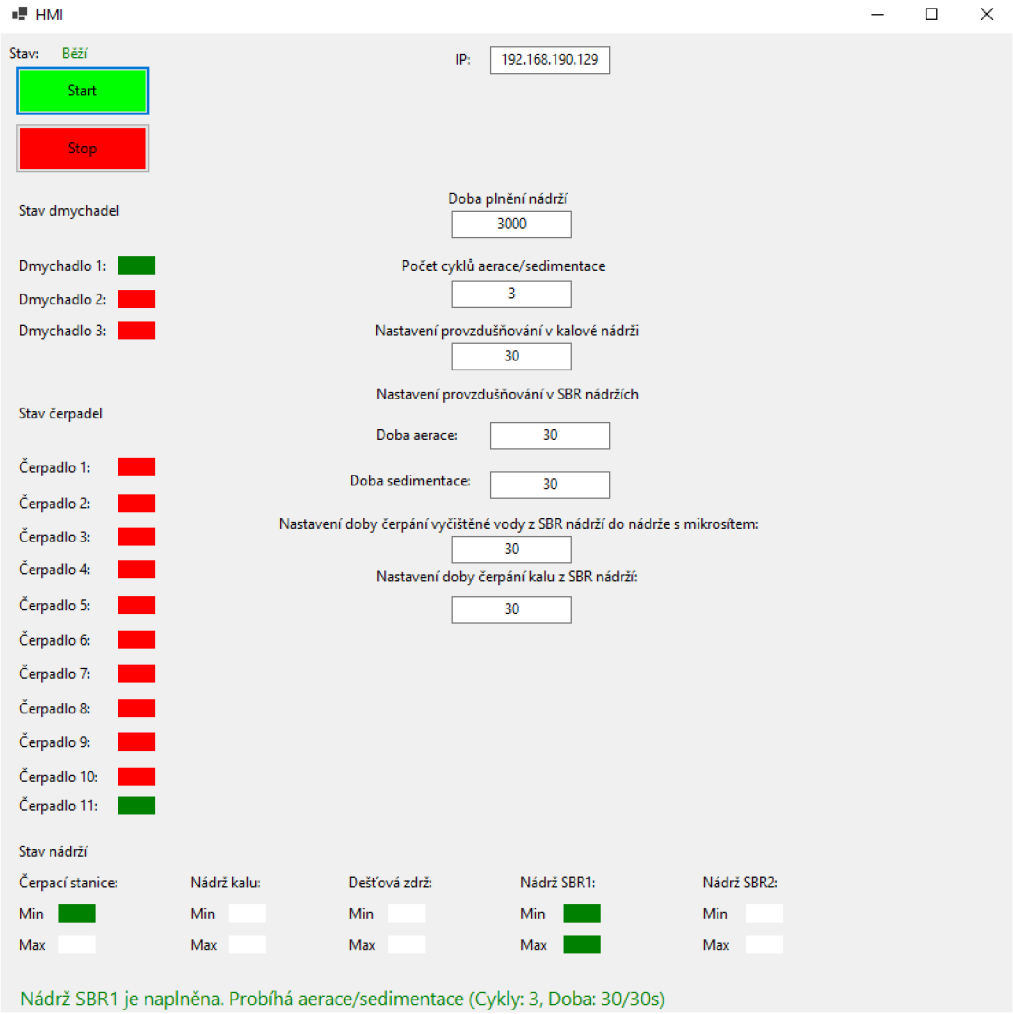
V případě splnění podmínek dojde k připojení k PLC skrze SNAP7.ConnectTo(`IP_adresa_PLC`, Rack, Slot). V tomto případě to Rack bude vždy 0 a Slot vždy 1. Poté dojde k definovaní bufferu s velikostí 80. Tato velikost stačí pro pokrytí všech čerpadel a senzorů. Nechybí ani podmínka pro kontrolu úspěšnosti připojení k PLC. Pokud připojení bylo neúspěšné, dojde k vypsání chyby v kolonce Stav za pomocí SNAP7.ErrorText(connect). Při úspěšném připojení dojde ke spuštění podmínky while, která má hodnotu true. To zajistí, že simulace se bude neustále opakovat. V podmínce while už dochází k simulaci čerpadel a senzorů. Příklad prvního spuštění čerpadla je vyobrazen ve výpise 4.2, kde S7.SetIntAt představuje zápis to bufferu. Parametr buf představuje buffer, v tomto případě je vyplněn samými hodnotami 0. Druhý parametr říká, že zápis hodnoty bude na pozici 10 a třetí parametr zajistí hodnotu, která bude zapsána, tedy v bufferu na pozici 10 bude zapsána hodnota 1. Dále SNAP7.DBWrite má 4 parametry, číslo databáze, startovací bod, velikost a buffer. Velikost musí být menší nebo stejná, jako samotný buffer. Zpozdeni je vytvořená funkce, která umožňuje simulovat dobu plnění nádrží. t7 jako parametr je číselná hodnota zadaná uživatelem v kolonce doba plnění nádrží. Všechny ostatní čerpadla i senzory fungují obdobně. O každé změně je informováno PLC zápisem do data bloku. V případě zvolení tlačítka Stop dojde k vyvolání funkce `button1_Click_1`

