Zabezpečení síťového připojení automatizované linky na platformě Siemens TIA Portal

Vojtěch Bartoň

Bakalářská práce
2018

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky
akademický rok: 2017/2018

ZADÁNÍ BAKALÁŘSKÉ PRÁCE
(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení:	**Vojtěch Bartoň**
Osobní číslo:	**A14157**
Studijní program:	**B3902 Inženýrská informatika**
Studijní obor:	**Bezpečnostní technologie, systémy a management**
Forma studia:	**kombinovaná**
Téma práce:	**Zabezpečení síťového připojení automatizované linky na platformě Siemens TIA Portal**
Téma anglicky:	**Assuring the Network Connection of an Automated Production-line on the Siemens TIA Portal Platform**

Zásady pro vypracování:

1. **Charakterizujte vývojové prostředí Tia Portal od společnosti Siemens.**
2. **Navrhněte projekt automatizované výrobní linky a vizualizace HMI na platformě Tia Portal.**
3. **Realizujte zabezpečené připojení výrobní linky do sítě Internet.**
4. **Vytvořte a zabezpečte webový server PLC s vybranými informacemi o procesu a stavu výrobních zařízení.**
5. **Vytvořte VPN tunel sloužící k bezpečnému vzdálenému připojení na řídící PLC výrobních zařízení.**

Rozsah bakalářské práce:

Rozsah příloh:

Forma zpracování bakalářské práce: **tištěná/elektronická**

Seznam odborné literatury:

1. **Automating with SIMATIC: Hardware and Software, Configuration and Programming, Data Communication, Operator Control and Monitoring, Hans Berger, 2016, ISBN: 978-3-89578-459-0.**
2. **Automating with SIMATIC S7-1500: Configuring, Programming and Testing with STEP 7 professional, Hans Berger, 2014, ISBN: 978-3-89578-404-0**
3. **HRUŠKA, František a Ladislav ŠMEJKAL. Technické prostředky informatiky a automatizace: (úvod, popis funkce, konstrukce a aplikace). Vyd. 1. Ve Zlíně: Univerzita Tomáše Bati, 2007, 193 s. ISBN 978-807-3185-350.**
4. **ŠMEJKAL, Ladislav a Marie MARTINÁSKOVÁ. PLC a automatizace. Praha: BEN – technická literatura, 1999. ISBN 9788086056586.**
5. **ŠMEJKAL, Ladislav. PLC a automatizace 2. Praha: BEN – technická literatura, 2005. ISBN 80-7300-087-3.**

Vedoucí bakalářské práce: **Ing. Petr Dostálek, Ph.D.**
Ústav automatizace a řídicí techniky

Datum zadání bakalářské práce: **12. prosince 2017**

Termín odevzdání bakalářské práce: **24. května 2018**

Ve Zlíně dne 12. prosince 2017

UNIVERZITA TOMÁŠE BATI VE ZLÍNĚ
Fakulta aplikované informatiky
L.S.

doc. Mgr. Milan Adámek, Ph.D.
děkan

Ing. Jan Valouch, Ph.D.
ředitel ústavu

Prohlašuji, že

- beru na vědomí, že odevzdáním bakalářské práce souhlasím se zveřejněním své práce podle zákona č. 111/1998 Sb. o vysokých školách a o změně a doplnění dalších zákonů (zákon o vysokých školách), ve znění pozdějších právních předpisů, bez ohledu na výsledek obhajoby;
- beru na vědomí, že bakalářská práce bude uložena v elektronické podobě v univerzitním informačním systému dostupná k prezenčnímu nahlédnutí, že jeden výtisk diplomové/bakalářské práce bude uložen v příruční knihovně Fakulty aplikované informatiky Univerzity Tomáše Bati ve Zlíně a jeden výtisk bude uložen u vedoucího práce;
- byl/a jsem seznámen/a s tím, že na moji bakalářskou práci se plně vztahuje zákon č. 121/2000 Sb. o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon) ve znění pozdějších právních předpisů, zejm. § 35 odst. 3;
- beru na vědomí, že podle § 60 odst. 1 autorského zákona má UTB ve Zlíně právo na uzavření licenční smlouvy o užití školního díla v rozsahu § 12 odst. 4 autorského zákona;
- beru na vědomí, že podle § 60 odst. 2 a 3 autorského zákona mohu užít své dílo – diplomovou/bakalářskou práci nebo poskytnout licenci k jejímu využití jen připouští-li tak licenční smlouva uzavřená mezi mnou a Univerzitou Tomáše Bati ve Zlíně s tím, že vyrovnání případného přiměřeného příspěvku na úhradu nákladů, které byly Univerzitou Tomáše Bati ve Zlíně na vytvoření díla vynaloženy (až do jejich skutečné výše) bude rovněž předmětem této licenční smlouvy;
- beru na vědomí, že pokud bylo k vypracování bakalářské práce využito softwaru poskytnutého Univerzitou Tomáše Bati ve Zlíně nebo jinými subjekty pouze ke studijním a výzkumným účelům (tedy pouze k nekomerčnímu využití), nelze výsledky bakalářské práce využít ke komerčním účelům;
- beru na vědomí, že pokud je výstupem bakalářské práce jakýkoliv softwarový produkt, považují se za součást práce rovněž i zdrojové kódy, popř. soubory, ze kterých se projekt skládá. Neodevzdání této součásti může být důvodem k neobhájení práce.

Prohlašuji,

- že jsem na bakalářské práci pracoval samostatně a použitou literaturu jsem citoval. V případě publikace výsledků budu uveden jako spoluautor.
- že odevzdaná verze bakalářské práce a verze elektronická nahraná do IS/STAG jsou totožné.

