VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

BRNO UNIVERSITY OF TECHNOLOGY

FAKULTA STROJNÍHO INŽENÝRSTVÍ

FACULTY OF MECHANICAL ENGINEERING

ÚSTAV VÝROBNÍCH STROJŮ, SYSTÉMŮ A ROBOTIKY

INSTITUTE OF PRODUCTION MACHINES, SYSTEMS AND ROBOTICS

PRŮMYSLOVÉ SBĚRNICE A KOMUNIKACE

INDUSTRIAL FIELD BUSES AND COMMUNICATION

BAKALÁŘSKÁ PRÁCE

BACHELOR'S THESIS

AUTOR PRÁCE — **Radovan Koštál**

AUTHOR

VEDOUCÍ PRÁCE — **Ing. Jakub Bražina**

SUPERVISOR

BRNO 2023

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
FAKULTA STROJNÍHO INŽENÝRSTVÍ

Zadání bakalářské práce

Ústav: Ústav výrobních strojů, systémů a robotiky

Student: **Radovan Košťál**

Studijní program: Strojírenství

Studijní obor: Stavba strojů a zařízení

Vedoucí práce: **Ing. Jakub Bražina**

Akademický rok: 2022/23

Ředitel ústavu Vám v souladu se zákonem č.111/1998 o vysokých školách a se Studijním a zkušebním řádem VUT v Brně určuje následující téma bakalářské práce:

PRŮMYSLOVÉ SBĚRNICE A KOMUNIKACE

Stručná charakteristika problematiky úkolu:

V rámci řešení této práce je student seznámen s problematikou průmyslových sběrnic a komunikace mezi periferiemi zahrnutých ve výrobních systémech. Hlavním cílem práce je dokumentace komunikačních možností a jejich využití v průmyslové praxi. Přínos této práce spočívá ve vytvořené dokumentaci, která bude sloužit jako základ pro řešení dalších témat týkajících se průmyslové automatizace.

Cíle bakalářské práce:

Rešerže možných průmyslových sběrnic a komunikací.

Popis využitelnosti v praxi.

Návrh modelového příkladu.

Vyhodnocení dosažených výsledků.

Seznam doporučené literatury:

NOF, Shimon. Springer Handbook of Automation. Berlin: Springer, 2009. ISBN 978-3-540-78830-0.

ŠMEJKAL, Ladislav a Marie MARTINÁSKOVÁ. PLC a automatizace 1: 1. základní pojmy, úvod do programování. Praha: BEN, 1999. ISBN 80-86056-58-9.

Beckhoff Information System [online]. Verl: Beckhoff Automation GmbH & Co., 2020 [cit. 2020-1103]. Dostupné z: https://infosys.beckhoff.com/index_en.htm

Termín odevzdání bakalářské práce je stanoven časovým plánem akademického roku 2022/23

V Brně, dne

L. S.

doc. Ing. Petr Blecha, Ph.D. ředitel ústavu	doc. Ing. Jiří Hlinka, Ph.D. děkan fakulty

ABSTRAKT

Táto bakalárska práca sa venuje problematike priemyselných zberníc a komunikácie. Teoretická časť popisuje súčasný stav implementácie priemyselných zberníc a vlastnosti jednotlivých komunikačných protokolov. Taktiež sú spomenuté možnosti zabezpečenia voči kyberútokom. Druhá, praktická časť, popisuje nadviazanie komunikácie medzi simulovaným PLC v programe TwinCAT 3 a prostredím Node-RED pomocou protokolu MQTT a brokera Mosquitto.

ABSTRACT

This bachelor's thesis deals with the issue of industrial fieldbuses and communication. The theoretical part describes the current state of implementation of industrial fieldbuses and the characteristics of individual communication protocols. Options for cybersecurity are also mentioned. The second, practical part, describes the establishment of communication between a simulated PLC in the TwinCAT 3 program and Node-RED environment using the MQTT protocol and Mosquitto broker.

KLÍČOVÁ SLOVA

Priemyselná zbernica, komunikačné protokoly, kyberbezpečnosť, OSI model, TCP/IP model, Node-RED

KEYWORDS

Industrial fieldbus, communication protocols, cybersecurity, OSI model, TCP/IP model, Node-RED

BIBLIOGRAFICKÁ CITACE

KOŠŤÁL, Radovan. *Průmyslové sběrnice a komunikace*. Brno, 2023. Dostupné také z: https://www.vut.cz/studenti/zav-prace/detail/149319. Bakalářská práce. Vysoké učení technické v Brně, Fakulta strojního inženýrství, Ústav výrobních strojů, systémů a robotiky. Vedoucí práce Jakub Bražina.

PODĚKOVÁNÍ

Chcem poďakovať Ing. Jakubovi Bražinovi za cenné rady a trpezlivosť. Obrovská vďaka patrí mojej rodine a blízkym priateľom, bez ktorých by som nebol človekom, akým som dnes.

ČESTNÉ PROHLÁŠENÍ

Prohlašuji, že tato práce je mým původním dílem, zpracoval jsem ji samostatně pod vedením Ing. Jakuba Bražiny a s použitím literatury uvedené v seznamu.

V Brně dne 25.5.2023 ……

Radovan Košťál

OBSAH

1 ÚVOD

V modernom výrobnom prostredí sa nachádza veľké množstvo rôznych strojov a zariadení, ktoré medzi sebou navzájom interagujú. Základom tejto interakcie je štandardizovaná priemyselná komunikácia, ktorá musí spĺňať vysoké nároky na spoľahlivosť, rýchlosť a efektivitu.

Priemyselné zbernice (fieldbus) slúžia na prenos informácií medzi dvomi a viacerými zariadeniami, typicky senzormi, regulátormi a akčnými členmi v priemyselnom prostredí. Taktiež umožňujú obojsmernú komunikáciu medzi týmito zariadeniami, ktorá je realizovaná pomocou rôznych štandardizovaných protokolov.

Pred zavedením priemyselných zberníc boli jednotlivé zariadenia prepojené pomocou sériových spojení (napríklad RS232), čo v praxi znamenalo, že dve zariadenia mohli spolu komunikovať iba prostredníctvom priameho spojenia. Naopak, priemyselné zbernice umožňujú komunikáciu niekoľkých zariadení naraz pomocou jedného spojného bodu. Tento bod sa následne spojí s ďalším riadiacim zariadením, ktoré umožní šírenie informácií celým systémom. Zbernice teda zabezpečujú nielen zdieľanie väčšieho spektra operačných informácií, väčšiu spoľahlivosť a jednoduchosť inštalácie, ale predstavujú tiež nemalé šetrenie na fyzických prepojeniach. Zbernice operujú iba na niekoľkých vrstvách modelu ISO/OSI.

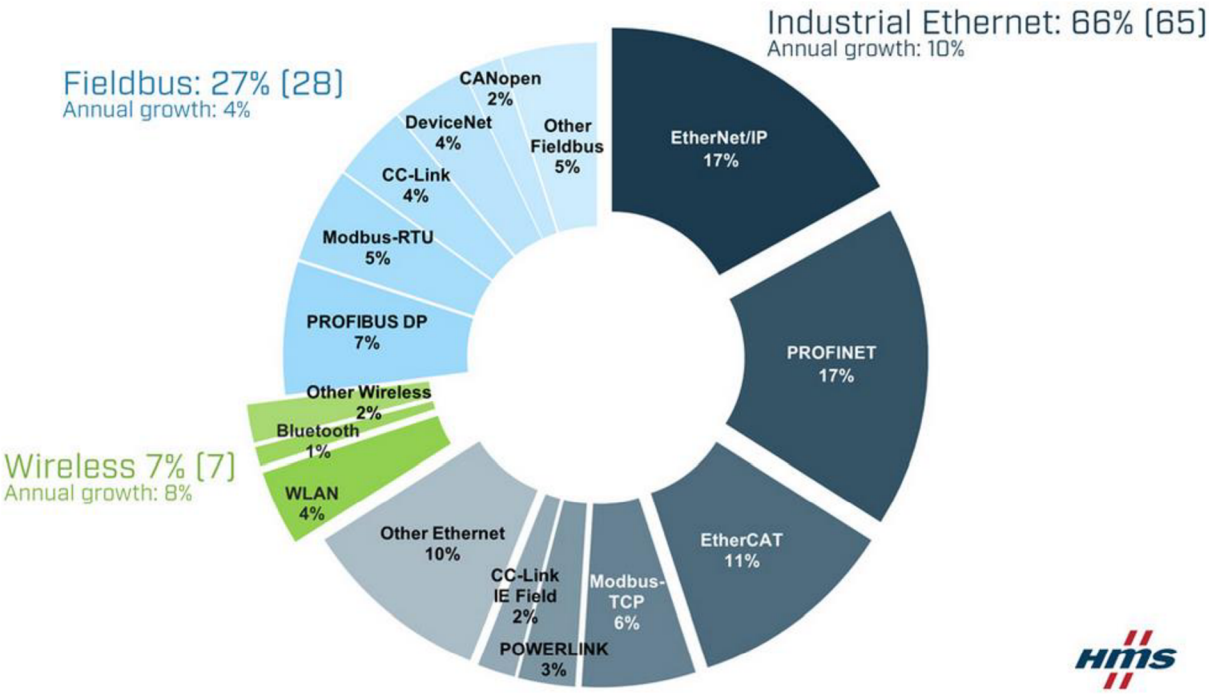
V moderných výrobných systémoch taktiež figurujú rôzne komunikačné protokoly, ktoré sú v súčastnosti už nevyhnutné pre spoľahlivé a prehľadné fungovanie rozsiahlych automatizovaných štruktúr. V neposlednom rade narastá práve kvôli zvýšenej prepojenosti týchto systémov hrozba kybernetických útokov, je preto potrebné neustále vyvíjať nové technológie pre ich aktívnu aj pasívnu ochranu.

Cieľom tejto bakalárskej práce je vytvoriť dokumentáciu slúžiacu na priblíženie problematiky novodobej priemyselnej komunikácie, porovnanie jednotlivých riešení a ozrejmenie súčasného stavu poznania, keďže dané odvetvie sa neustále dynamicky mení.

V prvej časti je popísaný súčasný stav poznania, základné pojmy automatizácie a vybrané komunikačné spôsoby, ako aj ochrana pred kyberútokmi. Nasleduje výber najimplementovanejších zberníc súčasnosti a ich stručný popis. V poslednej časti práce je predstavený modelový príklad, ktorý slúži na demonštráciu komunikácie PLC a prostredia Node-RED.

2 SÚČASNÝ STAV POZNANIA

V dnešnej dobe sú klasické priemyselné zbernice (fieldbus) na miernom ústupe. Môže za to rozmach komunikácie pomocou zberníc na báze priemyselného ethernetu, ktorý už v roku 2018 predbehol klasické zbernice a získal tak väčšinový podiel na trhu. [1]



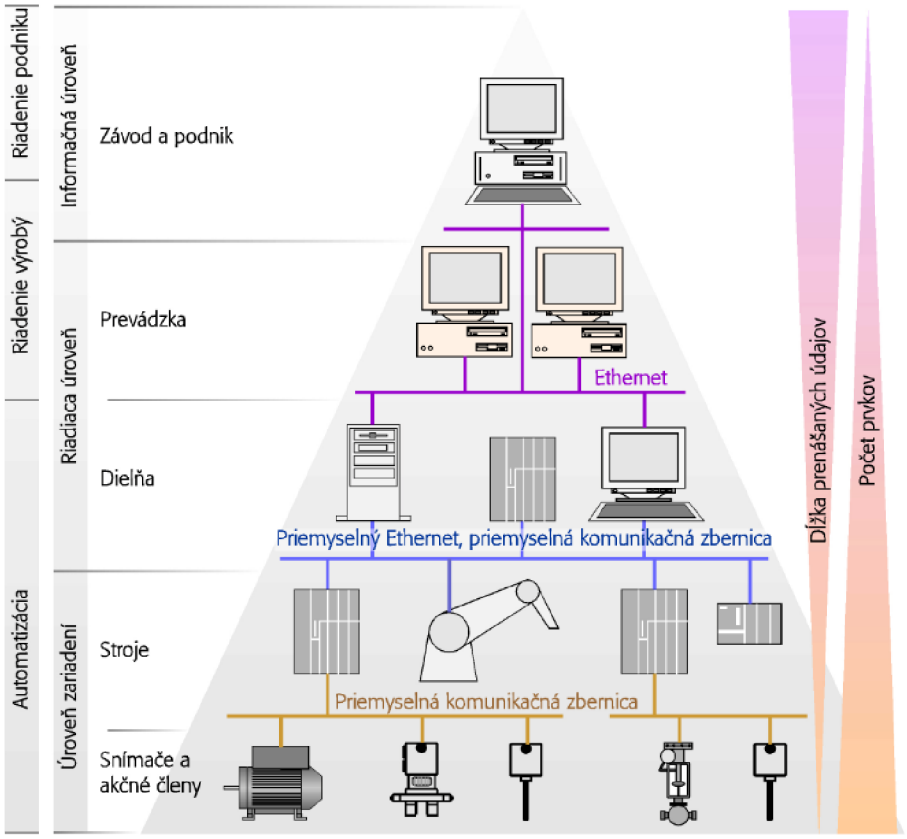
Obr. 1) Trhový podiel komunikačných štandardov z marca 2022 [1]

Dôvodom pre tento fakt môže byť napríklad to, že Industrial Ethernet poskytuje väčšiu šírku pásma (bandwidth), čo je žiaduce v moderných systémoch Priemyslu 4.0 využívajúcich IoT (Internet of Things), ktoré majú za úlohu poskytovať veľké množstvo dát v krátkom čase. [2] S príchodom technológie 5G však netreba zabúdať na bezdrôtovú komunikáciu, od ktorej sa taktiež očakáva určitá forma nárastu.

Aj napriek týmto prognózam sú priemyslové zbernice stále používaným komunikačným štandardom, po ktorom siahajú mnohé firmy.

3 PRIEMYSELNÁ KOMUNIKÁCIA

Komunikácia medzi zariadeniami v priemyselnom prostredí sa pre maximálnu možnú efektivitu riadi podľa hierarchie priemyselného automatizovaného systému. [3] V tejto hierarchii sa nachádzajú úrovne a ich podúrovne obsahujúce jednotlivé zariadenia, ich ovládacie prvky a spôsob, akým medzi sebou komunikujú. Tri hlavné úrovne tejto hierarchie sú úroveň zariadení, riadiaca úroveň a informačná úroveň. So stúpajúcou úrovňou rastie časová náročnosť prenášania údajov a klesá počet prvkov systému.



Obr. 2) Hierarchia priemyselného automatizovaného systému [3]

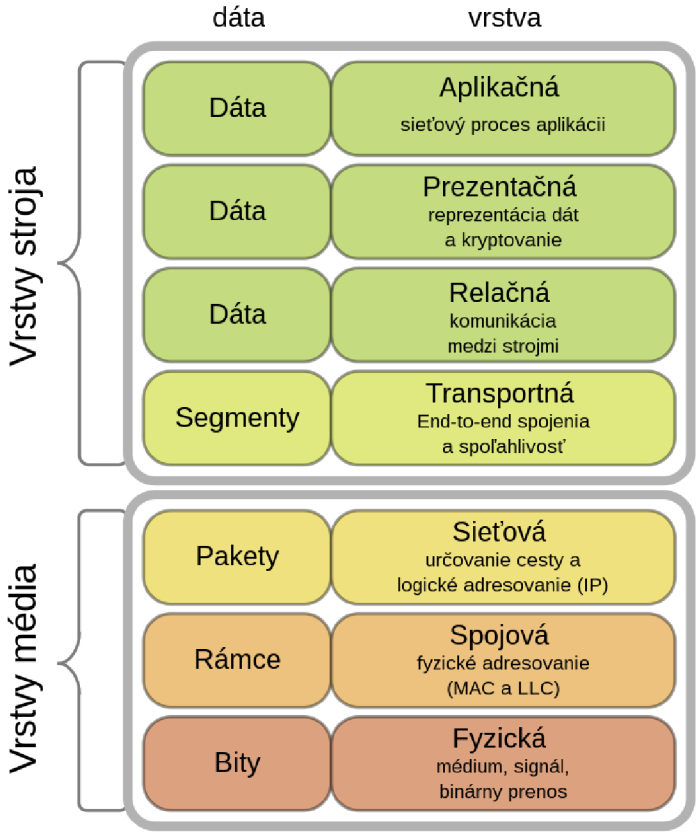
Úroveň zariadení je najnižšia úroveň hierarchie priemyselného automatizovaného systému. Obsahuje jednotlivé zariadenia ako sú napríklad senzory a akčné členy, ktoré prenášajú informácie medzi produktom a technologickým procesom používaným na jeho výrobu. V počiatkoch priemyselnej komunikácie na prenos týchto informácií používaná prúdová slučka 20 mA, neskôr pribudli sériové komunikačné štandardy ako RS232C, RS 422 a RS485, spolu so sériovým štandardom IEEE488. Tieto komunikačné metódy sa postupne vyvinuli do zbernicovej komunikácie, ktorá výrazne zmenšila nároky na počet jednotlivých káblových spojení medzi zariadeniami. Zbernice používané na úrovni zariadení sú napríklad PROFIBUS-DP, CANOpen, DeviceNet a iné. [4]

Riadiaca úroveň funguje na princípe prenosu programov, parametrov a údajov. Vo výrobných procesoch s krátkymi prestojmi strojov sa prenos dát deje priamo počas výroby, z čoho vyplývajú časové požiadavky na prenos. [3] Riadiaca úroveň sa ďalej delí na úroveň dielne a úroveň prevádzky. Dielňa pozostáva z programovateľných logických automatov, robotov a priemyselných počítačov. V rámci dielne vznikajú požiadavky na prenos údajov s krátkou časovou odozvou. Na komunikáciu medzi jednotlivými zariadeniami sa používajú priemyselné zbernice alebo priemyselný ethernet. Úroveň prevádzky združuje tieto dielne do skupín a používa ethernet na komunikáciu s vyššou úrovňou hierarchie.

Informačná úroveň je najvyššou úrovňou priemyselného automatizovaného systému. Riadiaca jednotka na tejto úrovni získava informácie z úrovne prevádzky a riadi celý automatizačný systém. Pomocou WAN sa dokážu prepájať rôzne výrobné závody a vymieňať si medzi sebou informácie.

3.1 OSI model

OSI (Open Systems Interconnection) model je abstraktný referenčný model slúžiaci na stanovenie spôsobu, akým sa prenášajú dáta prostredníctvom siete. Popisuje 7 vrstiev, ktoré obsahujú jednotlivé komunikačné protokoly. Tieto vrstvy sú štandardizované, čo v praxi znamená, že medzi sebou dokážu spolupracovať vrstvy od rôznych výrobcov.



Obr. 3) OSI model a jeho vrstvy [56]

1. **Fyzická vrstva:** popisuje fyzické prepojenie a jeho vlastnosti medzi dvomi zariadeniami v sieti, ako sú rozbočovače a opakovače. Má na starosti moduláciu údajov prichádzajúcich zo spojovej vrstvy a ich následný prenos po fyzickom médiu, buď medeným drôtom alebo optickým káblom.

2. **Spojová vrstva:** zabezpečuje prenos dát po sieti a prípadné opravovanie chýb, ktoré vznikli na fyzickej vrstve. Štandard IEE 802 túto vrstvu rozdeľuje na dve podvrstvy, MAC (Medium Acces Control) a LLC (Logical Link Control). MAC vrstva rozdeľuje dáta na menšie kusy, ktoré sa nazývajú rámce. Tieto rámce obsahujú informácie o zdrojovej a cieľovej MAC adrese. LLC vrstva následne pridáva hlavu a pätu rámca, ktoré slúžia na stanovenie komunikačného protokolu a kontrolovanie chýb. Hardvérom spojovej vrstvy sú switche a bridge.

3. **Sieťová vrstva:** volí najvhodnejšiu a najrýchlejšiu cestu pre prenášané údaje po sieti. Stará sa tiež o paketizovanie údajov z vyššej vrstvy pomocou internetového protokolu (IP) a ich následné adresovanie. Táto vrstva musí tiež rozpoznávať topológiu siete, po ktorej dáta posiela. Protokolmi sieťovej vrstvy sú IP, ARP a ICMP. Na tejto vrstve pracujú routery.

4. **Transportná vrstva:** zaisťuje spoľahlivý prenos informácií tak, že dáta sú doručované v poradí, v ktorom boli poslané a neprichádza k ich duplikácii. Dáta prijímané z vyššej vrstvy rozdeľuje na tzv. segmenty, z ktorých každý obsahuje jedinečné číslo, ktoré slúži na opätovné zloženie dát v cieľovej destinácii. Do tejto vrstvy sú integrované protokoly TCP (Transmission Control Protocol) a UDP (User Datagram Protocol). TCP zabezpečuje spomínanú segmentáciu dát a nadväzovanie spojenia medzi klientami. Naopak, UDP nezaručuje celistvosť doručovaných dát, môže teda nastať strata niektorých paketov, alebo ich duplicitné doručenie. Používa sa na serveroch, ktoré sú menej vyťažované.