Výpis 4.2: Spuštění čerpadla 11

```
// Čerpadlo 11
label68.BackColor = Color.Green;
S7.SetIntAt(buf, 10, 1);
SNAP7.DBWrite(1, 0, buf.Length, buf);
label5.Text = "Čerpání␣vody␣z␣nádrže.";
Zpozdeni(t7);
```

V případě zvolení tlačítka Stop dojde k vyvolání funkce `button1_Click_1` a dojde k odpojení od PLC pomocí funkce SNAP7.Disconnect(). Dále dojde k restartování celé aplikaci, aby se zajistilo vynulování všech čerpadel a senzorů. Tím je

zajištěný plynulý chod simulace pro další spuštění.



Obr. 4.5: Průběh simulace pomocí HMI.

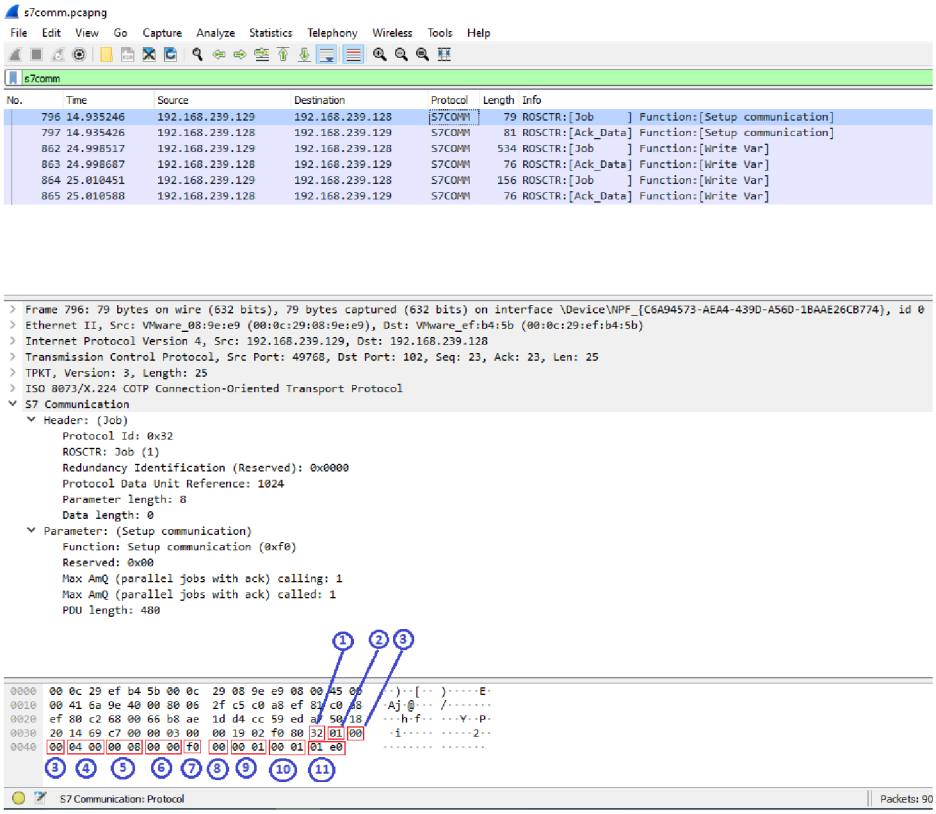
Popis funkcionality

Ihned po spuštění běhu programu pomocí HMI se začne automaticky napouštět voda z hlavní nádrže do čerpací stanice pomocí čerpadla 11. Napouštění se spouští pomocí tlačítka Start. Jakmile optický senzor detekuje minimální hladinu vody v čerpací stanici, dojde k napouštění nádrže SBR1 pomocí čerpadla 1. Společně s napouštěním nádrže SBR1 je spouštěno provzdušňování této nádrže pomocí dmychadla 1. Plnění nádrže SBR1 trvá do sepnutí plovákového senzoru, který slouží k detekci maximální hladiny vody. Po sepnutí je spuštěn určitý počet cyklů aerace a sedimentace, kdy se v časových intervalech střídá provzdušňování pomocí dmychadla 1 a sedimentace, kdy dochází k usazování kalu na dno nádrže. Po provedení všech cyklů je vyčištěná

voda z nádrže SBR1 odčerpávána do dešťové zdrže, která zastává roli v rámci simulace i nádrže s mikrosítem. Čerpání do dešťové zdrže z nádrže SBR1 je provedeno pomocí čerpadla 3. Po přečerpání vyčištěné vody do dešťové zdrže je spuštěno čerpání kalu z nádrže SBR1 do nádrže s kalem pomocí čerpadla 5. Společně s čerpáním kalu do nádrže s kalem je spuštěna aerace této nádrže pomocí dmychadla 3. Po přečerpání kalu do nádrže s kalem je jeden cyklus čištění ukončen a dojde k napouštění nádrže SBR2 z čerpací stanice pomocí čerpadla 2. Napouštění trvá do sepnutí plovákového senzoru pro detekci maximální hladiny vody v nádrži SBR2. Zároveň s napouštěním je nádrž provzdušňována pomocí dmychadla 2. Vzhledem k tomu, že se nachází v dešťové zdrži voda z předešlého cyklu a je jí dostatek pro detekci minimální hladiny pomocí optického senzoru, je pomocí čerpadla 9 přečerpávána z dešťové zdrže do čerpací stanice. Po napuštění nádrže SBR2 a tím sepnutí plovákového senzoru pro detekci maximální hladiny vody je spuštěn opět určitý počet cyklů aerace a sedimentace stejně, jako tomu bylo u nádrže SBR1. Po provedení všech cyklů je z nádrže SBR2 odčerpána vyčištěná vody do dešťové zdrže pomocí čerpadla 4. Po přečerpání vyčištěné vody je spuštěno čerpání kalu z nádrže SBR2 do nádrže s kalem pomocí čerpadla 6. Společně s čerpáním kalu je je spuštěna aerace nádrže s kalem pomocí dmychadla 3. Po přečerpání kalu z nádrže SBR2 je druhý cyklus čištění dokončen. Následně dojde k vypouštění. Dojde tedy k plnění nádrží SBR1 a SBR2 z čerpací stanice pomocí čerpadla 11 a čerpadla 2. Zároveň jsou tyto nádrže plněny vodou z nádrže s kalem pomocí čerpadla 7 a čerpadla 8. Z nádrží SBR1 a SBR2 je voda přečerpávána do dešťové zdrže pomocí čerpadla 3 a čerpadla 4. Z dešťové zdrže je potom voda čerpána do hlavní nádrže pomocí čerpadla 10. Tato čerpadla čerpají tak dlouho, dokud optické senzory pro detekci minimální hladiny vody nedetekují hladinu vody. Následně je simulace dokončena a dochází k vypouštění všech nádrží. Po vypuštění všech nádrží dochází k opakování simulace. Opakování lze zastavit pomocí tlačítka Stop.