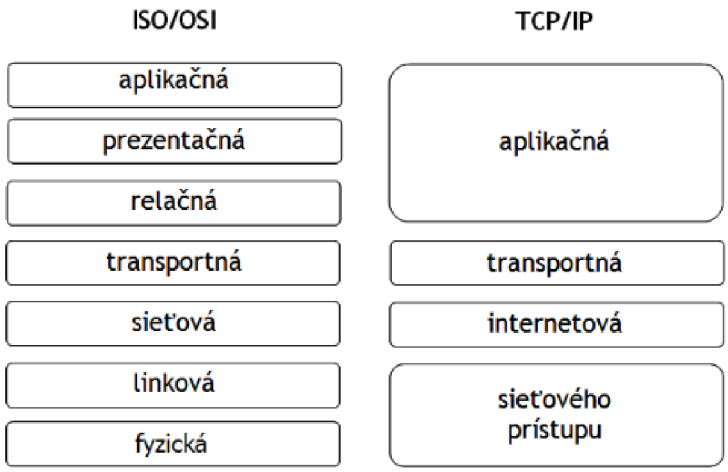
5. **Relačná vrstva:** nadväzuje, udržiava a synchronizuje komunikáciu (TCP/IP relácie) medzi zariadeniami.

6. **Prezentačná vrstva:** stará sa o správnu interpretáciu dát tým, že ich konvertuje na formát, ktorému rozumejú aplikácie zúčastňujúce sa výmeny dát. Zabezpečuje tiež kompresiu a šifrovanie dát.

7. **Aplikačná vrstva:** aplikácie ktoré spolupracujú s touto vrstvou poskytujú používateľovi funkcionality ako zdieľanie súborov, videohovory, zasielanie e-mailov a podobne. Tieto funkcionality používajú rôzne protokoly, ako napríklad HTTP, SNMP, FTP a iné.

3.2 TCP/IP model

TCP/IP protokolová sada bola vyvinutá v 70. rokoch 20. storočia v rámci projektu ARPANET. Je často porovnávaná s referenčným modelom OSI. Model OSI sa skladá zo 7 vrstiev, zatiaľ čo TCP/IP protokolová sada tento model redukuje na 4 vrstvy. Napriek tomu však TCP/IP model pokrýva väčšinu funkcií definovaných v modeli OSI a je považovaný za efektívnejší model pre sieťové komunikácie na internete.



Obr. 4) Porovnanie sieťových modelov OSI a TCP/IP

1. **Vrstva sieťového prístupu:** najnižšia vrstva modelu TCP/IP, ktorá definuje kritériá pre prenos dát prostredníctvom fyzického média. Medzi funkcie tejto vrstvy patrí napríklad rámcovanie dát a detekcia chýb. Zodpovedá prvej a druhej vrstve modelu OSI, na rozdiel od neho sa však táto vrstva nezaoberá špecifikáciami samotného fyzického média.

2. **Internetová vrstva:** tiež známa ako sieťová vrstva, sa často považuje za najdôležitejšiu vrstvtu tohto modelu. Zabezpečuje fragmentáciu a zostavovanie dát, detekciu chýb a celkové zabezpečenie doručenia dát medzi sieťovými zariadeniami. Taktiež rozhoduje o najefektívnejšej ceste prenosu dát cez sieť. Protokoly patriace do tejto vrstvy sú IP, ARP a ICMP.

3. **Transportná vrstva:** tak ako v OSI modeli, táto vrstva zabezpečuje riadenie spojenia medzi zariadeniami pomocou TCP a UDP protokolov.

4. **Aplikačná vrstva:** zodpovedá posledným trom najvyšším vrstvám OSI modelu, čiže zahŕňa protokoly ako sú napríklad SMTP, FTP, TELNET, SNMP a iné. Zaoberá sa poskytovaním rôznych služieb a protokolov pre používateľské aplikácie a zabezpečuje spoľahlivý prenos dát medzi nimi.

OSI a TCP/IP model sú dva základné modely používané pri návrhu a popise sieťových protokolov a ich komunikácie. Hoci oba modely sa snažia riešiť rovnaké problémy, ich zámer a vytvorenie sa líšia.

OSI model bol vyvinutý ako teoretický model s cieľom štandardizovať sieťové komunikácie a umožniť interoperabilitu medzi rôznymi sieťovými zariadeniami a protokolmi. Bol vytvorený skupinou medzinárodných štandardizačných organizácií, aby poskytol základ pre vývoj nových sieťových technológií a protokolov. Jeho hlavným cieľom bolo definovať sedem vrstiev, ktoré by poskytovali štandardizovaný prístup k sieťovej komunikácii.

Na druhej strane, TCP/IP model bol vyvinutý ako implementačný model pre internetovú komunikáciu a bol založený na skúsenostiach pri vývoji pôvodnej siete projektu ARPANET. Jeho hlavným zámerom bolo definovať štyri vrstvy, ktoré by poskytovali základné protokoly pre internetovú komunikáciu. TCP/IP bol teda implementovaný ako sada protokolov a nie ako teoretický model.

Z tohto dôvodu sa OSI model zameriava na abstraktný prístup k sieťovej komunikácii a je vhodný pre vývoj nových sieťových technológií a protokolov, zatiaľ čo TCP/IP model sa zameriava na konkrétne potreby internetovej komunikácie.

3.3 Vybrané spôsoby komunikácie

V oblasti priemyselnej automatizácie a IoT (Internet of Things) sú protokoly a knižnice, ktoré umožňujú efektívnu a spoľahlivú komunikáciu medzi zariadeniami a riadiacimi členmi, nevyhnutné pre ich úspešné fungovanie. Táto kapitola sa venuje týmto technológiám a ich použitiu v priemyselnom prostredí.

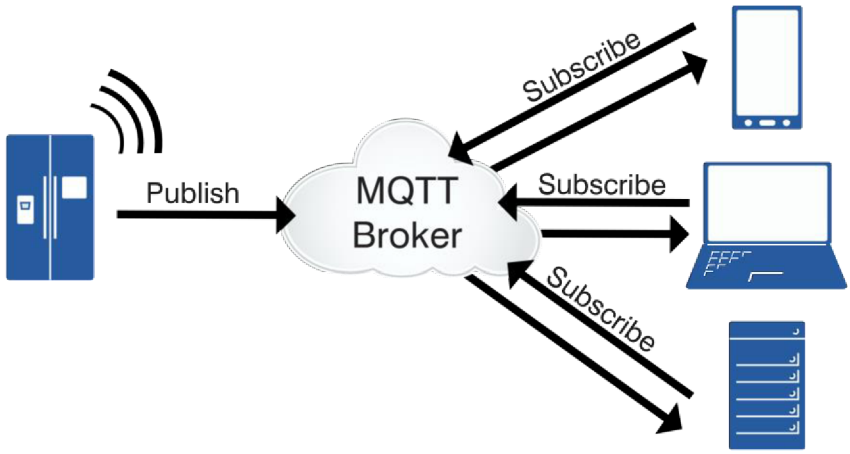
Protokol HTTP

HTTP (Hypertext Transfer Protocol) je protokol aplikačnej vrstvy pracujúci na princípe request/response (nazývaný aj client/server) využívajúci port 80. V priemyselnej komunikácii môže byť používaný na prenos dát z rôznych zariadení, napríklad priemyselných senzorov, ktoré zaznamenávajú teplotu, tlak, vlhkosť a iné parametre, do centrálneho systému, kde sa tieto dáta spracúvajú. [5] Taktiež môže byť používaný na získavanie údajov o produkcii alebo kvalite výrobkov z databázových serverov. V prípade IIoT (Industrial Internet of Things) aplikácií, kde sa senzory a zariadenia pripájajú na internet a umožňujú zber a spracovanie dát, je HTTP protokol často používaný ako jeden zo základných protokolov na prenos dát a ovládanie zariadení. [6]

Protokol HTTPS je rozšírením protokolu HTTP, ktoré je zamerané na bezpečnosť prenosu dát. Využíva port 443 a protokoly TLS (Transport Layer Security) a SSL (Secure Sockets Layer) na šifrovanie komunikácie pomocou certifikátov.

Protokol MQTT

Protokol MQTT (Message Queuing Telemetry Transport) funguje na princípe publisher/subscriber. V priemyselnej komunikácii sa používa na prenos dát medzi zariadeniami, napríklad senzormi, PLC (Programmable Logic Controller), alebo inými IIoT (Industrial Internet of Things) zariadeniami. Výhodou MQTT protokolu je jeho nízka spotreba energie, čo umožňuje efektívne spracovanie a prenos dát aj pre zariadenia s obmedzenými zdrojmi (napríklad batériou alebo výkonom).



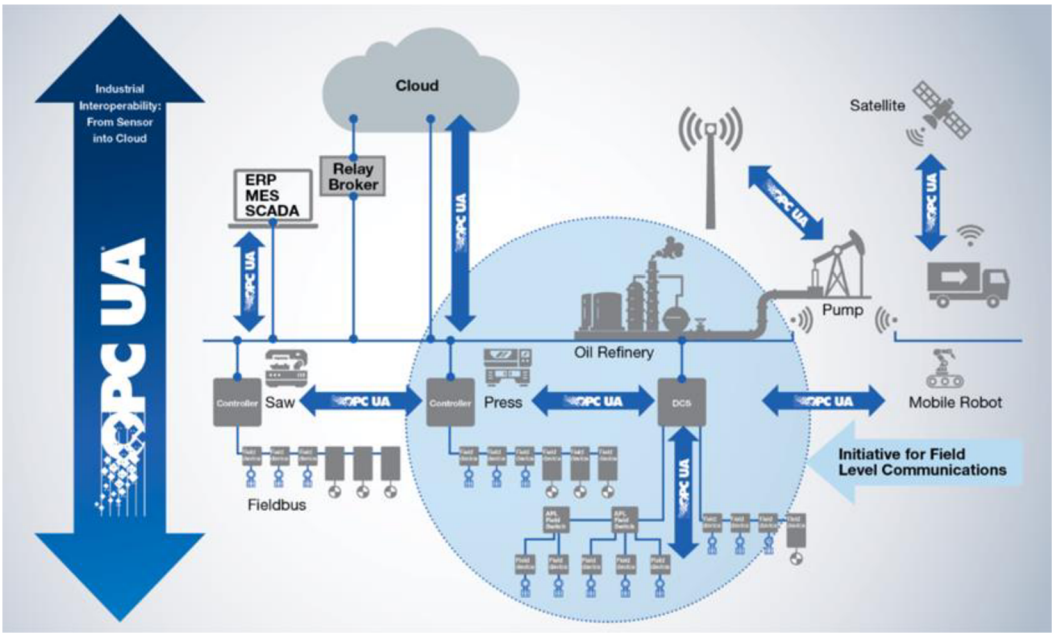
Obr. 5) Publisher/subscriber model ***Chyba! Nenašiel sa žiaden zdroj odkazov.***

Ďalšou z výhod MQTT protokolu v porovnaní s inými protokolmi (napríklad HTTP protokolom) je jeho schopnosť poskytovať real-time komunikáciu medzi zariadeniami, čo je veľmi dôležité pre priemyselné aplikácie, kde rýchla akvizícia a spracovanie dát môže zlepšiť efektivitu a produktivitu zariadení. [7] MQTT protokol tiež umožňuje veľmi jednoduchú integráciu s inými protokolmi a systémami, ako napríklad s databázami alebo ERP (Enterprise Resource Planning) systémami. Tým umožňuje účinnú integráciu v priemyselnej automatizácii a umožňuje realizovať pokročilé riešenia, ako napríklad inteligentné továrne alebo riešenia pre prediktívne údržbu. [8]

V priemyselnej komunikácii je MQTT protokol často používaný v kombinácii s inými protokolmi a technológiami, ako napríklad s protokolom OPC-UA (Open Platform Communications Unified Architecture) pre priemyselnú automatizáciu [9] alebo s protokolmi TLS/SSL pre zabezpečené prenosy dát.

Protokol OPC UA

OPC UA (Open Platform Communications Unified Architecture) je komunikačný protokol, ktorý sa využíva pre priemyselnú automatizáciu a riadenie procesov. Podporuje client/server, ako aj publisher/subscriber modely. [10] Zameriava sa na zabezpečenie interoperability medzi zariadeniami, systémami a aplikáciami v priemysle, čím umožňuje efektívnu výmenu informácií medzi nimi. Umožňuje vzdialený prístup a správu zariadení, čím zvyšuje efektivitu priemyselných procesov a poskytuje ich lepšiu automatizáciu. Používa sa na prenos informácií ako je teplota, tlak, množstvo materiálu, stav zariadenia a podobne. [11] OPC UA využíva šifrovanie a autentifikáciu pre zabezpečenie bezpečnej komunikácie a ochranu pred neoprávneným prístupom k informáciám pomocou X509 certifikátov. [12]



Obr. 6) Rozsah využitia OPC UA protokolu v priemysle ***Chyba! Nenašiel sa žiaden zdroj odkazov.***

Protokol OPC UA je považovaný za jednu z najrozšírenejších a najspoľahlivejších technológií v oblasti priemyselnej automatizácie a riadenia procesov. Využíva sa v rôznych odvetviach priemyslu, ako sú napríklad automobilový, potravinársky, chemický priemysel a iné. OPC UA sa tiež využíva na zber a spracovanie údajov, ktoré môžu byť použité na analýzu a optimalizáciu priemyselných procesov. Vďaka tomu, že protokol umožňuje jednoduchú a efektívnu výmenu informácií medzi rôznymi zariadeniami a systémami, je možné rýchlo reagovať na zmeny v priemyselných procesoch a zlepšiť ich efektivitu. [13]

V súčasnosti sa protokol OPC UA stáva stále populárnejším a jeho využitie sa rozširuje nielen v priemyselnej automatizácii a riadení procesov, ale aj v oblastiach ako sú smart cities, zdravotníctvo, energetika a iné. [14]

Protokol CoAP

CoAP (Constrainded Application Protocol) je) pomerne nový M2M (machine to machine) protokol, ktorého hlavnou výhodou je implementácia v bezdrôtových systémoch obsahujúcich zariadenia s obmedzeným výkonom. [15] Je navrhnutý tak, aby vedel podľa potreby nahradiť HTTP protokol, napríklad v situáciách, kedy sú zariadenia napájané pomocou akumulátora. [16] Pracuje na princípe request/response. Má viacero úrovní zabezpečenia, od NoSec (nezabezpečená) až po Certificate (využitie X.509 certifikátov). [17]

Protokol AMQP

AMQP (Advance Message Queueing Protocol) je aplikačný protokol pre asynchrónnu komunikáciu s garantovaným doručením správ. Podporuje viacero modelov ako publisher/subscriber, request/response a point-to-point. Jedná sa o wire-level protokol, čo v praxi znamená, že definuje formát zasielaných dát ako prúd bajtov, čím zabezpečuje interoperabilitu medzi rôznymi systémami a jazykmi. Okrem garantovaného doručenia správ poskytuje aj riadenie toku a šifrovanie založené na SASL a/alebo TSL. [18]

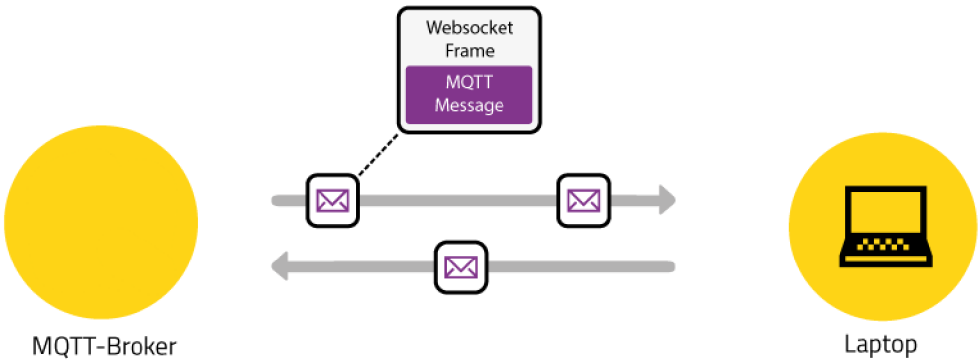
Výhodou AMQP protokolu je, že sa jedná o open-standard protokol, čo zvyšuje flexibilitu používateľa pri prispôsobovaní pre svoje potreby. [19] AMQP a MQTT protokoly sa taktiež ukázali ako 4-krát úspornejšie a rýchlejšie ako HTTP protokol. [20] Je vhodný pre aplikácie, kde sa pakety dát zasielajú kontinuálne s veľmi nízkou alebo veľmi vysokou stratovosťou. [21] Jeho nevýhodou môže byť vyššia komplikovanosť a strmšia krivka učenia.

Používa sa ako primárny protokol pre Azure Service Bus Messaging a Azure Event Hubs. [22] Je vhodný pre aplikácie, kde je potrebné vysoko kvalitné a rýchle doručovanie správ medzi aplikáciami a procesmi. Taktiež môže byť použitý na real-time získavanie, zasielanie a vyhodnocovanie dát z rôznych senzorov, napríklad v kombinácii s komunikačnou sadou Snap7. [23]

Protokol WebSocket

WebSocket je komunikačný protokol pre dvojcestnú real-time komunikáciu medzi klientom a serverom. Prvý krát bol predstavený v roku 2008, pričom bol štandardizovaný a popísaný dokumentom RFC6455 v roku 2011.

Používa sa napríklad v kombinácii s protokolom MQTT pre rýchle a spoľahlivé prenosy dát v reálnom čase. Táto kombinácia poskytuje možnosť dvojcestnej komunikácie medzi klientom a serverom spolu s možnosťou využitia HTTP portu 80 pre pripojenie. [24] Toto však nezabezpečuje lepšiu výkonnosť, ide skôr o zjednodušenie IoT riešenia. Šifrovanie prenosu dát zabezpečuje TLS.



Obr. 7) Kombinácia MQTT a WebSocket [24]

Framework gRPC

gRPC (Google Remote Procedural Call) je framework zameraný na vysoký výkon pre vzdialené volanie procedúr (RPC). Je založený na HTTP/2 protokole. Používa mechanizmus Protocol Buffers pre serializáciu štruktúrovaných dát. Takto serializované dáta vo formáte .proto môžu byť následne interpretované do rôznych programovacích jazykov, ako sú C# a C++, Java, Kotlin, Python, Ruby a iné. [25]

V moderných výrobných priestoroch využívajúcich inteligentné služby je uprednostňovaný protokol MQTT v kombinácii s architektúrou REST vďaka ich priamočiarosti, avšak Kafka a gRPC môžu byť vhodnejšími kandidátmi. [26] gRPC by taktiež mohol byť použitý v systémovej architektúre zaznamenávania dát pre rozpoznávanie chybových stavov pomocou akustických senzorov, kde by slúžil na zmenšenie objemu dát a zabezpečenie škálovateľnosti rôznych programovacích jazykov. [27]

Knižnica SignalR

Jedná sa o knižnicu pre ASP.NET vývojárov, ktorá primárne slúži na pridávanie real-time webových funkcionalít do aplikácií. Používa primárne WebSocket pre prenos tam, kde je to možné, inak používa pre prenos iné metódy. WebSocket sa pre prenos používa vďaka jeho nízkej odozve a efektívnemu využívaniu pamäte servera. Takáto kombinácia WebSocketu a SignalR ponúka rôzne funkcie, pričom sa používateľ nemusí starať o aktualizácie WebSocketu samotného. [28]

V priemyselnej komunikácii by mohol byť využitý pre integráciu s OPC UA protokolom aj spolu s protokolom MQTT pre možnosti asynchrónnej komunikácie. [29]

3.4 Kyberbezpečnosť v priemyselnej komunikácii

Svet je čoraz prepojenejší prostredníctvom Internetu vecí (IoT) či cloudových služieb, a tak potreba robustných bezpečnostných opatrení v priemyselnej komunikácii nikdy nebola väčšia. Nástup Priemyslu 4.0 a Priemyselného internetu vecí (IIoT) priniesol novú éru prepojenosti a výmeny údajov v oblasti výroby a ďalších priemyselných sektorov. Avšak táto zvýšená prepojenosť prináša aj nové zraniteľnosti a potenciálne prístupy zo strany kyberútočníkov.

Jednou z hlavných výziev pri zabezpečovaní priemyselnej komunikácie je potreba zosúladenia bezpečnosti s prístupnosťou. Priemyselné systémy často vyžadujú výmenu údajov v reálnom čase a vzdialený prístup pre účely monitorovania a riadenia. To znamená, že bezpečnostné opatrenia musia byť starostlivo navrhnuté tak, aby umožňovali potrebnú plynulosť procesov, zatiaľ čo stále chránia pred neoprávneným prístupom a porušením údajov.

Existuje niekoľko prístupov k zabezpečeniu priemyselnej komunikácie, vrátane použitia firewallov, systémov detekcie a prevencie prieniku a bezpečných komunikačných protokolov. Okrem toho sa mnoho spoločností obracia na riešenia zabezpečenia založené na cloudových službách, aby poskytli ďalšiu vrstvu ochrany pre svoje priemyselné systémy.