5 Analýza protokolu S7

Na obrázku 5.1 je snímek z programu Wireshark zobrazující zajištění komunikace mezi HMI a PLC. Zvýrazněné a číselně označené kódy jsou popsány v tabulce 5.1. Chování jednotlivých částí je specifikováno v kapitole 2.2.2.

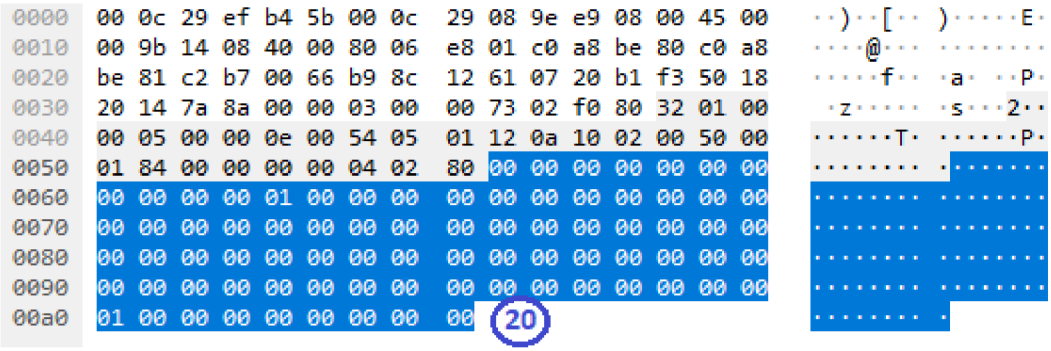


Obr. 5.1: Zachycení komunikace S7comm - setup.

Číslo pole	Popis	Číslo pole	Popis
①	ID protokolu	⑦	Funkce
②	ROSCTR	⑧	Rezervace
③	Identifikace redundance	⑨	MaxAmQ
④	PDU reference	⑩	MaxAmQ
⑤	Délka parametru	⑪	Délka PDU
⑥	Délka dat	-	-

Tab. 5.1: Rozbor záhlaví a parametru setupu

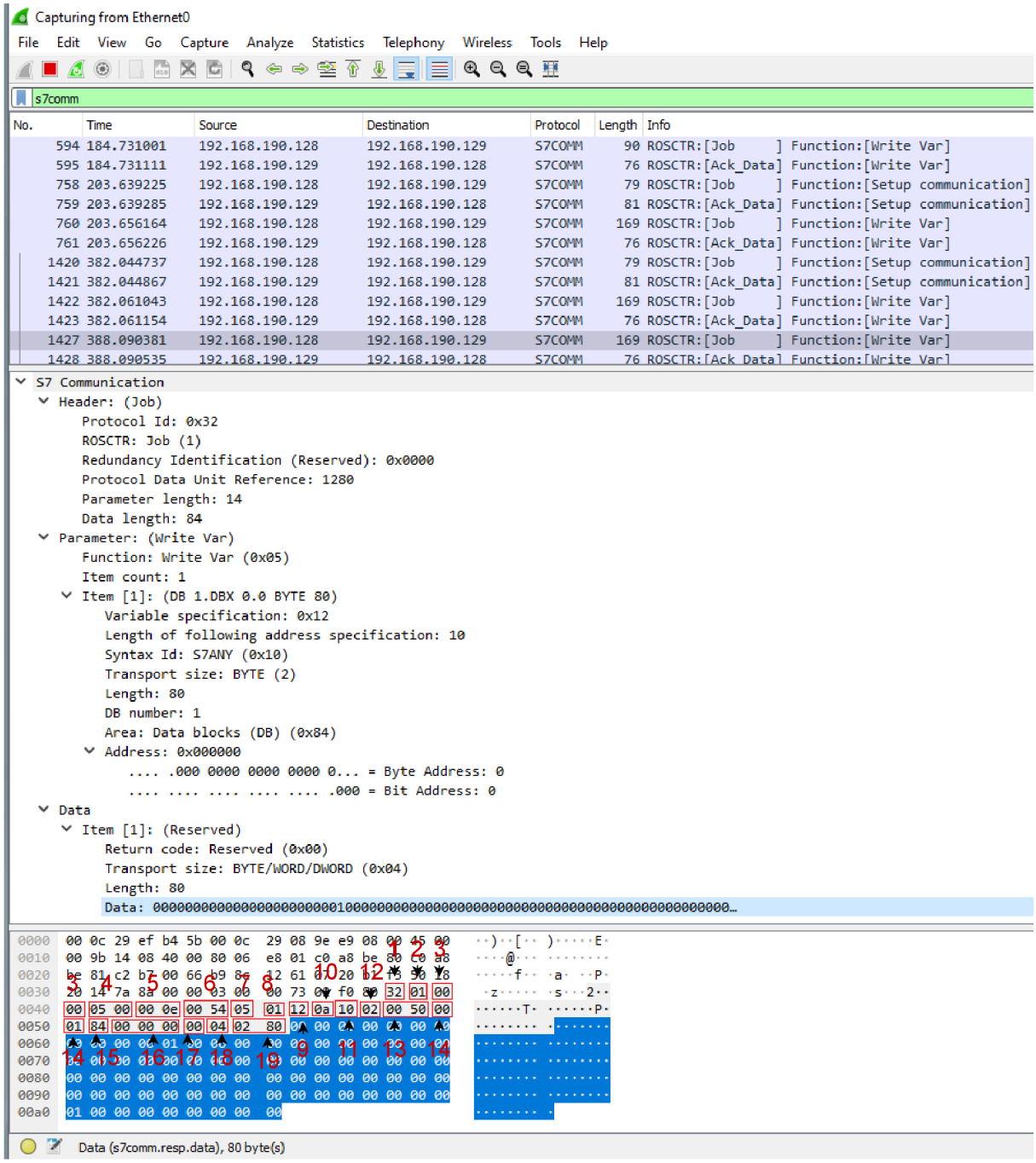
Na obrázku 5.3 je snímek z programu Wireshark zobrazující komunikaci mezi HMI a PLC. Takto zobrazená komunikace je detailně prozkoumaná a po vyhodnocení nedošlo k žádné chybě při přenosu. Zvýrazněné a číselně označené kódy jsou popsány v tabulce 5.2. Chování jednotlivých částí je specifikováno v kapitole 2.2.2. Na obrázku 5.2 jsou detailně vyobrazeny data přenášená mezi PLC a HMI která vyjadřují aktuální stav PLC, např. zda-li je zapnuté čerpadlo. Tato data vzniknou v případě, kdy je po úspěšném připojení HMI k PLC odeslán paket obsahující informace. Znalí útočníci by mohli identifikovat tyto informace a následně je modifikovat k narušení komunikace a případnému selhání.



Obr. 5.2: Přenášená data

Číslo pole	Popis	Číslo pole	Popis
(1)	ID protokolu	(11)	ID Syntaxe
(2)	ROSCTR	(12)	Velikost transportu
(3)	Identifikace redundance	(13)	Délka
(4)	PDU reference	(14)	Číslo DB
(5)	Délka parametru	(15)	Oblast
(6)	Délka dat	(16)	Adreas
(7)	Funkce	(17)	Vrácení kódu
(8)	Počet předmětů	(18)	Velikost transportu
(9)	Proměnná specifikace	(19)	Délka
(10)	Délka specifikace adresy	(20)	Data

Tab. 5.2: Rozbor záhlaví, parametru a dat Write var



Obr. 5.3: Zachycení komunikace S7comm - zápis.

Závěr

Cílem bakalářské práce bylo nastudovat a popsat problematiku průmyslových sítí. Popsat automatizační pyramidu, všechny její úrovně. Rozebrat uživatelské rozhraní, distribuované řídící systémy, SCADA Systémy. Dále popsat konvergenci informační a operační technologie. Zaměřit se na průmyslový Ethernet, determinismus a reálný čas a porovnat typy protokolů průmyslového Ethernetu.