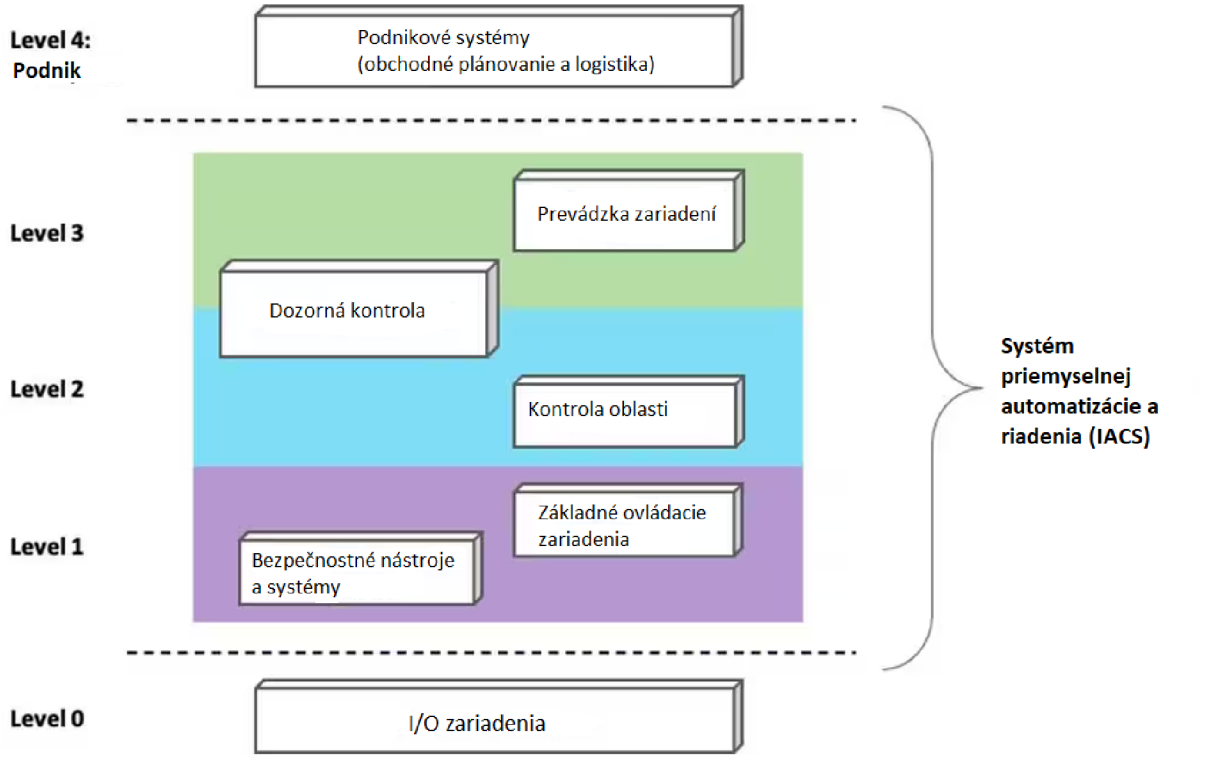
ISA/IEC 62443

Je to séria medzinárodných štandardov popisujúcich požiadavky a procesy pre implementáciu a udržiavanie bezpečných automatizovaných systémov. V tejto sérii štandardov figurujú tri hlavné role: **Produktový Dodávateľ** (Product Supplier – PS), **Systémový Integrátor** (SI) a **Majiteľ Aktív** (Asset Owner – AO). Každá z týchto rolí má jedinečné úlohy v navrhovaní, vývoji, marketingu a udržiavaní bezpečnostných riešení pre priemyselnú výrobu. Ďalej sú definované tri oblasti organizácie: Ľudia, Procesy a Použitá technológia. Tie musia plniť nasledujúce požiadavky: nesmú ovplyvňovať bezpečnostné funkcie výrobných systémov a musia vykonať protiopatrenia, aby zabezpečili požadovanú úroveň zabezpečenia, prípadne aby zabránili útokom. [30]

V sektore operačnej technológie (OT) sú definované tri princípy:

- **Princíp najmenšieho privilégia** – cieľom tohto princípu je poskytnúť užívateľom iba také práva, ktoré sú potrebné na vykonávanie ich práce, aby sa predišlo neoprávnenému prístupu k dátam alebo programom.
- **Hĺbková ochrana (Defense in Depth)** – táto technika umožňuje viacvrstvovým ochranným systémom pozdržať, alebo úplne zabrániť kyberútokom v priemyselnej sieti. Vyžaduje rozdelenie výrobných systémov do tzv. zón, ktoré medzi sebou komunikujú pomocou kanálov (conduit).
- **Analýza rizika** – adresuje riziká spojené s kyberútokmi, ako sú napríklad výpadky výroby, únik citlivých informácií či poškodenie majetku alebo zdravia osôb.

V tomto štandarde je taktiež definovaný funkčný referenčný model, ktorý pozostáva z už spomínaných zón a kanálov. Niektoré komponenty (switche, modemy, routery a iné) tohto referenčného modelu sa vzťahujú na referenčný model ISO/OSI, konkrétne na 2. a 3. vrstvu,



Obr. 8) ISA/IEC 62443 funkčný referenčný model [30]

Firewally

Sú to bezpečnostné prvky, ktoré slúžia na ochranu siete pred neoprávneným prístupom a bezpečnostnými hrozbami. Rozhodujú, či blokovať alebo povoliť komunikáciu na základe stanovených kritérií. Vo všeobecnosti firewall slúži na redukovanie alebo eliminovanie výskytu neželanej komunikácie v rámci siete, zatiaľ čo legitímna komunikácia prebieha bez obmedzení. Firewall reaguje tromi základnými typmi odpovedí: **accept** povoľuje komunikáciu, **reject** komunikáciu zamietne s odôvodnením (error) a **drop**, ktorý zamietne komunikáciu bez odpovede.

Pre náročnejšie priemyselné prostredie existujú špeciálne firewally, ktoré sú týmto sťaženým podmienkam (teplota, vibrácie a iné) prispôsobené. [31]

Obr. 9) Hirschmann EAGLE One Industrial FW Router [31]

Medzi bežné typy firewallov používaných v súčasnosti patria: [32]

- **Firewall s filtrovaním paketov** – skúma a porovnáva pakety na základe kritérií ako sú povolené IP adresy, typ paketu, číslo portu a iné. Výhodou je, že jediné zariadenie dokáže filtrovať prevádzku (traffic) pre celú sieť. Taktiež sa jedná o veľmi rýchle a finančne nenáročné riešenie. Nevýhodou je neschopnosť kontroly obsahu (payload).
- **Brána na úrovni spojenia (Circuit level gateway)** – monitoruje TCP spojenia a iné iniciačné relácie sieťových protokolov na základe dôveryhodnosti pripojeného systému, avšak nemonitoruje pakety samotné. Je jednoduchá na nastavenie a spravovanie s minimálnym dopadom na používateľskú skúsenosť, avšak nemonitoruje aplikačnú vrstvu a ak nie je používaná spolu s inými metódami zabezpečenia, neposkytuje ochranu voči úniku dát zo zariadení.
- **Brána aplikačnej vrstvy (proxy firewall)** – funguje ako prístupový a výstupný bod siete. Filtrujú pakety nielen podľa služby, pre ktorú sú určené (ako je špecifikované cieľovým portom) ale aj podľa ďalších charakteristík, ako napríklad reťazec požiadavky HTTP. Hoci brány aplikačnej vrstvy, poskytujú značnú bezpečnosť dát, môžu dramaticky ovplyvniť výkon siete, zvýšiť čas odozvy a môžu byť náročné na riadenie.
- **Firewall so stavovou kontrolou** – zariadenia so stavovou kontrolou preskúmavajú nielen každý paket, ale sledujú tiež či daný paket je alebo nie je súčasťou nadviazanej TCP alebo inej sieťovej relácie. Toto riešenie poskytuje väčšiu úroveň ochrany ako

firewall s filtrovaním paketov alebo brána na úrovni spojenia, ale aj vyvíja väčšie zaťaženie na výkon siete. Taktiež neposkytuje možnosť autentifikácie.

- **Firewall novej generácie (NGFW)** – kombinuje inšpekciu paketov (aj hĺbkovú) s inými prvkami zabezpečenia, ako sú systém detekcie útokov či systém prevencie útokov, malvérové filtre alebo antivírusy. V tradičnom firewalle sa packet preskúmava podľa jeho hlavičky, pričom firewall novej generácie dokáže skúmať samotné dáta prenášané paketom. Taktiež dokáže sledovať prevádzku od linkovej až po aplikačnú vrstvu. Môže však byť drahší a náročnejší na implementáciu s inými bezpečnostnými prvkami.

Systém detekcie útokov (IDS)

Je to technológia pre automatickú detekciu kybernetických útokov. Zbiera a analyzuje sieťovú prevádzku, bezpečnostné logy, údaje z auditovania a informácie z kľúčových bodov počítačového systému pre zistenie možného porušenia bezpečnosti. [33] Nasledujúce typy IDS sa používajú aj v priemyselnej komunikácii: [34]

- **Network-based (NIDS)** – monitoruje všetku prevádzku na sieti a dokáže rozpoznať hrozby v reálnom čase. Používa sa pre klasické aj bezdrôtové siete.
- **Host-based (HIDS)** – je inštalovaný na jednotlivých počítačoch a serveroch. Monitoruje aktivitua detekuje narušenia na týchto zariadeniach.
- **Signature-based (SIDS)** – používa predkonfigurované bezpečnostné podpisy pre detekciu možných hrozieb.
- **Anomaly-based (AIDS)** – využíva algoritmy strojového učenia pre identifikáciu nezvyčajnej aktivity. Je náročnejšia na konfiguráciu, ale poskytuje väčšiu presnosť pri rozpoznávaní hrozieb.

Rovnako dôležitú funkciu plnia systémy prevencie útokov (IPS), ktoré konštantne monitorujú aktivitu a prevázdku na sieti. Konsolidované IPS systémy môžu byť implementované vo firewalloch novej generácie. Medzi potenciálne hrozby, ktoré IPS detekujú a chránia pred nimi patria napríklad: [35]

- Address Resolution Protocol (ARP) Spoofing
- Buffer Overflow
- Distributed Denial of Service (DDoS)
- Ping of Death
- Port Scanning
- Server Message Block (SMB) Probes
- Secure Sockets Layer (SSL) Evasion

Zabezpečené komunikačné protokoly

Sú to zabezpečené metódy prenosu dát po sieti. Používajú šifrovanie a iné bezpečnostné opatrenia ktoré slúžia na zabránenie úniku či neoprávnenému prístupu k dátam. Medzi tieto protokoly patria:

- **SSL (Secure Sockets Layer) / TLS (Transport Layer Security)** – SSL a jeho nástupca TLS slúžia na nadväzovanie autentifikovaného a šifrovaného spojenia medzi zariadeniami v sieti. Na to slúžia mechanizmy ako kľúče, X.509 digitálne certifikáty a inicializácie (handshakes). [36]
- **SSH (Secure Shell)** – používa sa pre zabezpečené vzdialené prihlasovanie a iné sieťové služby. Taktiež na šifrovanie využíva súkromné a verejné kľúče. [37]

- **IPsec (Internet Protocol security) –** je to skupina spolupracujúcich protokolov, ktoré na zabezpečenie komunikácie používajú okrem kľúčov aj autentifikáciu každého zasielaného paketu. Pri tunelovom režime sú oproti transportnému šifrované aj hlavičky paketov. Medzi tieto protokoly patria Authentication Header (AH), Encapsulating Security Protocol (ESP) a Security Association (SA). [38]

Cloudové zabezpečenie

S vyššou dostupnosťou dát vďaka cloudovým riešeniam v priemyselnej komunikácii prichádza aj zvýšené riziko kyberútokov na tieto systémy. Medzi typy zabezpečenia cloudových systémov patria: [39]

- **Identity and Access Management (IAM) –** zabezpečuje prideľovanie práv užívateľom tak, aby mali prístup iba k funkciám ktoré sú nevyhnutné pre rozsah ich práce. Títo užívatelia môžu byť monitorovaní a prípadne obmedzovaní pri ich interakcii s dátami.
- **Data loss prevention (DLP) –** zabraňuje neoprávnenému nakladaniu s dátami, ich šíreniu alebo používaniu. Využíva mechanizmy ako antivírusy, umelú inteligenciu alebo strojové učenie na detekciu podozrivých aktivít. [40]
- **Security information and event management (SIEM) –** poskytuje monitorovanie procesov a udalostí v reálnom čase, pričom dokáže rozpoznávať hrozby skôr, ako dokážu narušiť chod systému. [41]

4 FIELDBUS

Hlavnou prednosťou priemyselných zberníc je determinizmus. Zbernice poskytujú veľmi spoľahlivý čas odozvy, čo je nevyhnutné pre použitie v pozične závislých operáciách, teda ak je činnosť jedného stroja presne načasovaná v závislosti od činnosti druhého. Výhodou je taktiež ekonomickejšia inštalácia fyzickej vrstvy, najmä pri nutnosti prenosu komunikácie na väčšiu diaľku. Medzi ďalšie výhody patrí jednoduchosť inštalácie, robustnejšie konektory a komponenty a menšia náchylnosť na elektrický šum. [42]

V spojení s priemyselnými zbernicami je bežné použitie zbernicovej topológie zapojenia, topológie typu stromu alebo hviezdy sú taktiež použiteľné, no menej bežné.

V súčasnosti sú najpoužívanejšími zbernicami PROFIBUS, Modbus, CC-Link, DeviceNet a CANopen.

4.1 PROFIBUS

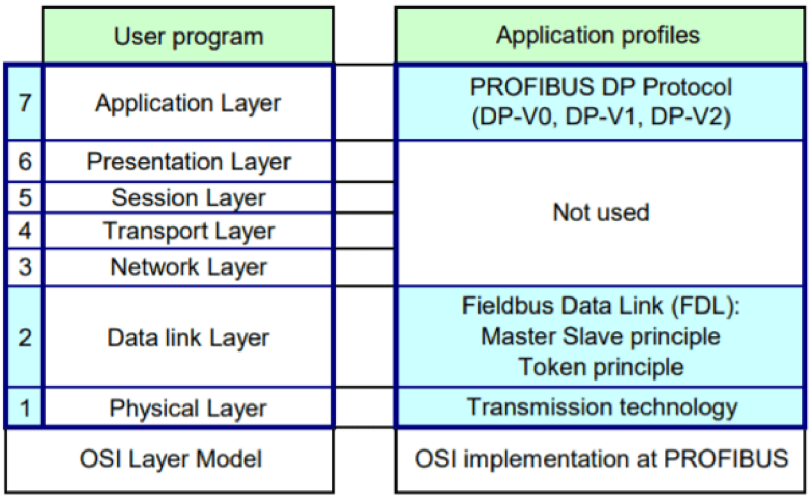
PROFIBUS je stále najpoužívanejším komunikačným štandardom v oblasti priemyselných zberníc, v skratke jeho názov znamená Process Field Bus. Prvý raz bol použitý v roku 1989 v Nemecku. Je zakotvený v medzinárodných štandardoch IEC 61158 a IEC 61784. [43] Operuje na 1., 2. a 7. vrstve ISO/OSI modelu. Delí sa na tri verzie, PROFIBUS FMS (Fieldbus Message Specifications), DP (Decentralized Peripherals) a PA (Process Automation).

Obr. 10) Logo PROFIBUS ***Chyba! Nenašiel sa žiaden zdroj odkazov.***

4.1.1 Vrstvy ISO/OSI modelu

PROFIBUS funguje na 1., 2. a 7. vrstve ISO/OSI modelu, teda na fyzickej, spojovej a aplikačnej.

- Vrstva 1: RS485 pre PROFIBUS DP a MBP pre PROFIBUS PA alebo optické vlákno
- Vrstva 2: pomocou FDL (Fieldbus Data Link) sú kombinované schémy, master-slave a token passing
- Vrstva 7: existuje viacero verzií zbernice PROFIBUS, každá používa iné typy komunikácie na aplikačnej vrstve, teda FMS, DP-V0, DP-V1 a DP-V2.



Obr. 11) Vrstvy OSI modelu pre PROFIBUS ***Chyba! Nenašiel sa žiaden zdroj odkazov.***

4.1.2 Prenosové technológie

Na prenos informácií pomocou fyzickej vrstvy môžu byť využité primárne tri riešenia. RS485, MBP alebo optické vlákno. Pre RS485 a MBP existujú naviac ich „bezpečnejšie“ verzie s prív

	RS485	RS485-IS	MBP	MBP-IS	Optické vlákno
Prenos dát	Digitálny, NRZ (No Return to Zero)	Digitálny, NRZ (No Return to Zero)	Digitálny, kódovanie Manchester, synchrónny	Digitálny, kódovanie Manchester, synchrónny	Optický, digitálny, NRZ
Prenosová rýchlosť	9,6 až 12000 Kbit/s	9,6 až 12000 Kbit/s	31,25 Kbit/s	31,25 Kbit/s	9,6 až 12000 Kbit/s
Zabezpečenie dát	HD=4, paritný bit, obmedzovač start/end	HD=4, paritný bit, obmedzovač start/end	Preambula, poistný obmedzovač start/end	Preambula, poistný obmedzovač start/end	HD=4, paritný bit, obmedzovač start/end
Kábel	Krútený, odtienený dvojdrôtový kábel typu A	Krútený, odtienený dvojdrôtový kábel typu A podľa IEC 61158	Krútený, odtienený dvojdrôtový kábel typu A	Krútený, odtienený dvojdrôtový kábel typu A podľa IEC 61158	Jedno alebo viacvidové sklenené vlákno, plastové vlákno
Vzdialené napájanie	Možné použitím dodatočných drôtov v kábli	Možné použitím dodatočných drôtov v kábli	Možné použitím signálových drôtov v kábli	Možné použitím signálových drôtov v kábli	Možné použitím hybridného kábla
Typy ochrany voči vznieteniu	Zvýšená ochrana Ex e, Ohňovzdorný EX d	Vnútorná ochrana EX ib	Zvýšená ochrana Ex e, Ohňovzdorný EX d	Vnútorná ochrana EX ib	Žiadne
Topológia	Zbernica s ukončením	Zbernica s ukončením	Zbernica a strom s ukončením (možnosť kombinácie)	Zbernica a strom s ukončením (možnosť kombinácie)	Hviezda a kruh (možnosť aj zbernicovej topológie)
Počet uzlov	Až 32 staníc pre jeden segment, max. 126 pre sieť	Až 32 staníc pre jeden segment, max. 126 pre sieť	Až 32 staníc pre jeden segment, max. 126 pre sieť	Až 32 staníc pre jeden segment, max. 126 pre sieť	Až 126 staníc pre sieť
Počet opakovačov	Max. 9 s obnovovaním signálu	Max. 9 s obnovovaním signálu	Max. 4 s obnovovaním signálu	Max.4 s obnovovaním signálu	Neobmedzený počet s obnovovaním signálu

Tab. 1) Vlastnosti prenosových technológií [62]

4.1.3 Rozšírenia PROFIBUS DP

Prvou verziou zbernice PROFIBUS bola **PROFIBUS FMS** (Fieldbus Message Specification). Používala sa pre komunikáciu medzi PLC a riadiacim zariadením. Aj napriek tomu, že je stále používaná malým množstvom výrobných závodov, pre jej malú flexibilitu a nevhodnosť komunikácie na širšej a komplikovanejšej sieti bola bola predstavená verzia **PROFIBUS DP**. Táto verzia sa delí na tri samostatné rozšírenia od najstaršieho po najnovšie.

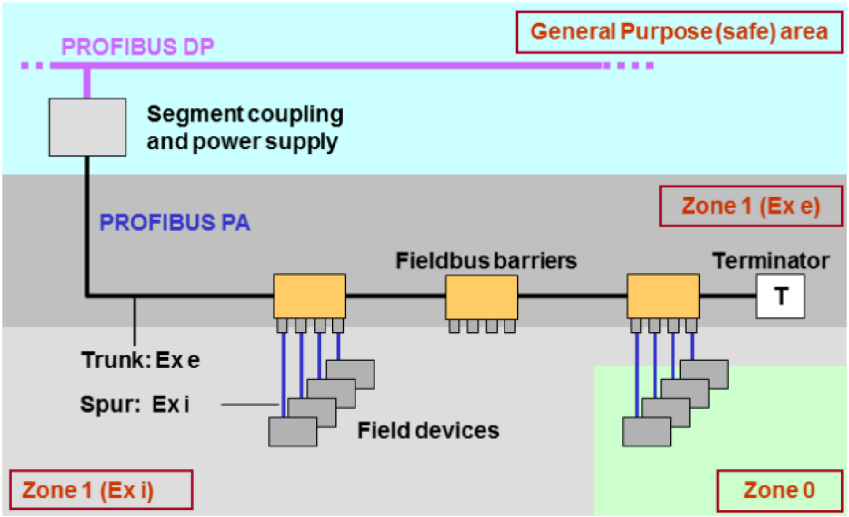
- **DPV0** – zavedená cyklická výmena dát medzi PLC a slave zariadeniami, doplnkové funkcionality sú GSD konfigurácia a diagnostika. Využíva sa najmä pri menej komplikovaných systémoch.
- **DPV1** – acyklická výmena dát, prináša alarmy, fail-safe komunikáciu cez PROFIsafe a integráciu technológií FDT a EDDL
- **DPV2** – izochrónny režim, slave to slave komunikácia, redundancia , segmentácia (upload a download), časová synchronizácia a integrácia HART protokolu

4.1.4 Topológia

Pre RS485: zariadenia sú zapojené do zbernice, pre túto topológiu je možný počet staníc do 32. Na začiatku a konci každého spojenia sa nachádzajú aktívne ukončenia, ktoré musia byť stále napájané zo zdroja. Ak sa počet staníc zvýši nad 32, alebo sa rozširuje celá sieť, je nutné použiť opakovače.