Ve druhé části bylo třeba se zaměřit na komunikační protokoly, zejména na Profinet a S7comm. Jejich použití, komunikaci, rozbor paketu. U S7comm bylo navíc řešeno zabezpečení jednotlivých verzí protokolu.

Třetí část se věnovala knihovně SNAP7. Převážně na obecnou problematiku a její komponenty, kterými jsou SNAP7 Client, Server a Partner. U Clienta byl rozebrán PDU, SmartConnect a asynchronní přenos dat. U Partnera byly rozebrány jednotlivé modely.

V praktické části byly vytvořeny dva programy, jeden představující PLC a druhý HMI. Tyto programy společně komunikují a simulují virtuální průmyslový scénář. Dále byla rozebrána komunikace S7 protokolu zachyceného programem Wireshark.

Programy se mohou rozšířit o třetí prvek, který bude z PLC číst jeho data a tím vytvořit databázi nebo může sloužit jako záloha dat v případě výpadku a možné ztráty dat.

Literatura

[1] ALSABBAGH, Wael a Peter LANGENDÖERFER. A New Injection Threat on S7-1500 PLCs-Disrupting the Physical Process Offline. IEEE Open Journal of the Industrial Electronics Society [online]. 2022 [cit. 2022-05-30]. Dostupné z: https://www.researchgate.net/publication/358617664_A_New_Injection_Threat_on_S7-1500_PLCs_-_Disrupting_the_Physical_Process_Offline

[2] Analog devices: What Is the Difference Between Ethernet and Industrial Ethernet [online]. [cit. 2022-05-29]. Dostupné z: https://www.analog.com/en/technical-articles/what-is-the-difference-between-ethernet-and-industrial-ethernet.html

[3] Analyzing an OT network, what to expect. INPROSEC-AUTO [online]. [cit. 2021-12-13]. Dostupné z: https://inprosec.es/wp-content/uploads/2019/11/Scanning_an_OT_network__what_to_expect_Corrected.pdf

[4] Automating with PROFINET: Industrial Communication Based on Industrial Ethernet [online]. 2008 [cit. 2021-12-13]. Dostupné z: https://books.google.cz/books?id=BqXYCgAAQBAJ&printsec=frontcover#v=onepage&q&f=false

[5] CC-Link IE Field Network. CC-Link [online]. [cit. 2021-12-13]. Dostupné z: https://www.cc-link.org/en/cclink/cclinkie/cclinkie_f.html

[6] CO JE PLC NEBOLI PROGRAMOVATELNÝ LOGICKÝ AUTOMAT. DREAMlandPLC [online]. [cit. 2021-12-13]. Dostupné z: https://dreamland-plc.cz/plc-programovatelny-logicky-automat/

[7] Control System Engineering Workstation. CISA [online]. [cit. 2021-12-13]. Dostupné z: https://www.cisa.gov/uscert/ics/Control_System_Engineering_Workstation-Definition.html

[8] DJIEV, Stancho. Industrial Networks for Communication and Control [online]. Technical University of Sofia, 2003 [cit. 2022-05-29]. Dostupné z: https://data.kemt.fei.tuke.sk/SK_rozhrania/en/industrial%20networks.pdf

[9] EtherNet/IP™. ODVA [online]. [cit. 2021-12-13]. Dostupné z: https://www.odva.org/technology-standards/key-technologies/ethernet-ip/

[10] Guide to Industrial Control Systems (ICS) Security. National Institute of Standards and Technology [online]. 2014 [cit. 2021-12-13]. Dostupné z: http://www.gocs.com.de/pages/fachberichte/archiv/164-sp800_82_r2_draft.pdf

[11] Industrial Ethernet Facts. POWERLINK-Office [online]. [cit. 2021-12-13]. Dostupné z: https://www.ethernet-powerlink.org/fileadmin/user_upload/Dokumente/Industrial_Ethernet_Facts/EPSG_IEF3rdEdition_en.pdf