Pre MBP: pre túto prenosovú technológiu je možné použiť ľubovoľnú topológiu. Je možné kombinovať aj rôzne topológie, napríklad stromovú a zbernicovú, ktorá sa de-facto stala štandardnou kombináciou pre PROFIBUS pre jej robustnosť. Celková dĺžka segmentov však nesmie presiahnuť 1900 metrov, pri použití MBP-IS nesmie dĺžka jedného spojenia presiahnuť 60 metrov.

Kombinácia RS485 a MBP: používa sa pre rizikové prostredie, v ktorom sa implementuje fyzická vrstva MBP, pričom v normálnom prostredí funguje RS485.



Obr. 12) Kombinácia RS485 a MBP v rôznych prostrediach [62]

4.1.5 Zabezpečenie

Slabou stránkou zbernice PROFIBUS z hľadiska zabezpečenia je absencia autorizácie a autentifikácie. Útoky typicky smerujú na master zariadenie, cieľom je získať k nemu prístup, prepísať dáta tak, aby bol narušený chod výroby, alebo ho úplne znefunkčniť. Ak má útočník prístup k master zariadeniu, vie ovládať aj jeho slave zariadenia. Kontrola nad master zariadením poskytuje útočníkovi prístup ku kominukácii v sieti, ako aj možnosť zobrazenia celkovej mapy jej topológie. Akonáhle sa útočník dostane do siete, je preňho relatívne ľahké získavať dáta práve kvôli chýbajúcej autentifikácii a autorizácii, ktorá by zabránila komunikovať kompromitovanému master zariadeniu so zvyškom siete.

Existujú dve možné riešenia, ako zabezpečiť zbernicu PROFIBUS. Prvým je integrácia protokolu IPSec a jeho dvoch zabezpečovacích mechanizmov, AH (Authentication Header) a ESP (Encapsulating Security Payload), ktoré môžu byť použité spolu alebo samostatne. Implementáciou tohoto protokolu je možné dosiahnuť autentifikáciu, dôvernosť, integritu a šifrovanie dát. Druhým riešením je integrácia OPC UA (Open Connectivity Unified Architecture) protokolu. Tento protokol umožňuje komunikáciu medzi zariadeniami od rôznych výrobcov a umožňuje autentifikáciu, integritu a dôvernosť komunikácie medzi OPC UA servermi a klientami. Poskytuje ochranu pred útokmi typu message spoofing, eavesdropping, session hijacking, message flooding a inými.

Implementácia týchto protokolov však znamená zvýšené nároky na sieť a jej komponenty, čo sa v praxi môže premietnuť do zvýšeného trvania cyklu zbernice. Ak sa ale implementujú nad field úrovňou, kde sú dané nevýhody zanedbateľné, môžu predstavovať vhodné riešenie pre zabezpečenie zbernice PROFIBUS.

5 INDUSTRIAL ETHERNET

Priemyselný ethernet je oproti bežnému ethernetu pozmenený tak, aby sa dokázal využívať v priemyselnom prostredí. Zmeny sú najbadateľnejšie na fyzickej vrstve ethernetu, ktorá musí odolávať extrémnejším teplotám, vibráciám a chemikáliám. Z tohoto dôvodu sú použité odolnejšie káble a konektory. [43]

Rozdiely existujú aj medzi použitou topológiou, v prípade bežného ethernetu sú zariadenia v drvivej väčšine prípadov usporiadané v hviezdicovej topológii, pričom priemyselný ethernet využíva topológie zbernice, stromu, hviezdy a prstenca.

Ethernetové protokoly ako EtherNet/IP, PROFINET, EtherCAT a ModbusTCP sú v súčasnosti najpoužívanejšie.

5.1 PROFINET

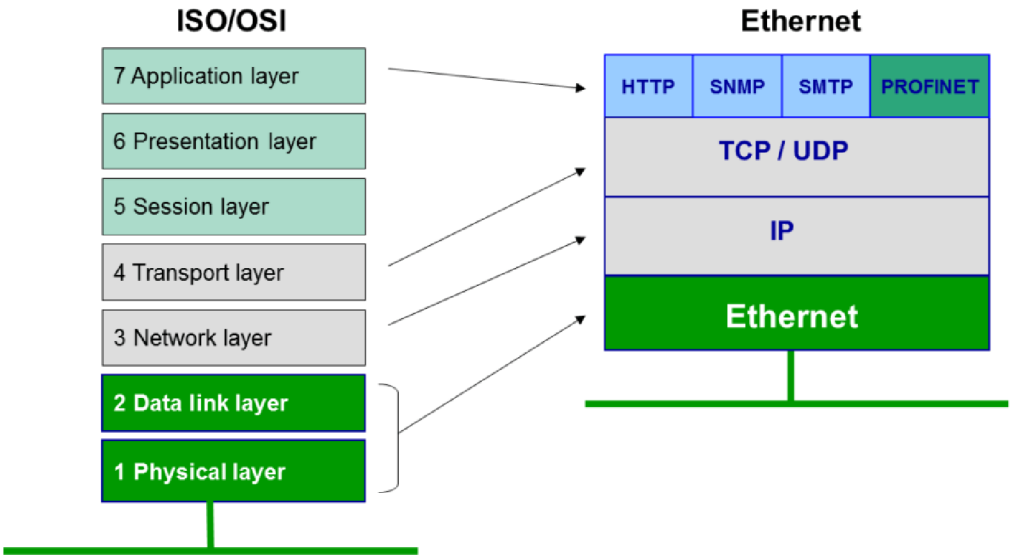
PROFINET (v skratke Process Field Network) je štandard pre komunikáciu cez priemyselný ethernet. Bol zavedený krátko po roku 2000, v roku 2001 bola predstavená prvá verzia, PROFIBUS CBA (Component Based Automation) spĺňajúca štandardy IEC 61158 / IEC 61784-1. V roku 2003 bola predstavená ďalšia verzia, PROFINET IO (Input/Output), ktorá sa v roku 2006 stala súčasťou štandardu IEC 61158 / IEC 61784-2. Najnovšia iterácia štandardu PROFINET je PROFINET TSN (Time Sensitive Networking) predstavená v roku 2019, ktorá sa radí do „triedy zhodnosti“ (conformance class) CC-D. [44]

Obr. 13) Logo PROFINET ***Chyba! Nenašiel sa žiaden zdroj odkazov.***

5.1.1 Vrstvy ISO/OSI modelu

PROFINET funguje na 7. vrstve ISO/OSI modelu, na prenos dát medzi zariadeniami využíva dodatočne model Ethernet a jeho 4 vrstvy, pričom tieto vrstvy používa podľa aktuálnej potreby. [45]

- Vrstva 1: Použitie káblov s medeným jadrom podľa IEC 6187-5-3 alebo 24702, optické vlákno, bezdrôtové pripojenie. Líši sa pre rôzne triedy zhodnosti PROFINET-u.
- Vrstva 2: V závislosti od typu operácie sa používa RT (Real Time), IRT (Isochronous Real Time) alebo TSN (Time Sensitive Networking).
- Vrstva 3: IP (Internet Protocol) umožňuje prenos dát medzi PROFINET zariadeniami pomocou ich IP adries.
- Vrstva 4: Používa sa TCP alebo UDP protokol, v závislosti na požadovanej operácii, alebo iterácii samotného PROFINET-u.
- Vrstva 7: Na tejto vrstve funguje PROFINET, je možné súbežne používať aplikačné protokoly ako HTTP, SMNP, MQTT,OPC UA a iné. [46]



Obr. 14) Mapovanie OSI modelu na Ethernet model [45]

5.1.2 PROFINET CC

Aby sa zaistila kompatibilita medzi zariadeniami, zaviedli sa tzv. „triedy zhodnosti“ (conformance classes), ktoré definujú, aké funkcie je dané zariadenie schopné vykonávať. Vyššie triedy zhodnosti obsahujú špecifikácie nižších tried zhodnosti a zároveň obsahujú pridané funkcie oproti nižším triedam. [47]

- **Trieda A (CC-A) -** zabezpečuje základné funkcie PROFINET IO s komunikáciou v reálnom čase
- **Trieda B (CC-B) -** rozširuje funkcie triedy A o sieťovú diagnostiku a informácie o sieťovej topológii. V rozširujúcej verzii CC-B(PA) je navyše obsiahnutá systémová redundancia, dôležitá pre automatizáciu procesov.
- **Trieda C (CC-D)** - popisuje základné vlastnosti pre zariadenia s hardvérovou podporou rezervácie sieťového pásma a synchronizáciou, je základom pre izochrónnu komunikáciu (IRT).
- **Trieda D (CC-D)** - rozširuje triedu C o štandard TSN (Time Sensitive Networking) operujúci na druhej vrstve OSI modelu, ktorý zaisťuje determinizmus komunikácie cez ethernet.

	Trieda A (CC-A)	Trieda B (CC-B)	Trieda C (CC-C)	Trieda D (CC-D)
Základné funkcie	Komunikácia v reálnom čase, Cyklický prenos I/O, Alarmy	Komunikácia v reálnom čase, Cyklický prenos I/O, Alarmy, Sieťová diagnostika cez SNMP, Detekcia topológie, Redundancia (pre CC-B(PA))	Komunikácia v reálnom čase, Cyklický prenos I/O, Alarmy, Sieťová diagnostika cez SNMP, Detekcia topológie, Redundancia, Hardvérová rezervácia šírky pásma, Synchronizácia	Komunikácia v reálnom čase, Cyklický prenos I/O, Alarmy, Sieťová diagnostika cez SNMP, Detekcia topológie, Redundancia, Rezervácia šírky pásma (TSN), Synchronizácia
Certifikácia pre	Ovládacie zariadenia	Ovládacie zariadenia, Sieťové komponenty	Ovládacie zariadenia, Sieťové komponenty	Ovládacie zariadenia, Sieťové komponenty
Kabeláž	IEC 61784-5-3 a IEC 24702: Medené jadro, Optické vlákno, Bezdrôtovo	IEC 61784-5-3 Medené jadro, Optické vlákno	IEC 61784-5-3 Medené jadro, Optické vlákno	IEC 61784-5-3 Medené jadro, Optické vlákno
Typické použitie	Automatizácia infraštruktúry v budovách	Priemyselná automatizácia, Automatizácia procesov	Ovládanie pohybu	Univerzálne použitie

Tab. 2) Špecifiká tried zhodnosti PROFIBUS [47]

5.1.3 Topológia

Voľba topológie závisí od viacerých kritérií, ako umiestnenie komponentov a vzdialenosť medzi nimi, požiadavky na elektromagnetickú kompatibilitu, izoláciu a triedu zhodnosti, zhodnotenie záťaže pre sieť a iné. [48]

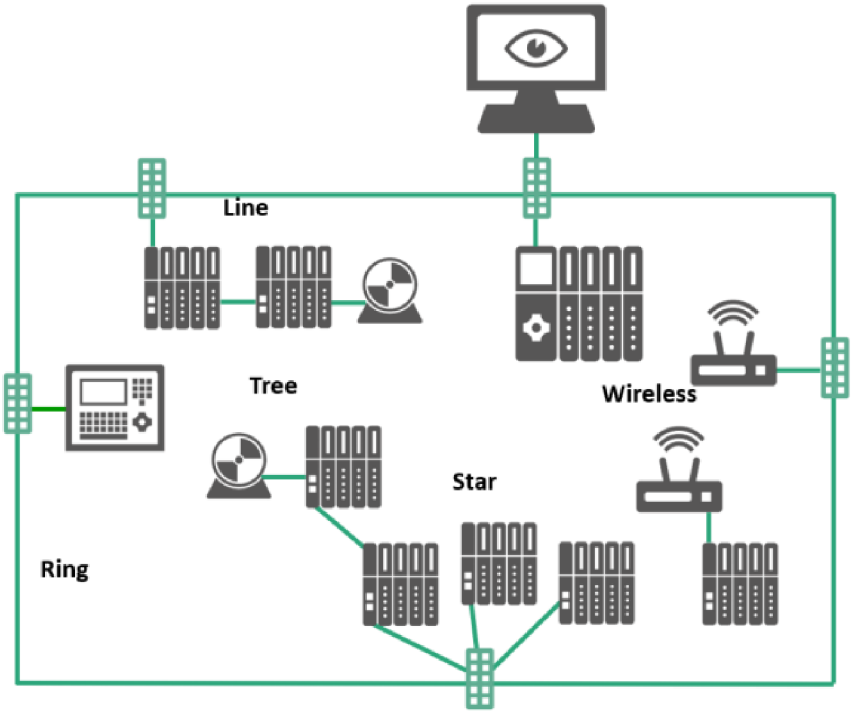
- **Zbernica** – známa topológia používaná v automatizácii nielen rozsiahlych výrobných závodov (pre množstvo dopravníkov), ale aj pre menej náročné požiadavky výroby
- **Hviezda** – tvorená viacerými komunikačnými stanicami pripojenými k spoločnému switchu
- **Strom** – kombinácia viacerých topológií typu hviezda, používa sa pre jasné odlíšenie jednotlivých výrobných oddelení vo výrobnom závode
- **Kruh** – vznikne spojením voľných koncov zbernicovej topológie, jedná sa o redundantnú topológiu

Topológia	Popis	Výhody	Nevýhody
Zbernica	známa topológia používaná v automatizácii nielen rozsiahlych výrobných závodov (pre množstvo dopravníkov), ale aj pre menej náročné požiadavky výroby.	v PROFINET zariadeniach sú switche väčšinou zabudované, možné použitie externých switchov, potrebné menšie množstvo kabeláže	ak jedna stanica zlyhá, nasledujúce stanice stratia pripojenie, nutné brať do úvahy možné oneskorenie signálu, ktoré vznikná pridaním switchu medzi ovládač a jeho zariadenie
Hviezda	tvorená viacerými komunikačnými stanicami pripojenými k spoločnému switchu	efektívna topológia pre spojenie staníc v tesnej blízkosti, zlyhanie jednej stanice neohrozí plnú funkčnosť ostatných zariadení na sieti	ak zlyhá centrálny switch, komunikácia medzi zariadeniami pripojenými na tento switch je narušená, nutnosť dodatočnej kabeláže
Strom	kombinácia viacerých topológií typu hviezda, používa sa pre jasné odlíšenie jednotlivých výrobných oddelení vo výrobnom závode.		
Kruh	vznikne spojením voľných koncov zbernicovej topológie, jedná sa o redundantnú topológiu	redundancia, v prípade zlyhania kábla alebo stanice v kruhovej topológii nie je narušená komunikácia medzi ostatnými zariadeniami	zariadenia pripojené do siete musia podporovať PROFINET redundanciu, nutnosť dodatočnej kabeláže a konfigurácie zariadení pripojených do siete

Tab. 3) Charakteristiky topológií PROFINET [48]

Topológie bezdrôtového pripojenia sa výrazne líšia oproti klasickým, výhodou použitia bezdrôtovej topológie je absencia kabeláže a množstva hardvéru, nevýhodou je obmedzená rýchlosť, determinizmus a nutná analýza podmienok pre bezdrôtové pripojenie. Taktiež je možné kombinovať v sieti bezdrôtové topológie s klasickými. Hoci sú klasické topológie rozšírenejšie, bezdrôtové topológie majú nenahraditeľné zastúpenie pri využívaní pohyblivých zariadení, ako sú automatizované vozíky, roboty a iné. [48]

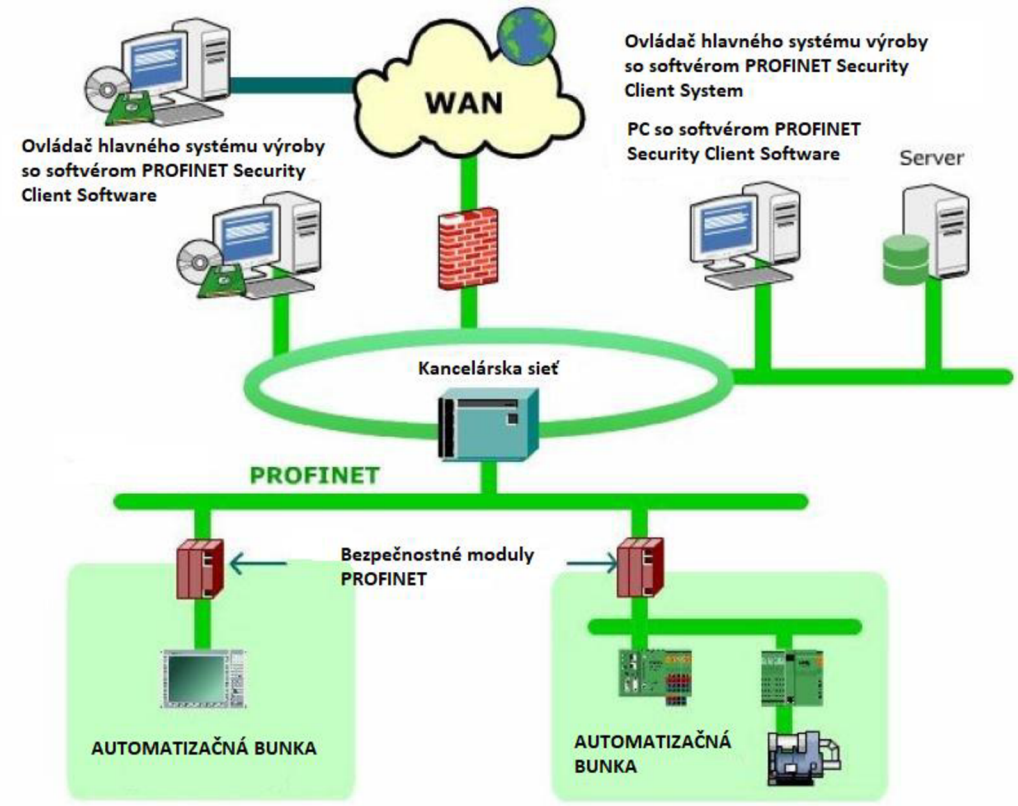
- **Point to Point (P2P) –** dedikované bezdrôtové spojenie medzi dvomi zariadeniami, dvomi prístupovými bodmi alebo medzi zariadením a prístupovým bodom. Tento kanál slúži iba na komunikáciu týchto dvoch elementov, tým pádom je dostupná väčšia šírka pásma.
- **Point to Multipoint (P2M) –** najbežnejšia forma bezdrôtovej konfigurácie, umožňuje spojenie viacerých klientov k ovládaču alebo inému zariadeniu pomocou jedného prístupového bodu.
- **Wireless Distribution System (WDS) -** klient s môže meniť pripojenie k viacerým prístupovým bodom bez toho, aby stratil pripojenie, výhodné použitie pri pohyblivých strojoch s bezdrôtovým pripojením (automatické vozíky a iné).
- **Mesh –** bezdrôtové zariadenia sa sú spojené mnohými redundantnými pripojeniami. V prípade, ak nejaké pripojenie zlyhá, existuje pre dané zariadenie viacero možností, ako spojenie k cieľovému prístupovému bodu obnoviť



Obr. 15) Znázornenie kombinácie klasických a bezdrôtových topológií [48]

5.1.4 Zabezpečenie

V minulosti zabezpečenie PROFINET-u pozostávalo z konceptu izolácie. V praxi to znamenalo oddeľovanie jednotlivých výrobných závodov od vonkajších sietí a ďalšie oddeľovanie výrobných buniek v danom závode. Sieťové komponenty sa starajú o zabezpečenie pomocou kontroly autorizácie a integrity. Dáta medzi zabezpečenými bunkami môžu byť taktiež šifrované pre dodatočné zabezpečenie komunikácie. [49]



Obr. 16) Príklad bezpečnostného konceptu PROFINET [49]

V dnešnej dobe Priemyslu 4.0 a potreby širšej komunikácie tento koncept nie je postačujúci, preto PROFINET definuje dodatočné 3 triedy bezpečnosti ako nadstavbu pre svoje systémy. Prvá trieda bezpečnosti je obsiahnutá v samostatnom dokumente má byť uvedená do používania v roku 2024, ostatné dve budú uvedené postupne. [50]

- **Trieda 1** – zmeny sa týkajú DCP a SNMP protokolov, ako aj ďalšieho zabezpečenia GSD súborov. PROFINET DCP (Discovery and basic Configuration Protocol) slúži na nachádzanie a identifikáciu zariadení ich ovládačmi a následnú konfiguráciu nastavení týchto zariadení, ako IP adresa a názov. Zmenou týchto konfiguračných príkazov na read-only sa zabráni možnej neoprávnenej manipulácii s nimi. Ďalej dostali PROFINET zariadenia oprávnenie úplne vypnúť používanie SNMP protokolu, alebo tento protokol používať v read-only režime. Poslednou zmenou je posilnenie ochrany GSD súborov virtuálnym certifikátom, ktorý má zaručovať, že s obsahom súboru nebolo neoprávnene manipulované.

5.2 EtherNET/IP

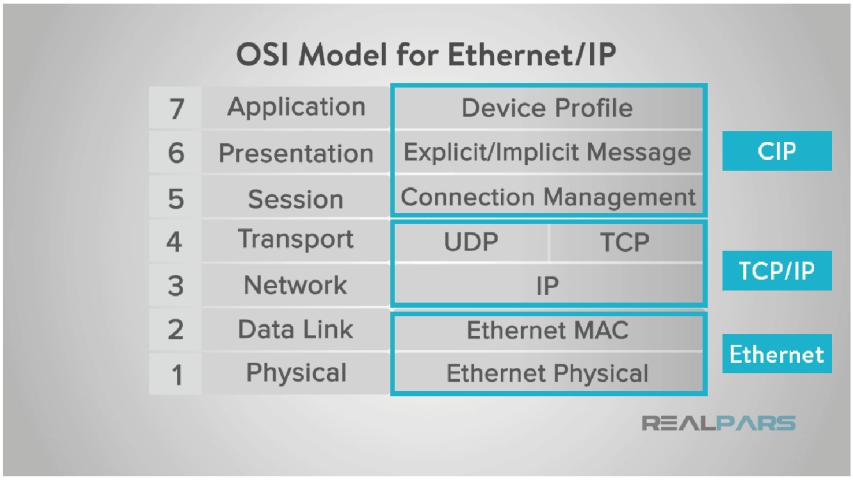
EtherNet/IP je sieťový protokol vyvinutý spoločnosťou Rockwell Automation špeciálne pre použitie v priemyselnom prostredí. Bol predstavený v roku 2001 a v súčastnosti ho spravuje spoločnosť ODVA. Využíva veľmi rozšírený priemyselný komunikačný protokol CIP (Common Industrial Protocol). Pre zabezpečenie kompatibility a interoperability medzi systémami existujú rôzne adaptéry, jedným z nich je adaptér FENA-21 od firmy ABB podporujúci komunikačné protokoly PROFINET IO, Modbus TCP a EtherNet/IP. [51]

Obr. 17) Logo EtherNET/IP [64]

1.1.1 Vrstvy ISO/OSI modelu

EtherNet/IP, ako jeho názov napovedá, využíva fyzickú vrstvu ethernetu a následne protokoly TCP/UDP pre transport, pričom od 5. až po 7. vrstvu OSI modelu implementuje objektovo orientovaný protokol CIP. [52]

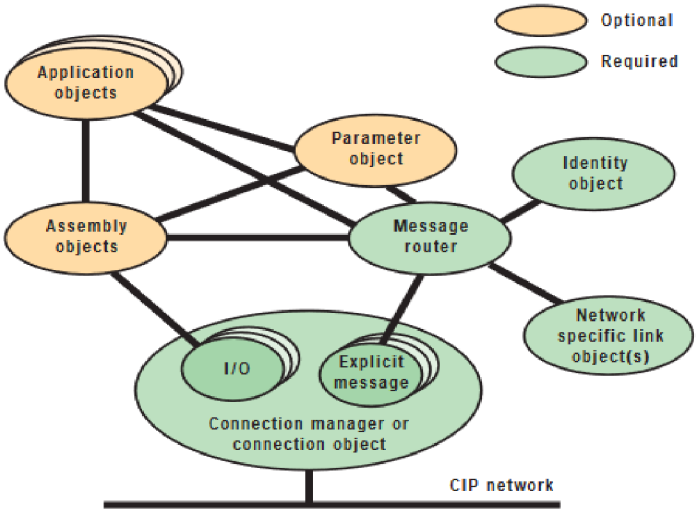
- Vrstva 1: Použitie štandardnej technológie podľa IEEE 802.3, krútené káble typu CAT 5E / CAT 6 sú pre náročnejšie priemyselné prostredie dodatočne chránené podľa IP67. Možnosť použitia tienených alebo netienených konektorov RJ45 pre krútené káble, alebo konektory LT, SC, ST a MTRJ pre optické vlákno.
- Vrstva 2: Taktiež podľa IEEE 802.3 sa používa protokol CSMA/CD pre prístup k prenosovým médiám.
- Vrstva 3 a 4: Používa sa komunikácia TCP/IP a UDP/IP pre real-time potreby.
- Vrstva 5 až 7: Okrem bežných protokolov aplikačnej vrstvy sa používa objektovo orientovaný protokol CIP (Common Industrial Protocol)



Obr. 18) Vrstvy OSI modelu pre EtherNet/IP [64]

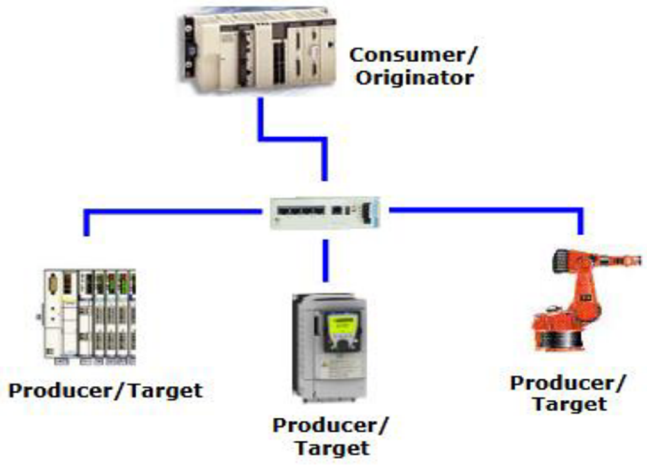
5.2.1 CIP object model

Spomínaný aplikačný protokol CIP používa tzv. object models, ktoré predstavujú skupinu objektov slúžiacich na reprezentáciu jednotlivých zariadení. Tieto objekty obsahujú atribúty (dáta), služby (príkazy), pripojenia a reakcie na udalosti, ktoré sú preddefinované v objektovej knižnici CIP. Táto knižnica podporuje mnohé automatizačné zariadenia a funkcie, ako analógový či digitálny I/O, pohybové systémy, klapky, senzory, aktuátory a iné. Pre zaistenie interoperability sa objekty, ktoré sú definované v dvoch a viacerých zariadeniach, správajú rovnako. [53]



Obr. 19) Objektový model v CIP komunikácii [65]

Objektový model používaný protokolom CIP je založený na komunikačnom modeli producer-consumer. Producer zariadenia vo všeobecnosti generujú dáta vo vopred stanovenom rozsahu bez nutnosti jednotlivých žiadostí pre každú generáciu. Tento rozsah sa označuje ako RPI (Request Packet Interval) a jedná sa o konfigurovateľný parameter. Consumer zariadenia zúžitkovávajú dáta generované producer zariadeniami, a stanovujú pravidlá pre generovanie týchto dát. Akékoľvek zariadenie sa podľa jeho možností môže prezentovať ako producer alebo consumer. [54]



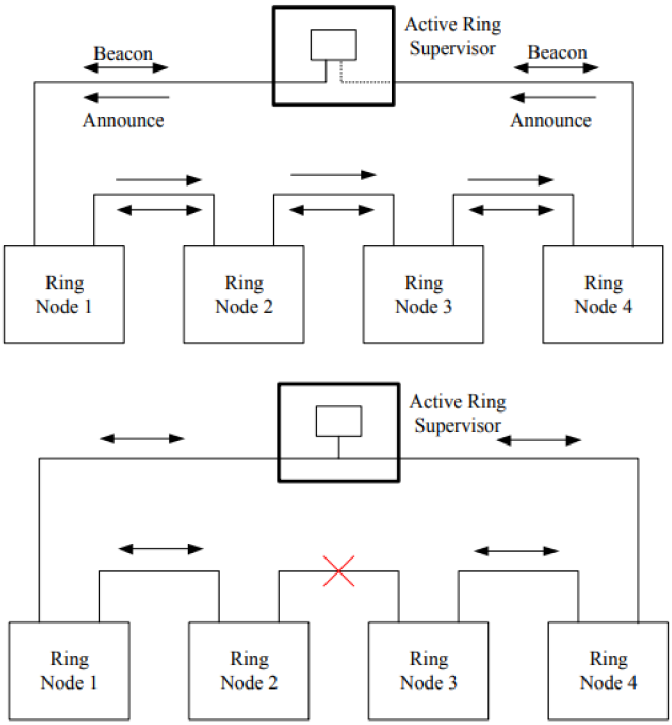
Obr. 20) Producer/consumer model [54]

Podpora pre zariadenia od rôznych výrobcov je zabezpečená pomocou tzv. Device Profiles (profily zariadení). Jedná sa o nadstavbovú skupinu objektov zariadenia, ktorá špecifikuje konfiguráciu a dátové formáty pre I/O. Zariadenia, ktoré používajú tieto profily dokážu reagovať na spoločné príkazy, tým pádom je možná integrácia Modbus, HART a IO-Link zariadení. [53]

5.2.2 Topológia

EtherNet/IP podporuje mnohé základné typy topológií ako sú zbernica, strom, hviezda a kruh. Pre zaistenie redundancie sa používa DLR (Device Level Ring). Ide o protokol, ktorý má za úlohu zaistiť čo najrýchlejšie obnovenie komunikácie v prípade zlyhania v kruhovej topológii. Figurujú v ňom tzv. Ring supervisor, a Ring participants, ktorí sá následne delia na announce-based a beacon-based. [52]

- **Ring Supervisor** – zariadenie tohoto typu zasiela a spracúva rámce typu beacon a announce pre detekciu možných chýb v topológii. V prípade takýchto chýb supervízor zariadenie presmeruje komunikáciu tak, aby nedošlo k výpadku. Delia sa na aktívnych a záložných supervízorov.
- **Ring Participant** – tieto zariadenia takisto dokážu informovať o chybách v topológii. Delia sa podľa schopnosti spracovávať typy rámcov. Rámce typu beacon sú omnoho rýchlejšie ako rámce typu announce.
  -



Obr. 21) Reakcia DLR topológie na chybu [52]

5.2.3 Zabezpečenie

Okrem štandardných spôsobov zabezpečenia využíva EtherNet/IP spomínané Device Profiles, konkrétne EtherNet/IP Confidentiality Profile. Medzi ďalšie profily patria EtherNet/IP Integrity Profile (dnes už zastaraný) a CIP Authorziation Profile (pripravovaný). Existuje takisto Resource-Constrained CIP Security Profile navrhnutý pre použitie v systémoch s obmedzeným výkonom. [55]

- **EtherNet/IP Integrity Profile (zastaraný)** – poskytoval bezpečnú komunikáciu medzi koncovými bodmi v EtherNet/IP sieti pre zaistenie integrity dát a zabezpečenia zariadení.
- **EtherNet/IP Confidentiality Profile -** poskytuje bezpečnú komunikáciu medzi koncovými bodmi v EtherNet/IP sieti pre UDP komunikáciu. Starší Integrity Profile je v ňom obsiahnutý.
- **CIP Authorization Profile (pripravovaný) -** poskytuje bezpečnú komunikáciu medzi koncovými bodmi v CIP sieti.
- **CIP User Authentication Profile** – poskytuje autentifikáciu na úrovni používateľa pre CIP komunikáciu
- **Resource-Constrained CIP Security Profile** – poskytuje menej náročnú verziu zabezpečenia CIP pre zariadenia s obmedzeným výkonom

Vlastnosti zabezpečenia	EtherNet/IP Confidentiality Profile	CIP Authorization Profile	CIP User Authentication Profile	Resource-Constrained CIP Security Profile
Autentifikácia zariadení	✓	✓	✓	✓
Rozsah dôveryhodnosti domény	skupina zariadení	skupina zariadení	jednotlivé zariadenie/používateľ	jednotlivé zariadenie/používateľ
Identita zariadenia	✓	✓	✓	✓
Integrita dát	✓	✓		✓
Dôvernosť dát		✓		
Autentifikácia používateľa			✓	
Detekcia zmien (audit)			✓	
Presadzovanie politík (autorizácia)			✓	

Tab. 4) Profily zabezpečenia EtherNet/IP [55]

6 ZHRNUTIE

V predchádzajúcich kapitolách boli predstavené klasické a ethernetové zbernice, ktoré sú v súčasnosti najpoužívanejšie. Medzi ďalšie rozšírené zbernice sa radia taktiež EtherCAT a Modbus-RTU. V tejto kapitole sú zhrnuté ich základné parametre.

	PROFIBUS	PROFINET	EtherNET/IP	EtherCAT	Modbus-RTU
Rýchlosť prenosu	12 Mbps	100 Mbps až 1 Gbps	100 Mbps až 1 Gbps	100 Mbps až 1 Gbps	10 Mbps
Maximálna vzdialenosť	1200 m	100 m	100 m	100 m	1200 m
Topológie	zbernica, hviezda, kruh, strom	zbernica, hviezda, kruh, strom	zbernica, hviezda, kruh, strom, DLR	zbernica, strom, hviezda	zbernica, daisy-chain
Maximálny počet zariadení	126	-	256	65 535	247
Fyzická vrstva	RS485, MBP, optické vlákno	IEEE 802.3	IEEE 802.3	IEEE 802.3	RS232, RS485
Metóda	master/slave	consumer/ provider	client/server	master/slave	master/slave

Tab. 5) Parametre priemyselných zberníc používaných v súčasnosti

Z tejto tabuľky je zrejmé, že klasické zbernice výrazne zaostávajú v rýchlosti prenosu dát, čo môže byť pre ich používanie v budúcnosti rozhodujúce. Čoraz väčšia potreba rýchlosti výmeny dát a integrácie výrobných systémov s modernými technológiami posunula priemyselné zbernice na báze ethernetu do popredia. To však neznamená, že klasické zbernice nemajú svoje miesto na trhu. Medzi ich prednosti patrí väčšia jednoduchosť inštalácie, odolnosť voči elektronickému šumu, robustnosť a v neposlednom rade aj menšia finančná náročnosť. Z tohoto dôvodu ide stále o relevantné riešenie pre firmy, ktoré pre svoju výrobnú činnosť uprednostnia jednoduchosť pred väčšími možnosťami integrácie.

7 MODELOVÝ PRÍKLAD

Súčasťou práce je návrh modelového príkladu. Je zvolené prostredie TwinCAT 3 od firmy Beckhoff pre simuláciu PLC a nástroja Node-RED pre programovanie a vizualizáciu procesov.

Cieľom je ukázať modelový príklad prepojenia, vzájomnej komunikácie a možností riadenia technologických prvkov prostredníctvom voľne dostupných softvérových nástrojov s vysokou mierou flexibility. Pre samotnú komunikáciu je zvolený komunikačný protokol MQTT.

Predmetom príkladu je simulácia jednoduchého PLC pre riadenie technologického stroja a príprava vizualizovaného prostredia pre jeho ovládanie z počítača.

Pre vypracovanie príkladu boli použité nasledovné komponenty a technológie:

Komponent	Verzia	Určenie
Beckhoff TwinCAT 3 eXtended Automation Engineering (XAE)	3.1 build 4024.44	Vývojový a modelovací nástroj pre ovládanie a simuláciu PLC a iných zariadení
Node.js	16.20 x64	JavaScript Runtime prostredie pre beh Node-RED
Node-RED	3.0.2	Programovací nástroj pre vizualizáciu a ovládanie hardvérových zariadení
Eclipse Mosquitto	2.0.15	Message broker pre sprostredkovanie komunikácie pomocou MQTT protokolu
MQTT Explorer	0.4.0-beta	MQTT klient uľahčujúci ladenie komunikácie na strane message brokera

Tab. 6) Komponenty modelového príkladu

Modelový príklad bol vytvorený v rámci virtuálneho stroja s nasledovnými parametrami:

- 4 logické procesory
- 4 GB RAM
- 40 GB HDD
- OS Windows 10 Pro 22H2

Virtuálny stroj bol zriadený v prostredí Hyper-V na bežnom kancelárskom počítači s Windows 11 Pro, vybavenom procesorom Intel Core i7-10700T @ 2GHz, 16 GB RAM a lokálnym SSD úložiskom. Hyper-V prostredie je okrem serverových edícií operačného systému Windows dostupné zdarma aj na desktopových verziách Windows 10/11 Pro a vyšších.

Výkon virtuálneho stroja bol pre modelový príklad dostačujúci, operačný systém aj jednotlivé komponenty reagovali svižne a nebolo badať žiadne známky nedostatku výkonu pre priebeh testov.

7.1 Inštalácia a konfigurácia

Nasleduje návod na inštaláciu a konfiguráciu jednotlivých komponentov tak, aby bol modelový príklad jednoducho reprodukovateľný na ľubovoľnom zariadení.

7.1.1 TwinCAT 3

Inštalácia TwinCAT 3 bola vykonaná pomocou inštalačného balíka vo forme .exe súboru, stiahnutého zo stránok firmy Beckhoff. Samotné vývojové prostredie je voľne dostupné, licenciám podliehajú jednotlivé moduly, ktoré je možné doinštalovať. Pre účely testovania je možné vygenerovať 7 dňové dočasné licencie.

Nástroj TwinCAT je postavený na technológii Microsoft Visual Studio, čo programátorom, ktorí pracovali s týmto vývojárskym prostredím výrazne uľahčí prácu. K dispozícii je známe integrované vývojové prostredie, debugger a ďalšie možnosti tohto nástroja. V prípade, že sa TwinCAT inštaluje na počítači s už inštalovaným softvérom Visual Studio, ponúkne možnosť integrácie priamo do neho. Vtedy môže programátor používať svoje známe prostredie, do ktorého pribudnú komponenty nástroja TwinCAT.

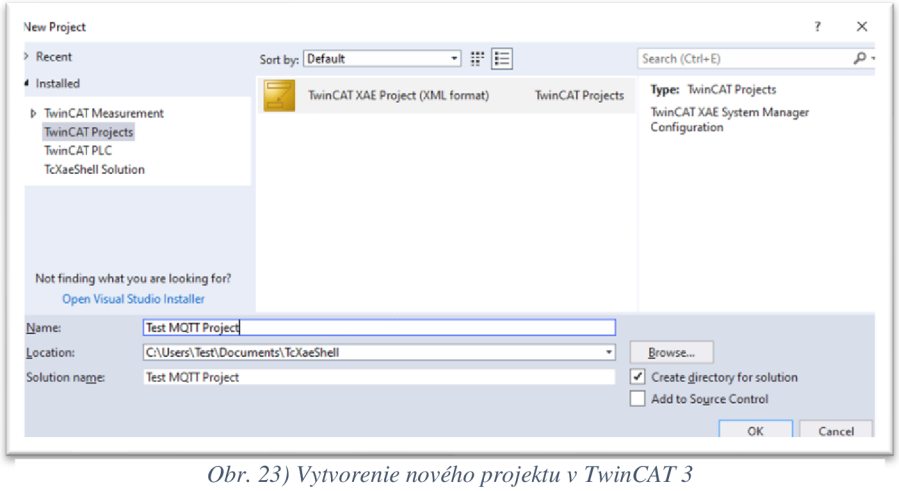
Pokiaľ Visual Studio na počítači inštalované nie je, TwinCAT nainštaluje jeho okliešteną verziu, v ktorej sú dostupné iba komponenty TwinCAT a nie je možné v ňom využívať iný jazyk. Dokumentácia uvádza upozornenie, že po inštalácii TwinCAT nie je možné doinštalovať plné Visual Studio – výsledkom môže byť nefunkčné prostredie TwinCAT. Riešením je odinštalácia TwinCAT a inštalácia oboch prostredí v správnom poradí – najprv Visual Studio, potom TwinCAT.

Prostredie TwinCAT je veľmi komplexné, pri inštalácii do systému pribudne viacero systémových služieb, bežiacich na pozadí:

Name	Description	Status	Startup Type	Log On As
TwinCAT Motion Control GST	Provides execution of g-code files...	Running	Automatic	Local Syste...
TwinCAT Nc Interpreter	Provides execution of g-code files...	Running	Automatic	Local Syste...
TwinCAT3 AdsGitServer	Provides a source control server f...	Running	Automatic	Local Syste...
TwinCAT3 Reporting Server	Reporting of data from different ...	Running	Automatic	Local Syste...
TwinCAT3 Scope Server	Allows to record data from differe...	Running	Automatic	Local Syste...
TwinCAT3 System Service	Provides background functionalit...	Running	Automatic	Local Syste...