[12] Industrial Ethernet University: IE304: Real Time Ethernet, Part 1 [online]. [cit. 2022-05-29]. Dostupné z: https://www.industrialethernetu.com/courses/ie304.html

[13] INTRODUCTION TO MODBUS TCP/IP. ACROMAG INCORPORATED [online]. 2005 [cit. 2021-12-13]. Dostupné z: https://www.prosoft-technology.com/kb/assets/intro_modbustcp.pdf

[14] IT OT Convergence – Benefits and Challenges in Manufacturing. Tiempo Development [online]. 2020 [cit. 2021-12-13]. Dostupné z: https://www.tiempodev.com/blog/it-ot-convergence-benefits-and-challenges-in-manufacturing/

[15] MIRU, Gyorgy. The Siemens S7 Communication - Part 2 Job Requests and Ack Data. GyM's Computer Security Rag [online]. 2017 [cit. 2022-05-30]. Dostupné z: http://gmiru.com/article/s7comm-part2/

[16] MIRU, Gyorgy. The Siemens S7 communication-part 1 general structure. GyM's Computer Security Rag [online]. 2016 [cit. 2022-05-30]. Dostupné z: http://gmiru.com/article/s7comm/

[17] PIGAN, Raimond a Mark METTER. Automating with PROFINET: industrial communication based on Industrial Ethernet [online]. Erlangen: Publicis, c2006 [cit. 2021-12-13]. ISBN 38-957-8256-4. Dostupné také z: https://books.google.cz/books?id=pZarsUR6dWQC

[18] PROFINET TECHNOLOGY. Profinet [online]. [cit. 2021-12-13]. Dostupné z: https://us.profinet.com/technology/profinet/

[19] Průmyslový Ethernet II: Referenční model ISO/OSI. Automa [online]. 2007 [cit. 2021-12-13]. Dostupné z: https://automa.cz/cz/casopis-clanky/prumyslovy-ethernet-ii-referencni-model-iso/osi-2007_03_34209_3890/

[20] Průmyslový Ethernet III: Fyzické provedení sítě Ethernet. Automa [online]. 2007 [cit. 2022-05-30]. Dostupné z: https://automa.cz/cz/casopis-clanky/prumyslovy-ethernet-iii-fyzicke-provedeni-site-ethernet-2007_06_34395_2402/

[21] Průmyslový Ethernet IV: Principy průmyslového Ethernetu. Automa [online]. 2007 [cit. 2022-05-30]. Dostupné z: https://automa.cz/cz/casopis-clanky/prumyslovy-ethernet-iv-principy-prumysloveho-ethernetu-2007_10_34198_3258/

[22] Průmyslový Ethernet. Automa [online]. 2005 [cit. 2021-12-13]. Dostupné z: https://automa.cz/cz/casopis-clanky/prumyslovy-ethernet-2005_04_30417_493/

[23] Regulátory [online]. [cit. 2022-05-30]. Dostupné z: http://home.pf.jcu.cz/~kyklop/SERYM/automatizace/jer/Kap06/Kap_06.htm

[24] S7 Communication (S7comm). Wireshark [online]. [cit. 2021-12-13]. Dostupné z: https://wiki.wireshark.org/S7comm

[25] Siemens communications overview. Snap7 [online]. [cit. 2021-12-13]. Dostupné z: http://snap7.sourceforge.net/siemens_comm.html

[26] Step7 Open Source Ethernet Communication Suite. Snap7 [online]. [cit. 2021-12-13]. Dostupné z: http://snap7.sourceforge.net

[27] THE INDUSTRIAL COMMUNICATION SYSTEMS PROFIBUS AND PROFInet [online]. 2009 [cit. 2021-12-13]. Dostupné z: https://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.468.7320&rep=rep1&type=pdf

[28] The Industrial Communication Technology [online]. 2005 [cit. 2021-12-13]. Dostupné z: https://books.google.cz/books?id=Ic4qBgAAQBAJ&printsec=frontcover#v=onepage&q&f=false