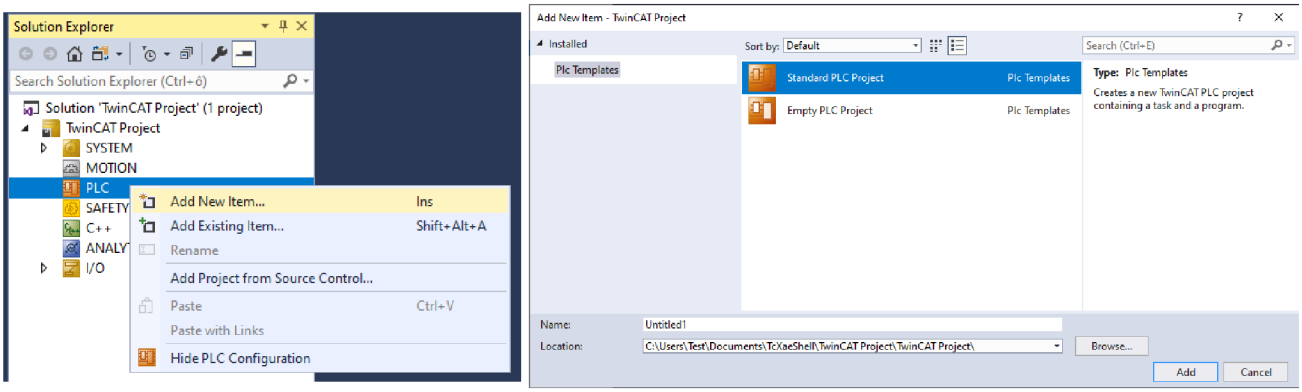
Obr. 22) Služby TwinCAT 3 XAE bežiace na pozadí

Prvým krokom konfigurácie prostredia je vytvorenie nového projektu (File -> New -> Project) typu TwinCAT XAE Project:



Obr. 23) Vytvorenie nového projektu v TwinCAT 3

Vo vytvorenom projekte vznikne základná kostra, do ktorej je vložený nový prvok typu „Standard PLC Project“:



Obr. 24) Vytvorenie PLC prokejtu v TwinCAT 3

Skôr, než môžeme plne využívať prostredie pre účely tohto príkladu, je potrebné vykonať ešte zopár úkonov:

- Pridanie potrebných modulov
- Vygenerovanie licencií
- Nastavenie zdrojov počítača

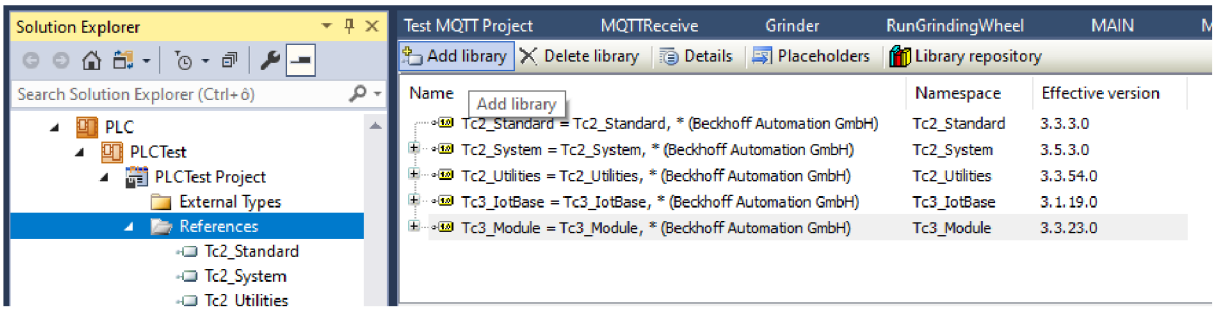
Pri vytvorení projektu sú v ňom predinštalované tri knižnice:

- Tc2_Standard – obsahuje základné funkčné bloky pre stavbu riešenia a tiež bežné programové funkcie pre podporu programovacieho jazyka
- Tc2_System – obsahuje moduly a funkcie pre spoluprácu s operačným systémom, napr. funkcie pre prácu so súbormi, systémovým časom a pod.
- Tc3_Module – je potrebný pre komunikáciu medzi komponentmi (TcCOM)

Pre potrebu modelového príkladu je nutné pridať ďalšie dve knižnice:

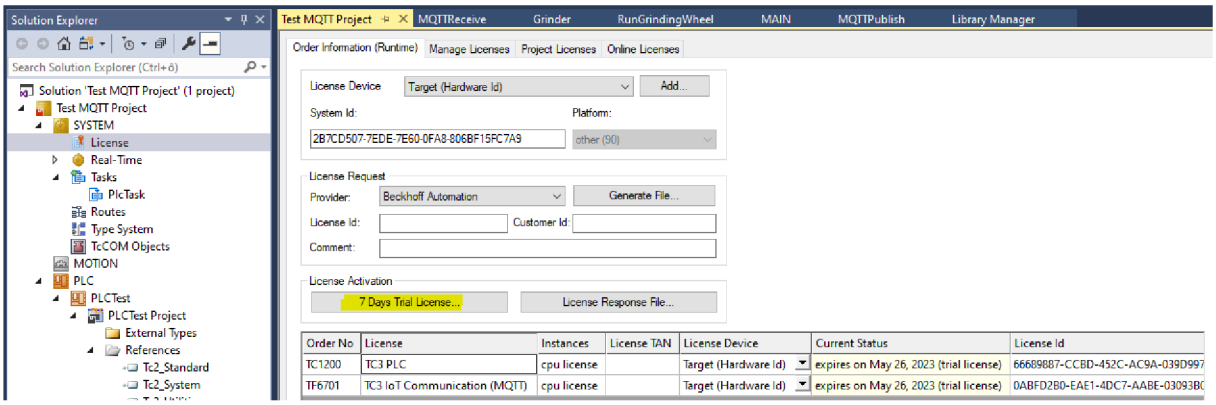
- Tc2_Utilities – obsahuje funkcie pre podporu bežných programátorských potrieb, napr. funkcie pre konverziu dátových typov, funkcie pre prácu s reťazcami a pod.
- Tc3_IotBase – knižnica z modulu TF6701 (IoT Communication), obsahujúca funkcie pre komunikáciu s MQTT serverom

Tieto knižnice sa do systému pridajú pomocou funkcie Add library v kontajneri References:



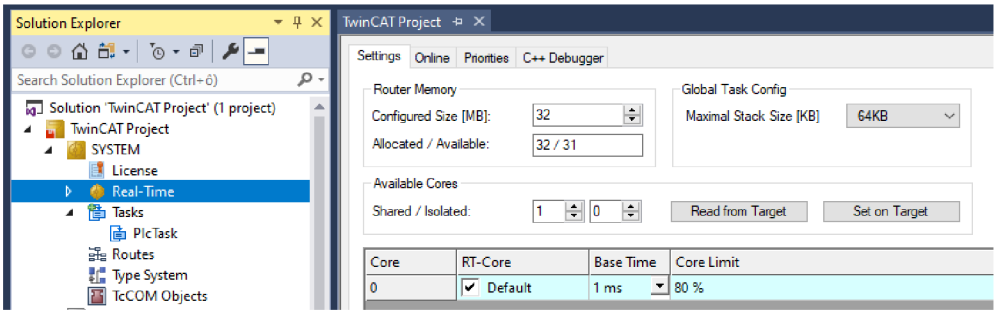
Obr. 25) Pridané knižnice programu TwinCAT 3

Niektoré z knižníc potrebujú pre svoj beh licencie. Okrem základnej knižnice pre podporu PLC je to práve knižnica pre komunikáciu s MQTT serverom. Tie sú spravované v kontajneri System/License, kde je možné aktivovať 7 dňovú trial licenciu



Obr. 26) Spravovanie licencií v programe TwinCAT 3

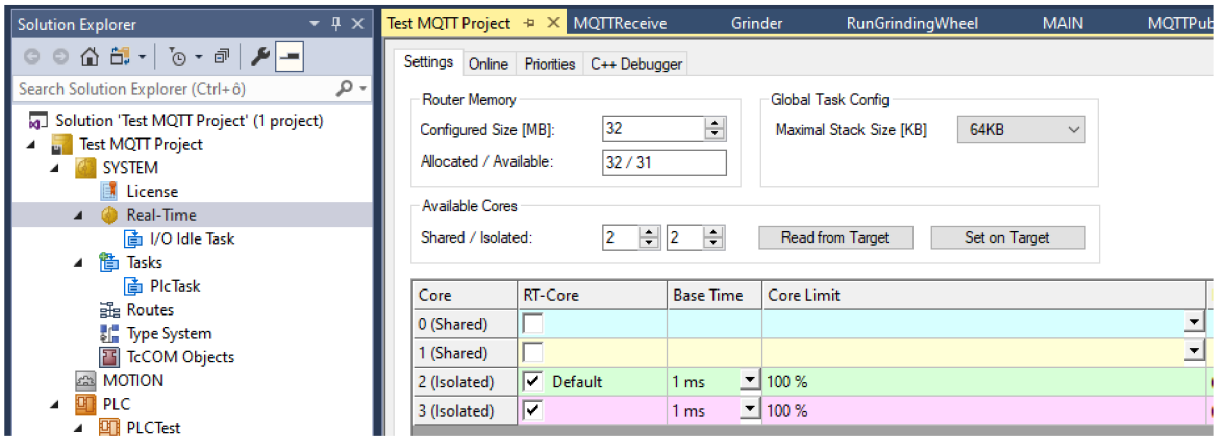
Posledným prípravným krokom prostredia je nastavenie zdrojov počítača, konkrétne pridelenie procesorov. Pri vytvorení nového projektu je defaultne použitý jediný procesor systému, ktorý však runtime nemôže zdieľať s operačným systémom, preto sa nedá spustiť:



Obr. 27) Základné nastavenie využívania jadier programom TwinCAT 3

Nastavenie procesorov sa vykoná v kontajneri SYSTEM/Real-Time. Kliknutím na tlačidlo „Read from target“ sa načítajú všetky dostupné procesory systému, a potom je možné prerozdeliť procesory pre použitie v TwinCAT runtime.

V prostredí modelového príkladu boli vyhradené dva procesory pre použitie runtime (Isolated):

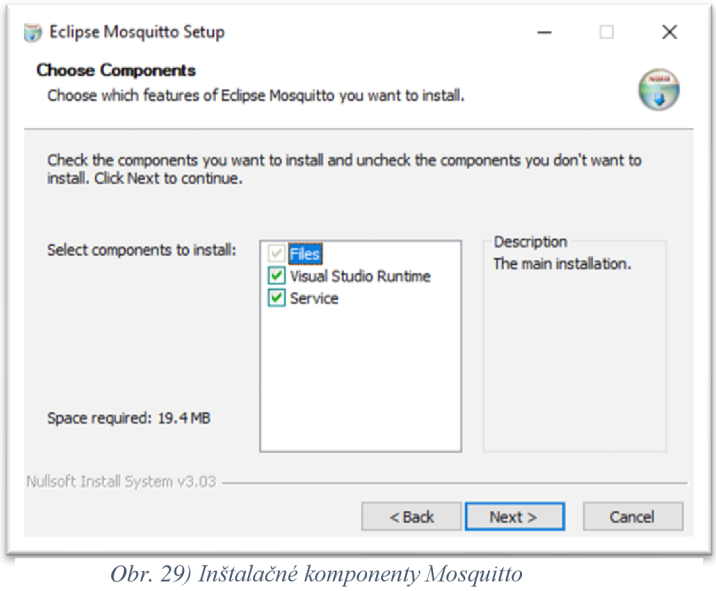


Obr. 28) Úprava nastavení využívania jadier

7.1.2 Mosquitto

Eclipse Mosquitto je odľahčený server (message broker) pre komunikáciu pomocou MQTT protokolu. V našom prípade sprostredkúva komunikáciu medzi TwinCAT 3 PLC a Node-RED, oba systémy v roli klientov.

Inštalácia je veľmi jednoduchá, použitý bol inštalátor pre 64bitovú verziu Windows, stiahnutý zo stránok výrobcu. Nastavenia v inštalácii boli ponechané v základnom stave, kedy sa inštaluje služba:

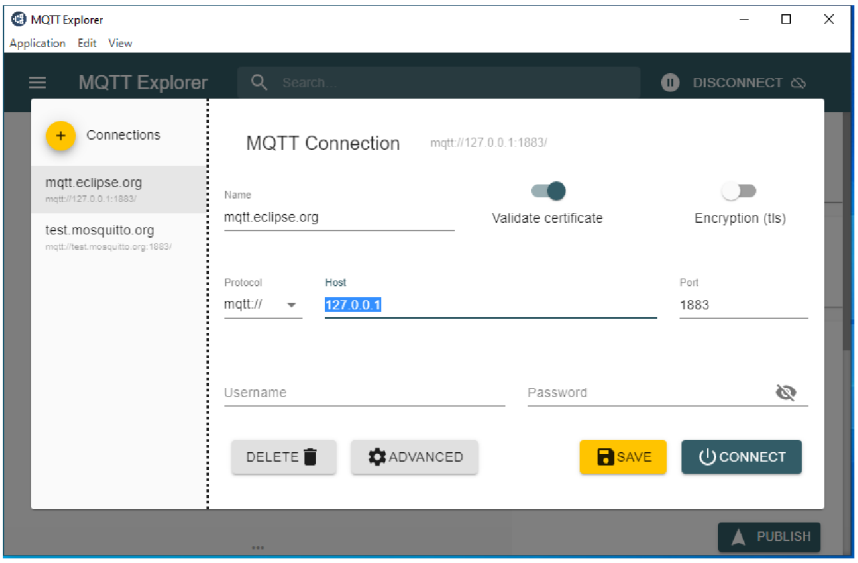


Obr. 29) Inštalačné komponenty Mosquitto

V takomto prípade nie je potrebné starať sa o spustenie servera, služba beží na pozadí a spúšťa server automaticky pri nábehu operačného systému (tesne po inštalácii je potrebné službu manuálne spustiť, alebo reštartovať počítač). V základe je Mosquitto konfigurovaný tak, že komunikuje na internej adrese operačného systému (localhost - 127.0.0.1), čo pre účely vzorového príkladu postačuje.

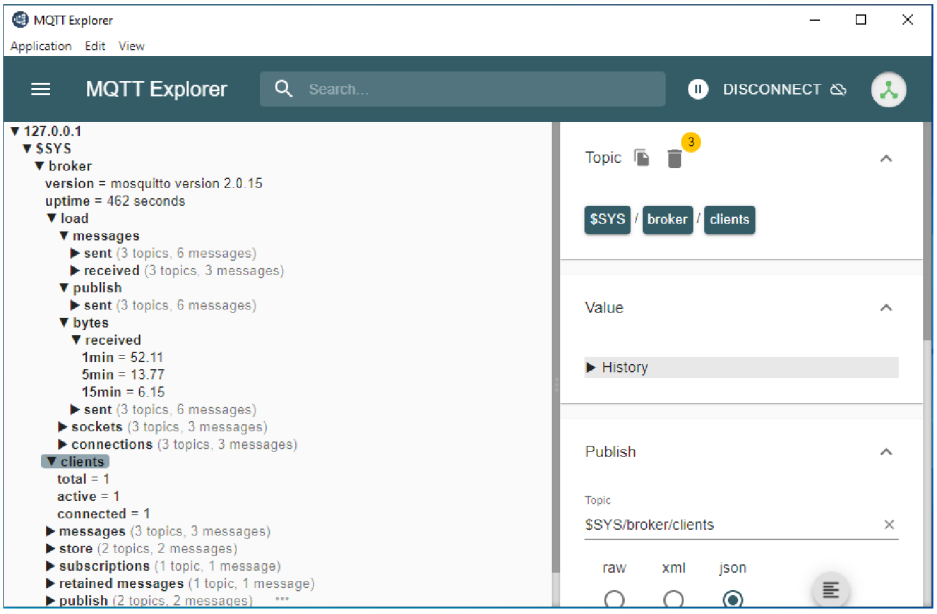
Aby bolo možné jednoduchšie ladiť komunikáciu, okrem MQTT servera bol použitý aj jednoduchý MQTT klient, umožňujúci monitorovať vnútorný stav servera a prebiehajúcu výmenu dát. Pre tieto účely bol využitý voľne dostupný nástroj „MQTT Explorer“, v našom prípade postačila „portable“ verzia bez nutnosti inštalácie.

Pri prvom spustení bolo nutné nasmerovať klienta na lokálny Mosquitto server uvedením internej adresy 127.0.0.1 (TCP port bol ponechaný na základnej hodnote 1883):



Obr.k 30) Nastavenie servera Mosquitto cez MQTT Explorer

Toto nastavenie je pre ďalšie prihlásenia už zapamätané, takže postačuje pripojiť sa k serveru tlačidlom Connect:



Obr. 31) Fungujúce prostredie MQTT Explorer

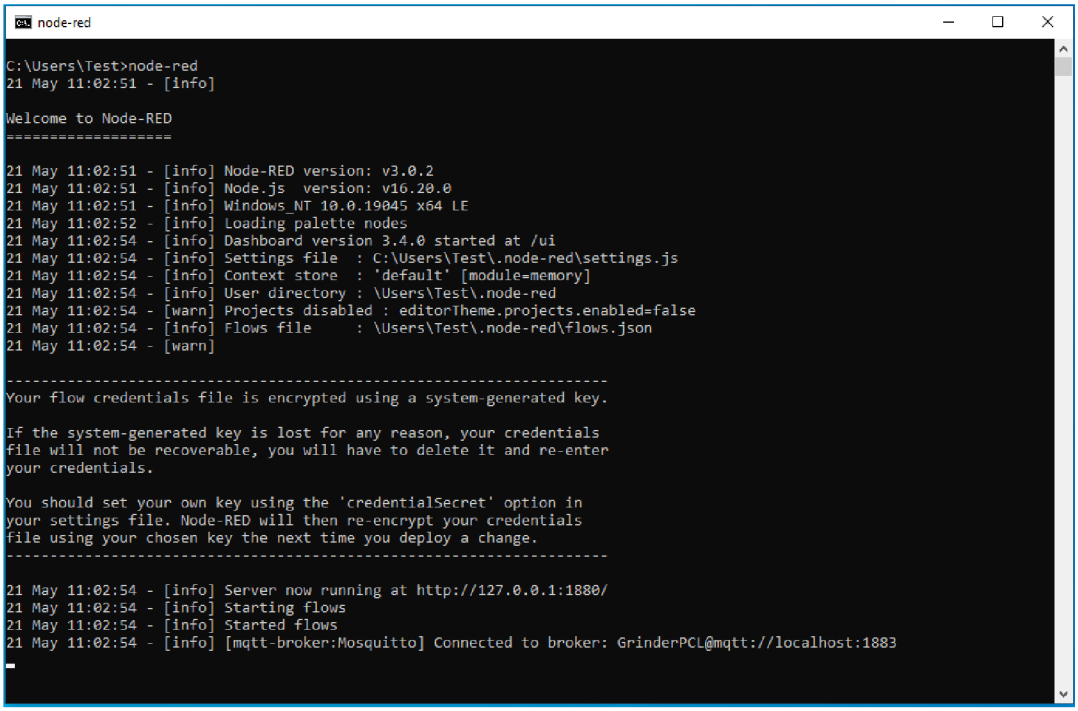
7.1.3 Node-RED

Nakoľko bolo celé prostredie budované v čerstvo nainštalovanom operačnom systéme bez akýchkoľvek doplnkov, pozostáva inštalácia Node-RED z viacerých krokov. Prvým krokom je inštalácia runtime prostredia Node.JS. Použitý bol inštalačný balík pre Windows x64 vo verzii, ktorá je odporúčaná na stránkach Node-RED (16.20). Pri inštalácii boli použité defaultné nastavenia inštalátora.

Samotný Node-RED už bol inštalovaný pomocou prostredia Node.JS s využitím správcu inštalačných balíčkov (npm) a príkazu:

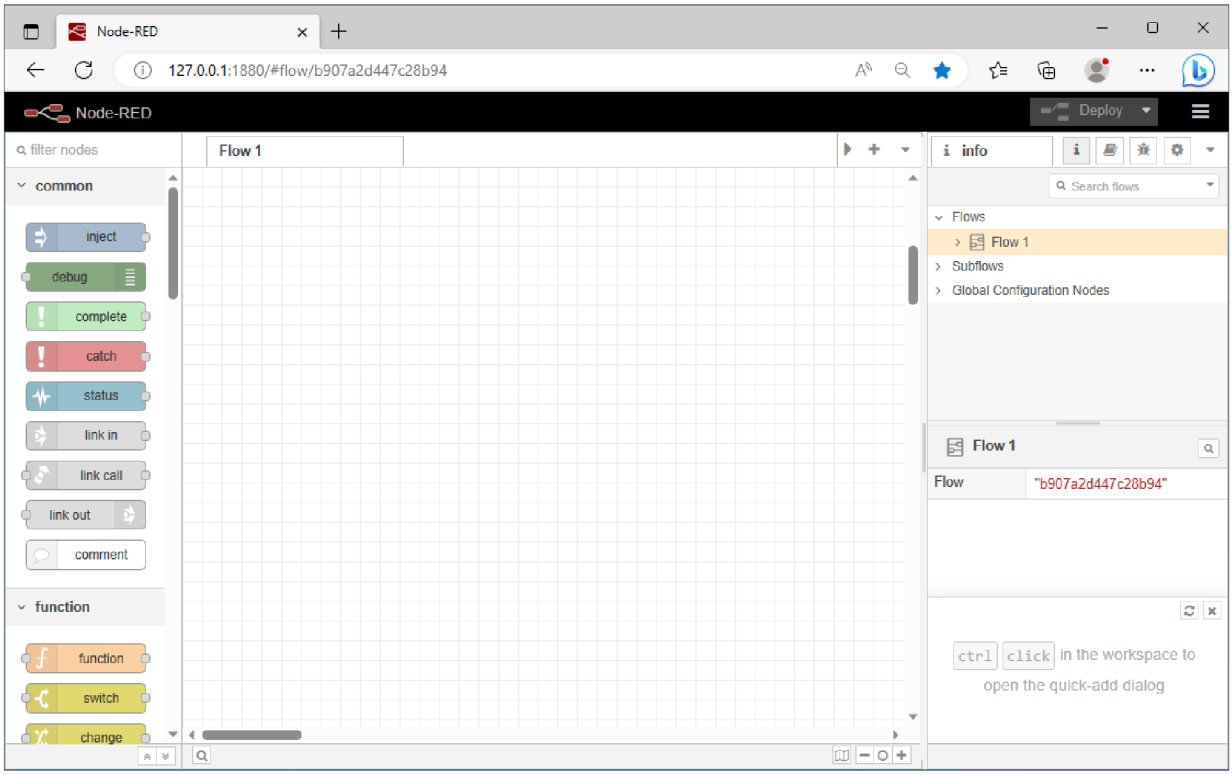
```
npm install -g --unsafe-perm node-red
```

Uvedený príkaz nainštaloval aktuálnu verziu Node-RED. Spustenie prostredia zabezpečí príkaz „node-red“, spustený z príkazového riadku Windows:



Obr. 32) Úspešné spustenie prostredia Node RED

Grafické rozhranie Node-RED je dostupné na lokálnej adrese https://127.0.0.1:1880:



Obr. 33) Grafické rozhranie Node RED

Posledným krokom prípravy prostredia Node-RED je doinštalovanie knižnice Dashboard, ktorá obsahuje grafické prvky použité pri ovládaní PLC. Inštaláciu je možné opäť vykonať pomocou správcu inštalačných balíčkov príkazom:

```
npm i node-red-dashboard
```

Druhá možnosť je použiť priamo grafické rozhranie Node-RED využitím funkcie Manage Palette priamo z hlavného menu. Tá umožňuje vyhľadávanie potrebných balíčkov a ich jednoduchú inštaláciu spolu s kontrolou kolízií s inými už nainštalovanými balíčkami.