[29] The spear to break the security wall of S7CommPlus [online]. [cit. 2021-12-13]. Dostupné z: https://infocon.org/cons/Black%20Hat/Black%20Hat%20Europe/Black%20Hat%20Europe%202017/presentations/eu-17-Lei-The-Spear-To-Break%20-The-Security-Wall-Of-S7CommPlus-wp.pdf

[30] TIAN, Zheng, Weidong WU, Shu LI, Xi LI a Zhongwei CHEN. Industrial control intrusion detection model based on s7 protocol. IEEE 3rd Conference on Energy Internet and Energy System Integration (EI2) [online]. 2019, s. 2647-2652 [cit. 2022-05-29]. Dostupné z: https://ieeexplore.ieee.org/abstract/document/9062159

[31] What is a PLC? AMCI [online]. [cit. 2021-12-13]. Dostupné z: https://www.amci.com/industrial-automation-resources/plc-automation-tutorials/what-plc/

[32] What is Human Machine Interface, or HMI? AVEVA [online]. [cit. 2021-12-13]. Dostupné z: https://www.aveva.com/en/solutions/operations/hmi/#:~:text=HMI%20stands%20for%20Human%20Machine,processes%20in%20factories%20and%20plants.

[33] ZEZULKA, František, Zdeněk BRADÁČ, Petr FIEDLER, Pavel KUČERA a Radek ŠTOHL. Programovatelné automaty. Brno: Vydavatelství VUT, 2003.

[34] ZHAO, Chunhui a Sujuan QIN. A research for high interactive honepot based on industrial service. 3rd IEEE International Conference on Computer and Communications (ICCC) [online]. 2017, s. 2935-2939 [cit. 2022-05-29]. Dostupné z: https://ieeexplore.ieee.org/abstract/document/8323069

[35] MARTINEZ, Edwin Mauricio, Pedro PONCE a Arturo MOLINA. Automation Pyramid as Constructor for a Complete Digital Twin, Case Study: A Didactic Manufacturing System: Sensors [online]. 2021 [cit. 2022-05-29]. Dostupné z: https://www.mdpi.com/1424-8220/21/14/4656

Seznam symbolů a zkratek

ADU	Application Data Unit
BPID	Based-Protocol Instrusion Detection
CAN	Controller Area Network
CIP	Common Industrial Protocol
CN	Control Node
CNC	Computer Numerical Control
COM	Component Object Model
COTP	Connection-Oriented Transport Protocol
CP	Communication Processor
CPU	Central Processing Unit
DA	Data Access
DB	Data-block
DCS	Distributed Control Systems
DMZ	Demilitarized Zone
DoS	Denial of Service
DX	Data Exchange
ERP	Enterprise Resource Planning
FBD	Function Block Diagram
FIP	Factory Instrumentation Protocol
FTP	File Transfer Protocol
HMI	Human-Machine Interface
HTTP	Hyper Text Transfer Protocol
I/O	Input/Output
ICMP	Internet Control Message Protocol

ICS	Idustrial Control Systems
IL	Instruction List
IoT	Internet o Things
IRT	In Real Time
IT	Information Technology
KDK	Key Derivation Key
LAN	Local Area Network
MAC	Media Access Control
MBAP	Modbus Application Protocol
MSDN	Microsoft Developer Network
MES	Manufacturing Execution Systems
MN	Managed Node
OPC	Open Platform Communications
OS	Operation System
OT	Operation Technology
PAC	Programmable Automation Controller
PDU	Protocol Data Unit
PG	Programmer
PID	Proportional-Integra-Derivative
PLC	Programmable Logic Controller
RFID	Radio-Frequency Identifikation
SCADA	Supervisory Control And Data Acquisition
SFC	Sequential Function Chart
SoC	Start of Cycle
ST	Structured Text

TPKT Transport Packet

TSAP Transport Service Access Point

WAN Wide Area Network

A Programy pro PLC a HMI včetně kódu