7.2 Realizácia modelového príkladu

Modelový príklad obsahuje simuláciu PLC v programe TwinCAT 3 s riadiacou logikou pre spúšťanie fiktívneho zariadenia. V tomto prípade sa jedná o mlynček, ktorý je možné spustiť stlačením tlačidla, pričom mlynček má časový spínač s nastaviteľným intervalom, po uplynutí ktorého sa automaticky vypne. Okrem toho je definovaný bezpečnostný vypínač – tlačidlo, ktoré vypne mlynček kedykoľvek počas behu. Doba behu má byť nastaviteľná v rozsahu 1 – 10 sekúnd.

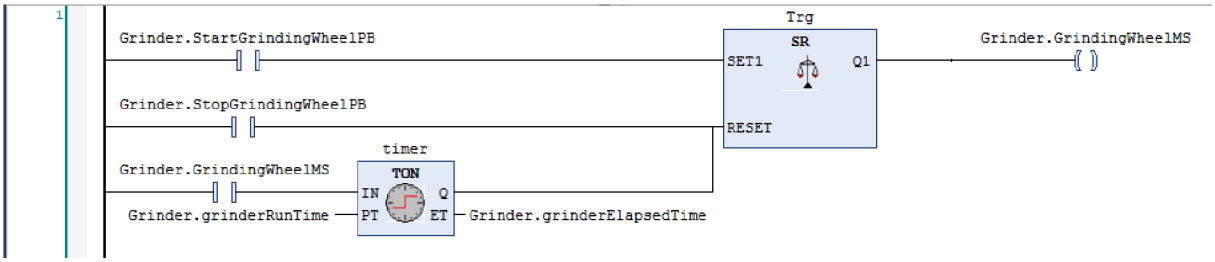
PLC program

Program je rozdelený do viacerých modulov:

Názov	Umiestnenie	Typ/jazyk	Obsah
Main	POUs	ST	Hlavná programová rutina
Grinder	GVLs	GVL	Definícia globálnych premenných
Grinder Logic	POUs	Ladder Logic	Logické zapojenie komponentov PLC programu
MQTTPublish	POUs	ST	Rutina pre publikovanie výstupov pomocou MQTT
MQTTReceive	POUs	ST	Rutina pre príjem výstupov pomocou MQTT

Tab. 7) Moduly obsiahnuté v programe

Logika PLC je vyjadrená v module GrinderLogic a je implementovaná vo formáte Ladder Logic Diagram. Vo vývojovom prostredí je táto definícia zobrazená v grafickej forme:



Obr. 34) Ladder Logic Diagram modelového programu

Vstupnými hodnotami sú signály od tlačidiel pre spúšťanie a zastavovanie mlynčeka (StartGrindingWheelPB a StopGrindingWheelPB) a nastavenie hodnoty časového spínača (grinderRunTime). Výstupom je signál pre motor mlynčeka (GrindingWheelMS).

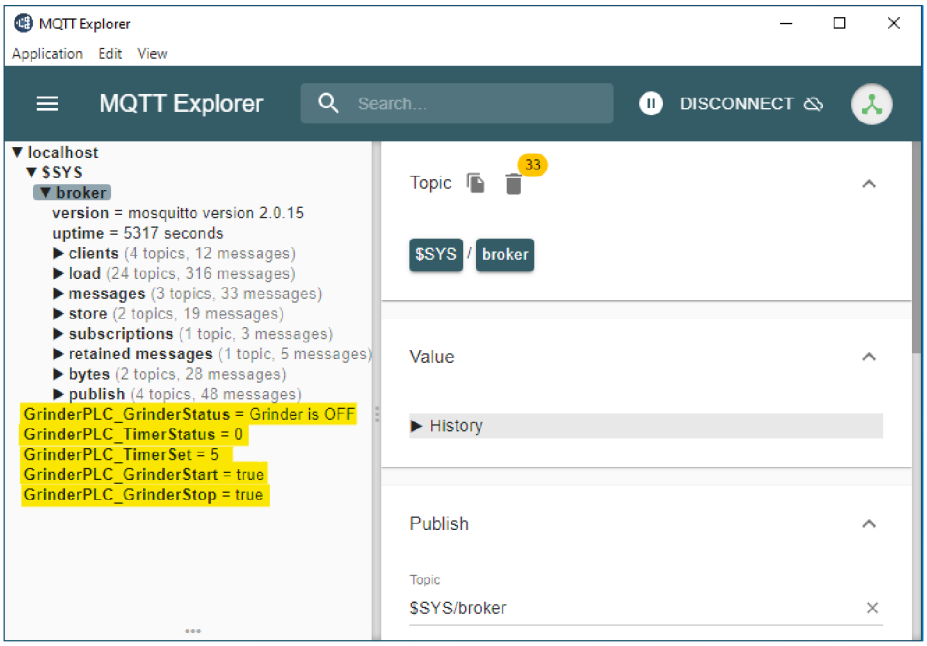
Riadenie zabezpečuje funkčný blok typu SR (bistabilný spínač), ktorý po privedení signálu na vstup SET1 (predpokladá sa signál od štartovacieho tlačidla) zopne výstup Q1 a ponechá v zopnutom stave aj po ukončení signálu SET1. Signál Q1 zostáva zopnutý až do privedenia signálu RESET (predpokladá sa signál od vypínacieho tlačidla). Celkovú logickú implementáciu je možné vyjadriť výrazom:

```
Q1: = NOT RESET1 AND (Q1 OR SET);
```

Aby bolo zabezpečené vypnutie po stanovanom čase, je na vstup RESET okrem signálu vypínacieho tlačidla paralelne zapojený časovač typu TON (reaguje na nástupnú hranu signálu), ktorý sa štartuje výstupným signálom pre motor. V momente, keď po signáli pre štart zopne motor, zapne časovač počítanie času, ktoré je nastavené na vstupe PT (vstupná hodnota pre časový spínač). Počas počítania odosiela aktuálny čas na výstup ET (elapsed time), ktorý bude využitý na odosielanie informácie o behu.

Po ukončení odpočtu času je na výstup Q časovača odoslaný signál, ktorý je privedený na resetovací vstup SR bloku a zabezpečí vypnutie motora mlynčeka. Pri ladení je možné nastavovať a kontrolovať hodnoty premenných priamo v debuggeri vývojového prostredia. Pri normálnej prevádzke PLC sa predpokladá preberanie vstupných signálov z a odosielanie výstupných hodnôt do prostredia Node-RED.

Výmenu dát s Node-RED zabezpečujú funkcie MQTTPublish a MQTTReceive. Ich účel je zrejmý z názvu, presný postup je vysvetlený v komentároch programového kódu. Pre každú z prijímaných či odosielaných hodnôt je určený samostatný kanál (topic), takže je možné výmenu dát jednoducho sledovať a kontrolovať pomocou klienta MQTT Explorer:



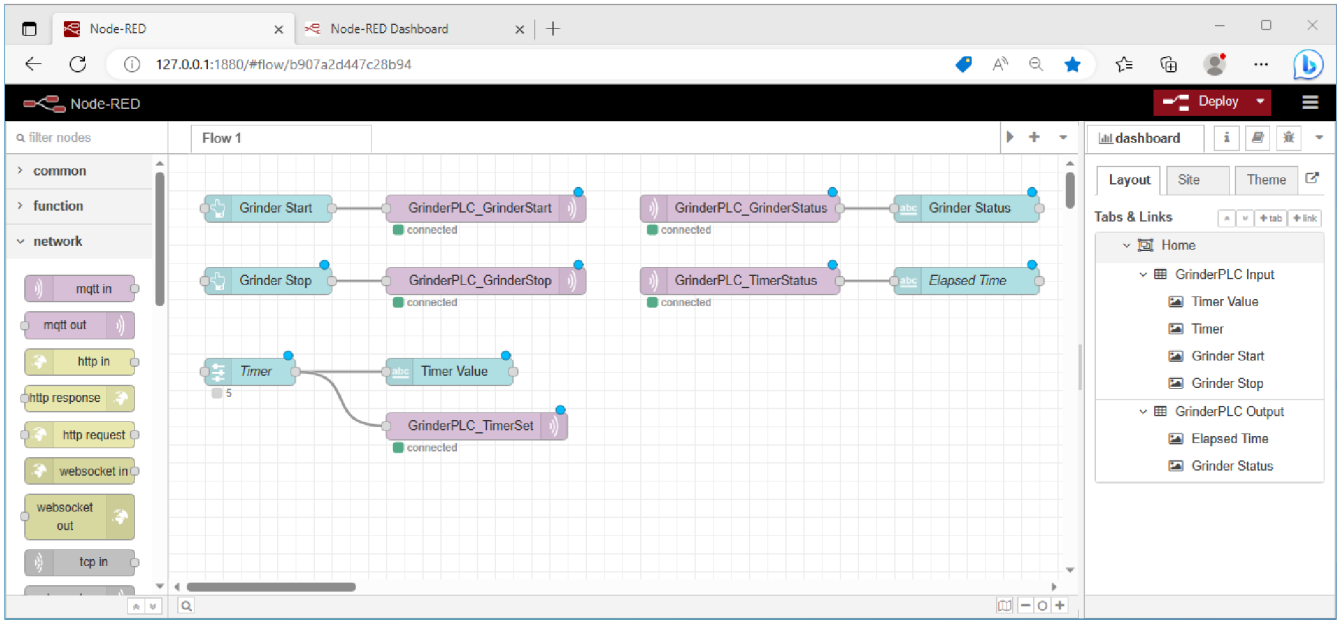
Obr. 35) Zmeny stavu programu zobrazované v nástroji MQTT Explorer

Parametre prepojenia sú nastavené priamo v procedúre MAIN, ktorá zabezpečuje hlavný cyklus programu. Tu sa v cykle vykonáva postupnosť krokov:

- Nadviazanie/obnova spojenia s MQTT (parametre spojenia sa nastavujú iba pri prvom behu cyklu)
- Načítanie vstupných hodnôt a signálov z MQTT (MQTTReceive)
- Vykonanie cyklu PLC (GrinderLogic)
- Odoslanie výstupných hodnôt do MQTT (MQTTPublish)

Node-RED

V prostredí Node-RED sú jednoduchým spôsobom definované potrebné prvky pre vstupné a výstupné hodnoty, ktoré sa odovzdávajú do, resp. preberajú zo simulovaného PLC:



Obr. Vizualizácia riadiacich prvkov v prostredí Node-RED

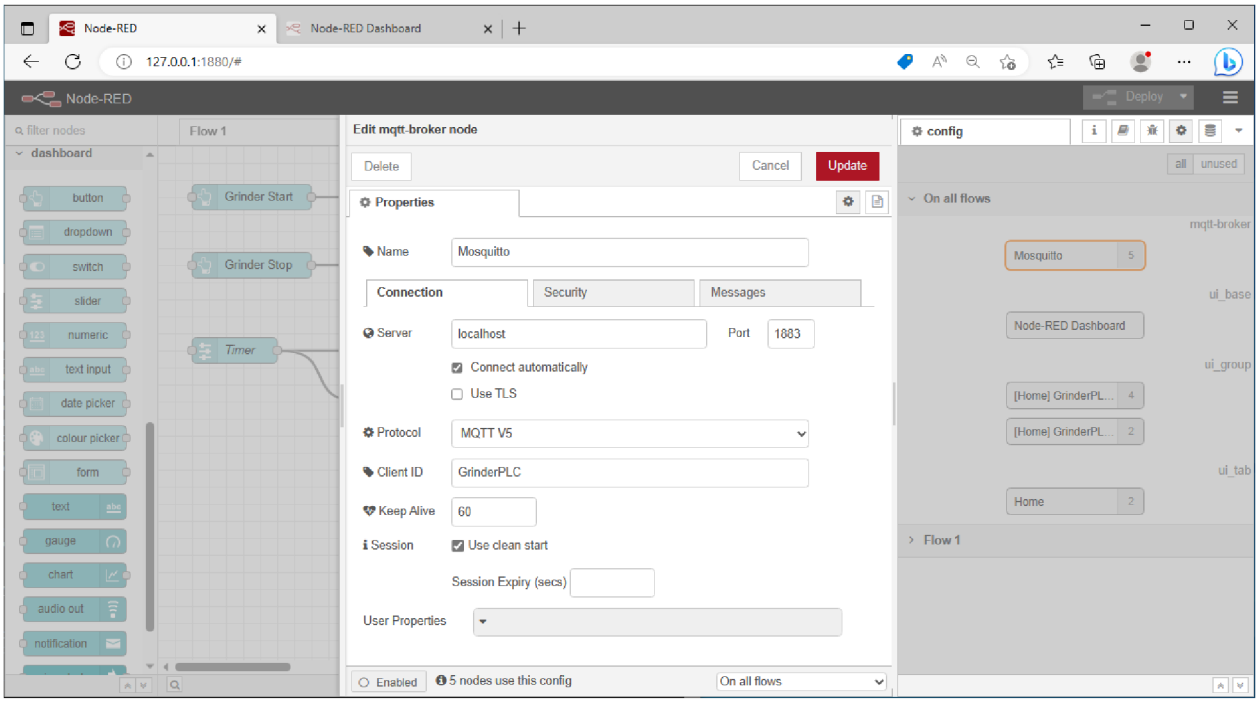
Každý prvok predstavuje spravidla dvojica navzájom prepojených objektov:

- Grafická reprezentácia prvku z knižnice Dashboard (zeleno-modrá farba)
- Komunikačný prvok MQTT z knižnice Network (fialová farba)

Výnimkou je objekt, predstavujúci nastavenie času behu motora, kde bol použitý slider (Timer) bez textového výstupu nastavenej hodnoty, čo je pomerne neprehľadné. Preto je pridaný textový prvok, ktorý danú hodnotu zobrazí (Timer Value).

Komunikácia s MQTT serverom bola definovaná pri prvom komunikačnom prvku a následne použitá pri ostatných. Pri prvotnej definícii vznikol skrytý prvok ‚mqtt-broker' obsahujúci tieto nastavenia, ktorý je možné upravovať v sekcii ‚config':

Tu sú vidieť parametre komunikácie s MQTT serverom – ako server je uvedený localhost (predstavuje internú adresu 127.0.0.1).

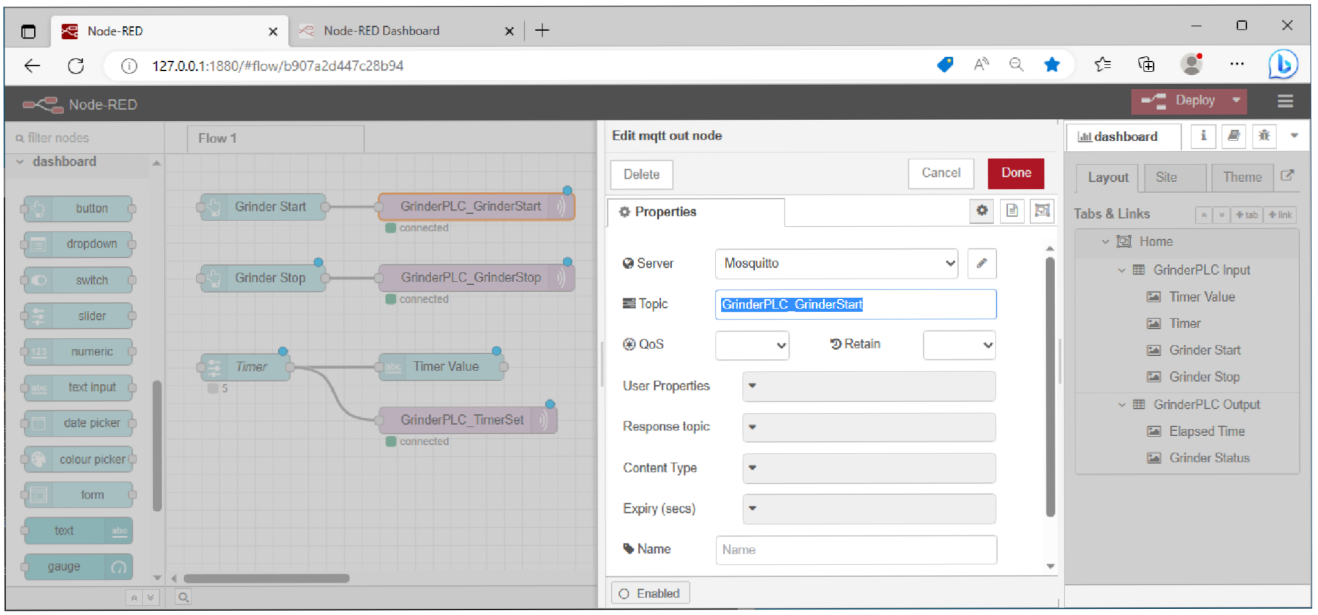


Obr. 36) Konfigurácia MQTT prvku v prostredí Node-RED

Pre prehľadné zobrazenie v grafickom prostredí boli prvky rozdelené do dvoch skupín podľa určenia:

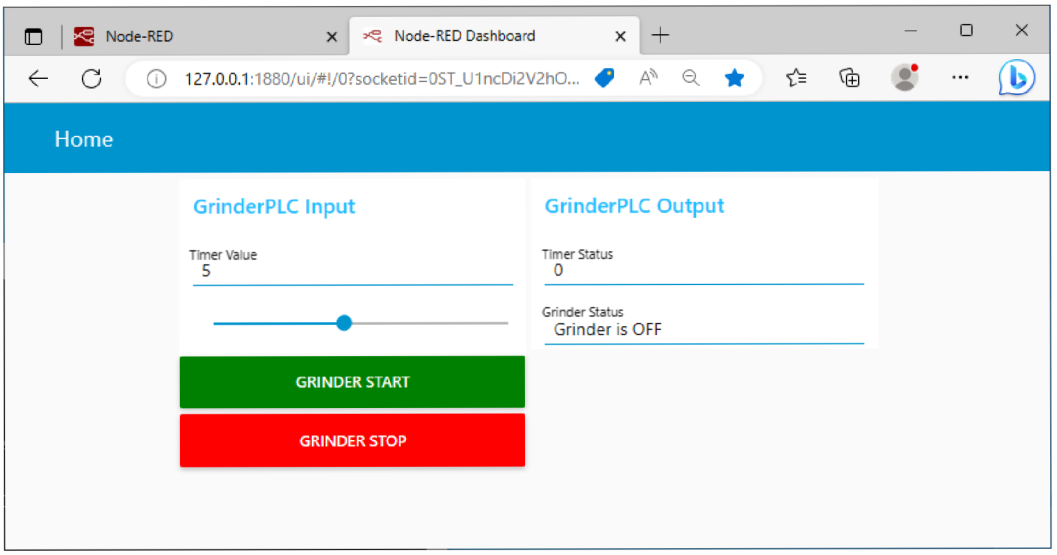
- Ovládacie prvky do skupiny GrinderPLC Input
- Zobrazovače výstupných hodnôt a stavov do skupiny GrinderPLC Output

Každý z komunikačných prvkov prenášal hodnoty vo vyhradenom kanáli (Topic). Pre všetky kanály v príklade bola zvolená spoločná predpona „GrinderPLC_“. Konfigurácia prvku bola tak urobená nasledovne:



Obr. 37) Špecifikácia komunikačného kanála (Topic)

Grafická reprezentácia bola ponechaná na samotný dashboard podľa základného nastavenia prvkov:



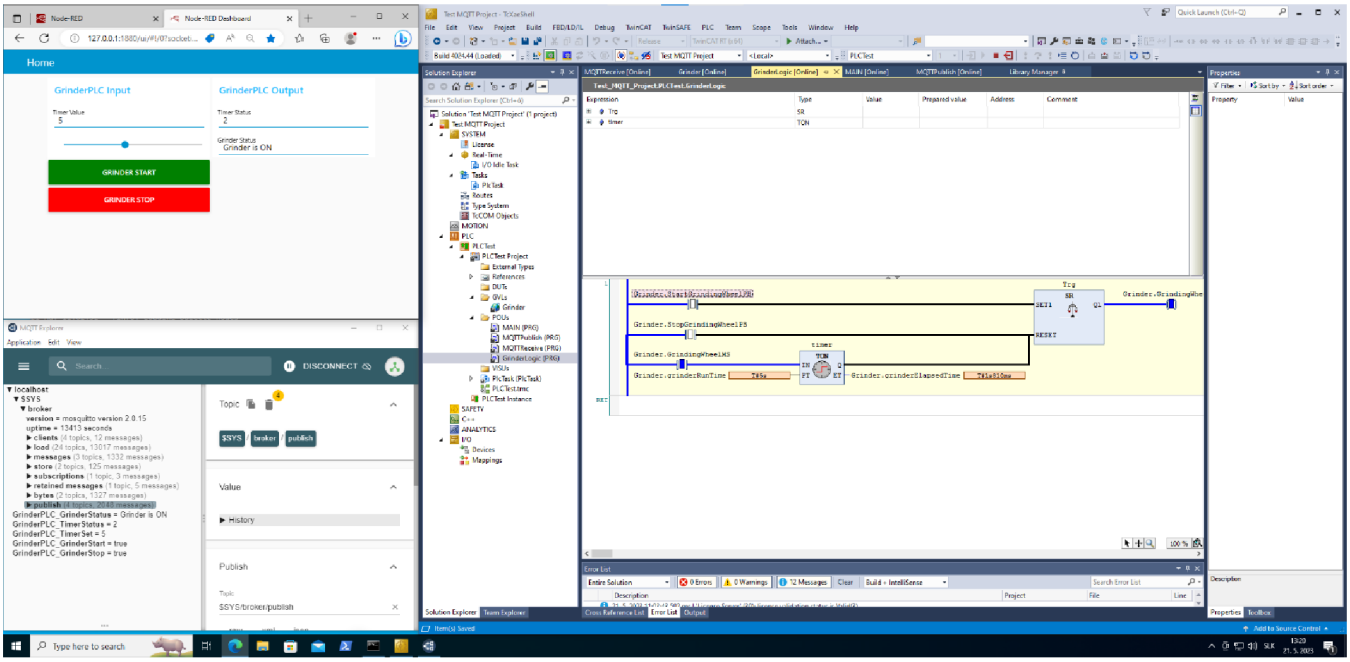
Obr. 38) Vizualizácia ovládacích prvkov simulovaného stroja

Celkový výstup

Pre spustenie simulovaného prostredia je potrebné mať rozbehnutý Node-RED (spúšťa sa manuálne príkazom ‚node-red') a spustený program PLC vo vývojovom prostredí postupnosťou príkazov:

- Activate Configuration (zahŕňa Build Solution)
- Login
- Start

Všetky príkazy sú dostupné na toolbaroch v hornej časti okna vývojového prostredia. Ovládanie z grafického prostredia ako aj sledovanie prenášaných hodnôt v MQTT brokeri a aktuálneho stavu PLC vo vývojovom prostredí je možné vidieť pri súčasnom zobrazení relevantných okien v rámci operačného systému:



Obr. 39) Sledovanie stavu všetkých spolupracujúcich programov

V ľavej časti grafického ovládacieho panelu (otvorený v okne prehliadača vľavo hore) sú vidno vstupné ovládacie prvky a parametre pre PLC, v pravej je zobrazovaný aktuálny stav. Po stlačení tlačidla GRINDER START sa spustí motor mlynčeka, čo je indikované zmenou poľa „Grinder Status" na hodnotu „Grinder is ON". Zároveň sa v poli Timer status odrátava čas, až kým nedosiahne vstupnej hodnoty „Timer Value", pri ktorej sa motor vypne, status sa zmení na „Grinder is OFF" a časovač sa vynuluje.

Ak sa počas odpočítania stlačí tlačidlo GRINDER STOP, motor sa vypne a časovač sa vynuluje. Hodnoty prenášané prostredníctvom MQTT servera sú v reálnom čase zobrazované v nástroji MQTT Explorer (okno vľavo dolu). Aktuálny stav PLC je možné sledovať aj vo vývojovom prostredí, najlepšie pri zobrazení grafickej podoby PLC (GrinderLogic).

8 ZÁVĚR

Táto bakalárska práca pojednáva o súčasnom stave priemyselných zberníc a komunikácie. Ide o neustále a dynamicky rozvíjajúce sa odvetvie priemyslu, ktoré musí pružne reagovať na zmeny požiadaviek výrobných firiem. Medzi tieto požiadavky patrí napríklad rýchlosť a spoľahlivosť prenosu dát, integrácia s rôznymi nadstavbovými systémami pre lepšie možnosti kontroly nad výrobnými procesmi a taktiež potreba vývoja nových spôsobov ochrany pred kyberútokmi.

S ohľadom na dnešný vývoj trhu a týchto požiadaviek sa dá preto tvrdiť, že klasické priemyselné zbernice budú pokračovať v ústupe, pričom ich budú nahrádzať zbernice založené na priemyselnom ethernete, ktoré posyktujú oveľa väčšiu mieru rýchlosti, spoľahlivosti a flexibility. Vylepšenia pre tieto zbernice (ako napríklad PROFINET IRT a iné) riešia problém so spoľahlivým prenosom dát v reálnom čase, čo je pre výrobné prostredie nevyhnutné.

Moderné priemyselné zbernice však potrebujú aj nadstavbové protokoly na to, aby mohli plniť spomínané požiadavky. Protokoly ako MQTT, AMQP a OPC UA sú vhodným riešením pre priemyselné systémy. Netreba zabúdať na bezdrôtové riešenia ako ZigBee alebo Wireless HART. Taktiež ostatné spomínané spôsoby komunikácie napomáhajú k implementácii inteligentných výrobných riešení.

Po tomto priereze súčasne používaných technológií nasleduje modelový príklad, ktorý má primárne slúžiť na ukážku nadviazania komunikácie pomocou už spomínaného MQTT protokolu medzi simulovaným PLC (v softvéri TwinCAT 3) a prostredím Node-RED slúžiacim pre prepojenie hardvérových zariadení a online služieb. Okrem ukážky spôsobu nadviazania komunikácie pomocou MQTT brokera obsahuje aj jednoduchý PLC program.

9 SEZNAM POUŽITÝCH ZDROJŮ

[1] *Trhový podiel priemyselných zberníc* [online]. [cit. 2023-05-23]. Dostupné z: https://www.hms-networks.com/news-and-insights/news-from-hms/2022/05/02/industrial-networks-keep-growing-despite-challenging-times

[2] *Ethernet a klasické zbernice* [online]. [cit. 2023-05-23]. Dostupné z: https://www.controlglobal.com/network/industrial-networks/article/11380197/the-ethernet-vs-fieldbus-cage-match

[3] *Komunikácia v priemyselnej automatizácii* [online]. [cit. 2023-05-23]. Dostupné z: https://elearning.mechatronika.cool/lessons/komunikacia-v-priemyselnej-automatizacii/

[4] DJIEV, Sancho, 2003. *Industrial networks for communication and control*. Technical University of Sofia (2003).

[5] JALOUDI, Samer. Communication Protocols of an Industrial Internet of Things Environment: A Comparative Study. *Future Internet* [online]. 2019, **11**(3) [cit. 2023-05-23]. ISSN 1999-5903.

[6] ANITHA, T., S. MANIMURUGAN, S. SRIDHAR, S. MATHUPRIYA a G. Charlyn Pushpa LATHA. A Review on Communication Protocols of Industrial Internet of Things. In: *2022 2nd International Conference on Computing and Information Technology (ICCIT)* [online]. IEEE, 2022, 2022-1-25, s. 418-423 [cit. 2023-05-23]. ISBN 978-1-6654-3605-2

[7] *Použitia MQTT protokolu* [online]. [cit. 2023-05-23]. Dostupné z: https://www.influxdata.com/blog/mqtt-use-cases/

[8] *Integrácia MQTT protokolu* [online]. [cit. 2023-05-23]. Dostupné z: https://www.yglworld.com/mqtt-integration/

[9] *Interoperabilita MQTT a OPC UA* [online]. [cit. 2023-05-23]. Dostupné z: https://opcconnect.opcfoundation.org/2021/12/opc-ua-mqtt-and-information-interoperability/

[10] *OPC UA model* [online]. [cit. 2023-05-23]. Dostupné z: https://prosysopc.com/blog/opc-ua-pubsub-explained/

[11] *Použitia OPC UA protokolu* [online]. [cit. 2023-05-23]. Dostupné z: https://opcconnect.opcfoundation.org/2021/06/opc-ua-is-in-the-air-lots-of-use-cases/

[12] *Zabezpečenie OPC UA protokolu* [online]. [cit. 2023-05-23]. Dostupné z: https://www.ptc.com/en/blogs/iiot/opc-ua-security

[13] *OPC UA v priemysle* [online]. [cit. 2023-05-23]. Dostupné z: https://opcconnect.opcfoundation.org/2021/06/opc-ua-cybersecurity-and-smart-manufacturing/

[14] GARCÍA-RETUERTA, David, Roberto CASADO-VARA a Javier PRIETO. Enhanced Cybersecurity in Smart Cities: Integration Methods of OPC UA and Suricata. In: CORCHADO, Juan M. a Saber TRABELSI, ed. *Sustainable Smart Cities and Territories* [online]. Cham: Springer International Publishing, 2022, 2022-07-31, s. 61-67 [cit. 2023-05-23]. Lecture Notes in Networks and Systems.ISBN 978-3-030-789008

[15] IGLESIAS-URKIA, Markel, Adrián ORIVE a Aitor URBIETA. Analysis of CoAP Implementations for Industrial Internet of Things: A Survey. *Procedia Computer Science* [online]. 2017, **109**, 188-195 [cit. 2023-05-23]. ISSN 18770509S

[16] *CoAP protokol* [online]. [cit. 2023-05-23]. Dostupné z: https://medium.com/@harshhvm/what-is-coap-protocol-coap-protocol-introduction-overview-3e8bac4d7f8e

[17] SHELBY, Z. The Constrained Application Protocol (CoAP) [online]. June 2014 [cit. 2023-05-23]. Request For Comments (RFC) 7252. Dostupný z: https://www.rfc-editor.org/rfc/rfc7252#section-9

[18] *Zabezpečenie AMQP klientov* [online]. [cit. 2023-05-23]. Dostupné z: https://www.ibm.com/docs/en/ibm-mq/8.0?topic=security-securing-amqp-clients

[19] *Popis AMQP* [online]. [cit. 2023-05-23]. Dostupné z: https://www.amqp.org/about/what

[20] GEMIRTER, Cavide Balki, Cagatay SENTURCA a Sebnem BAYDERE. A Comparative Evaluation of AMQP, MQTT and HTTP Protocols Using Real-Time Public Smart City Data. In: *2021 6th International Conference on Computer Science and Engineering (UBMK)* [online]. IEEE, 2021, 2021-9-15, s. 542-547 [cit. 2023-05- 23]. ISBN 978-1-6654-2908-5

[21] UY, Nguyen Quoc a Vu Hoai NAM. A comparison of AMQP and MQTT protocols for Internet of Things. In: *2019 6th NAFOSTED Conference on Information and Computer Science (NICS)* [online]. IEEE, 2019, 2019, s. 292-297 [cit. 2023-05-23]. ISBN 978-1-7281-5163-2.s

[22] *Integrácia AMQP protokolu a MS Azure* [online]. [cit. 2023-05-23]. Dostupné z: https://learn.microsoft.com/en-us/azure/service-bus-messaging/service-bus-amqp-protocol-guide

[23] CAIZA, Gustavo, Erick S. LLAMUCA, Carlos A. GARCIA, Fabian GALLARDO-CARDENAS, David LANAS a Marcelo V. GARCIA. Industrial Shop-Floor Integration Based on AMQP protocol in an IoT Environment. In: *2019 IEEE Fourth Ecuador Technical Chapters Meeting (ETCM)* [online]. IEEE, 2019, 2019, s. 1-6 [cit. 2023-05- 23]. ISBN 978-1-7281-3764-3.

[24] *MQTT over WebSocket* [online]. [cit. 2023-05-23]. Dostupné z: https://www.hivemq.com/blog/mqtt-essentials-special-mqtt-over-websockets/

[25] *Protocol Buffers* [online]. [cit. 2023-05-23]. Dostupné z: https://protobuf.dev/overview/

[26] STRLJIC, Matthias Milan, Chris VOLLMANN a Oliver RIEDEL. Shop-Floor Service Connector - a message-oriented Middleware Focused on the Usability and Infrastructure Requirements of SMEs Developing Smart Services. In: *2020 3rd IEEE International Conference on Knowledge Innovation and Invention (ICKII)* [online]. IEEE, 2020, 2020-8-21, s. 37-40 [cit. 2023-05-23]. ISBN 978-1-7281-9333-5.S

[27] SERIZAWA, Yasutaka a Yusuke SHOMURA, 2019. A Loosely Coupled Sensing System Architecture and Implementation for Industrial IoT.*Sensors & Transducers* [online]. IFSA Publishing, S. L [cit. 2023-05-23]. Dostupné z: www.sensorsportal.com/HTML/DIGEST/november_2019/Vol_238/P_3134.pdf

[28] *Úvod do SignalR* [online]. [cit. 2023-05-23]. Dostupné z: https://learn.microsoft.com/en-us/aspnet/signalr/overview/getting-started/introduction-to-signalr

[29] SCROPPO, Marco-Stefano, 2019. *Enhancing interoperability in industry 4.0*. Doctoral Thesis. Università di Catania. [cit. 2023-05-23] Dostupné z: http://hdl.handle.net/10761/4151

[30] *Štandard ISA/IEC 62443* [online]. [cit. 2023-05-23]. Dostupné z: https://www.cisco.com/c/en/us/td/docs/solutions/Verticals/IoT_Security_Lab/IEC62443_WP.pdf

[31] *Hirschmann EAGLE ONE Security Router* [online]. [cit. 2023-05-23]. Dostupné z: https://www.hirschmann.com/en/Hirschmann_Produkte/Industrial_Ethernet/security-firewall/EAGLE_One_Security_Router_/index.phtml

[32] *Typy firewallov* [online]. [cit. 2023-05-23]. Dostupné z: https://www.techtarget.com/searchsecurity/feature/The-five-different-types-of-firewalls

[33] HU, Yan, An YANG, Hong LI, Yuyan SUN a Limin SUN. A survey of intrusion detection on industrial control systems. *International Journal of Distributed Sensor Networks* [online]. 2018, 14(8) [cit. 2023-05-23]. ISSN 1550-1477. S

[34] *IDS systém* [online]. [cit. 2023-05-23]. Dostupné z: https://www.fortinet.com/resources/cyberglossary/intrusion-detection-system

[35] *Typy IDS systémov* [online]. [cit. 2023-05-23]. Dostupné z: https://www.fortinet.com/resources/cyberglossary/what-is-an-ips

[36] *SSL protokol* [online]. [cit. 2023-05-23]. Dostupné z: https://www.ssl.com/faqs/faq-what-is-ssl/

[37] *SSH protokol* [online]. [cit. 2023-05-23]. Dostupné z: https://www.ssh.com/academy/ssh/ssh-key-basics

[38] *Skupina protokolov IPsec* [online]. [cit. 2023-05-23]. Dostupné z: https://www.cloudflare.com/learning/network-layer/what-is-ipsec/

[39] *Cloudové zabezpečenie* [online]. [cit. 2023-05-23]. Dostupné z: https://www.ibm.com/topics/cloud-security

[40] *Data loss prevention (DLP)* [online]. [cit. 2023-05-23]. Dostupné z: https://www.microsoft.com/en-us/security/business/security-101/what-is-data-loss-prevention-dlp

[41] *SIEM* [online]. [cit. 2023-05-23]. Dostupné z: https://www.ibm.com/topics/siem

[42] *Výhody a nevýhody priemyselných zberníc* [online]. [cit. 2023-05-23]. Dostupné z: https://library.automationdirect.com/industrial-ethernet-or-fieldbus-network/

[43] *Priemyselný ethernet* [online]. [cit. 2023-05-23]. Dostupné z: https://www.rtautomation.com/industrial-library/what-is-industrial-ethernet/

[44] *PROFINET* [online]. [cit. 2023-05-23]. Dostupné z: https://us.profinet.com/profinet-explained/

[45] *OSI model PROFINET* [online]. [cit. 2023-05-23]. Dostupné z: https://profinetuniversity.com/industrial-automation-ethernet/network-reference-model/

[46] *Protokoly používané súbežne s PROFINET* [online]. [cit. 2023-05-23]. Dostupné z: https://us.profinet.com/can-profinet-and-ethernet-employ-the-same-switch/

[47] *Triedy zhodnosti PROFINET* [online]. [cit. 2023-05-23]. Dostupné z: https://www.profibus.com/index.php?eID=dumpFile&t=f&f=44266&token=1d81c134b224334c62d388673080f12267581e62

[48] *Topológie PROFINET* [online]. [cit. 2023-05-23]. Dostupné z: https://us.profinet.com/wp-content/uploads/2019/08/Topology.pdf

[49] *Zabezpečenie PROFINET* [online]. [cit. 2023-05-23]. Dostupné z: https://www.infoplc.net/files/descargas/phoenix_contact/infoplc_net_cml3_profinet_basics_students_checked.pdf

[50] *Triedy zabezpečenia PROFINET* [online]. [cit. 2023-05-23]. Dostupné z: https://profinews.com/2023/01/profinet-security-classes-1-2-3/

[51] *Adaptéry FENA* [online]. [cit. 2023-05-23]. Dostupné z: https://new.abb.com/drives/connectivity/fieldbus-connectivity/profinet/fena-21

[52] *CIP protokol* [online]. [cit. 2023-05-23]. Dostupné z: https://www.odva.org/wp-content/uploads/2020/06/PUB00123R1_Common-Industrial_Protocol_and_Family_of_CIP_Networks.pdf

[53] *CIP protokol základy* [online]. [cit. 2023-05-23]. Dostupné z: https://www.odva.org/technology-standards/key-technologies/common-industrial-protocol-cip/

[54] *Princípy komunikácie EtherNET/IP* [online]. [cit. 2023-05-23]. Dostupné z: https://scadahacker.com/library/Documents/ICS_Protocols/Schneider%20-%20Principles%20of%20EtherNetIP%20Communication.pdf

[55] WIBERG, Joakim, David SMITH a Jack VISOKY. *Expanding CIP Security™ with the CIP Authorization Profile* [online]. [cit. 2023-05-23]. Dostupné z: https://www.odva.org/wp-content/uploads/2022/03/2022-ODVA-Conference_CIP_Authorization_Profile_Smith-Visoky-Wiberg_FINAL.pdf

[56] *OSI model* [online]. [cit. 2023-05-25]. Dostupné z: https://sk.wikipedia.org/wiki/Model_OSI#/media/S%C3%BAbor:OSI_Model_v1.svg

[57] *OSI model vs TCP/IP model* [online]. [cit. 2023-05-25]. Dostupné z: https://encyklopediapoznania.sk/clanok/275/pocitacove-siete-tcp-ip-referencny-model

[58] *MQTT model* [online]. [cit. 2023-05-25]. Dostupné z: https://www.bivocom.com/blog/bivocom-has-added-mqtt-protocol-to-its-routers-and-gateways

[59] *OPC UA rozsah* [online]. [cit. 2023-05-25]. Dostupné z: https://opcconnect.opcfoundation.org/2021/09/flc-corner-september-2021/

[60] *Logo PROFIBUS* [online]. [cit. 2023-05-25]. Dostupné z: https://en.wikipedia.org/wiki/Profibus#/media/File:PROFIBUS_rgb_2010.png

[61] *PROFIBUS OSI model* [online]. [cit. 2023-05-25]. Dostupné z: https://us.profinet.com/profibus_tech/iso-osi-model/S

[62] *PROFIBUS návod* [online]. [cit. 2023-05-25]. Dostupné z: https://www.profibus.com/index.php?eID=dumpFile&t=f&f=51702&token=285ebc6925fc6d2d2ad000ee5452095c44ac17a1

[63] *PROFINET logo* [online]. [cit. 2023-05-25]. Dostupné z: https://us.profinet.com/webinar/an-introduction-to-profinet/

[64] *EtherNET/IP* [online]. [cit. 2023-05-25]. Dostupné z: https://realpars.com/ethernet-ip/

[65] *CIP object model* [online]. [cit. 2023-05-25]. Dostupné z: https://literature.rockwellautomation.com/idc/groups/literature/documents/um/857-um005_-en-p.pdf

10 SEZNAM ZKRATEK, SYMBOLŮ, OBRÁZKŮ A TABULEK

10.1 Seznam tabulek

10.2 Seznam obrázků