Ve Zlíně, dne 21.5.2018

.....

podpis diplomanta

ABSTRAKT

Bakalářská práce si klade za cíl charakterizovat problematiku síťového zabezpečení průmyslového zařízení s řídicím PLC Siemens na platformě TIA Portal. Vytvoření modelového projektu zabezpečení výrobní linky, vytvoření Webového serveru PLC a vzdáleného připojení na zařízení, vše za pomocí komunikačních modulů Siemens Scalance řady S. Výstupem je vzorový příklad zabezpečení zařízení s řídicím PLC Siemens.

V teoretické části jsou popsány vybrané technologie, doporučené postupy a techniky pro práci s PLC a zabezpečení síťového připojení.

Praktická část je zaměřena na vytvoření projektu výrobní linky, zabezpečeného webového serveru řídicího PLC s informacemi o zařízení a vytvoření bezpečné VPN pro vzdálenou správu na zařízení.

Klíčová slova: PLC programování, vizualizace, síťové zabezpečení, webový server

ABSTRACT

The bachelor thesis aims to characterize the problem of network security of industrial equipment with the PLC Siemens on the TIA Portal platform. Creating of model project securing production line, created by the Web server PLC and remote connection to the device using Siemens Scalance series S. The output is a sample example of device security with PLC Siemens PLC.

The theoretical part describes selected technologies, best practices and techniques for working with PLC and security of network connection.

The practical part focuses on creating a production line project, secured PLC web server with device information, and creating a secure VPN for remote management of device.

Keywords: PLC programming, visualization, network security, web server

Tímto bych chtěl poděkovat Ing. Petru Dostálkovi, Ph.D. za cenné rady a doporučení poskytnuté na konzultacích při tvorbě této bakalářské práce. Současně bych rád poděkoval mému zaměstnavateli, firmě CBG Impex s.r.o., za poskytnutí technického vybavení k realizaci projektu.

Prohlašuji, že odevzdaná verze bakalářské práce a verze elektronická nahraná do IS/STAG jsou totožné.

OBSAH

ÚVOD

Automatizační technika od společnosti SIEMENS má za sebou dlouholeté zkušenosti a vývoj, který se promítá do vývojového prostředí softwaru TIA Portal. Software je orientován na uživatele a zároveň na funkčnost, která sdružuje všechny důležité funkce při práci s automatizační technikou.

Průmyslová automatizace se neustále vyvíjí. V roce 2013 byl představen koncept 4. průmyslové revoluce, což je vize vývoje automatizační techniky, která se má orientovat na robotizaci pracovních procesů a na centrálním řízení využívajícím vzdálenou obsluhu. Řídicí procesní technologie se mají orientovat do WAN sítí (rozsáhlé sítě, např. Internet), odkud budou řídit dílčí řídicí systémy. Zde je tedy patrný budoucí vývoj, který se bude dotýkat síťové problematiky, proto se i síťová bezpečnost automatizační techniky začne vnímat jako důležité téma návrhu průmyslové výroby.

Společnost SIEMENS má se svými produkty na poli automatizace velký podíl. Možnost implementace síťového zabezpečení integrovaného do společné platformy TIA Portal, přináší své výhody a jde ruku v ruce s vývojem průmyslové automatizace. Díky tomuto získává společnost velkou konkurenční výhodu, která má své místo v konceptu 4. průmyslové revoluce.

Cílem bakalářské práce je vytvořit projekt, který umožní blíže poznat vývojové prostředí, jeho dílčí části a implementované vývojové nástroje. Ukáže jakým způsobem se konfiguruje řídicí sestava, aby bylo možné na projektu pracovat. Pomůže nastínit problematiku programování PLC, rozdělení programovacích jazyků a přívětivost uživatelského rozhraní. V rámci projektu práce představí vybraný zabezpečovací komunikační modul, jeho možnosti a jeho využití při síťovém zabezpečování automatizace. Vytvoření ukázky zabezpečení jednoduché sítě vymezující výrobní linku, nebo zařízení povede k pochopení funkce a smyslu využitých zabezpečovacích technologií.

I. TEORETICKÁ ČÁST

1 PRŮMYSLOVÁ AUTOMATIZACE, TIA PORTAL

Automatizační technika prošla vývojem, jak z pohledu prostředků, tak z pohledu poznání, aplikované teorie a metodiky aplikací. Změnily se technické prostředky pro vývoj a tvorbu aplikací, a proto dnes automatizace není nic unikátního. Kvalitní a inteligentní řízení je dostupné i pro obyčejné stroje, jednoduché mechanismy, nebo různá technologická zařízení napříč všemi obory. [1]

1.1 Řídicí systémy

Průmyslové počítače se používají pro přímé řízení strojů, nebo i jako komunikační, informační systémový prvek. Zejména jsou využitelné tam, kde je třeba zpracovávat velké množství dat, kde je výhodné mít standardní počítačové rozhraní, nebo při využití speciálních softwarových nástrojů. V některých případech je možné se setkat s využitím standardních PC pro řízení technologických procesů, což je většinou riskantní, protože takovýto počítač není konstruován pro provoz v náročných průmyslových podmínkách. Bývá málo spolehlivý a citlivý na rušení. Pro tyto případy existuje alternativa - průmyslový PC. [1]

Dalším důležitým tématem výrobní automatizace je komunikace. Ta zajišťuje vzájemné propojení řídicích systémů a jejich periferních částí. V procesní komunikaci existují dva důležité trendy a to integrace a distribuovanost.

Integrované řídicí systémy vznikají sdružováním systémů, které dosud pracovaly samostatně. Na nejvyšší úrovni se do informační sítě připojují i prvky, které sloužily pouze pro potřeby řízení. Sdružují se tak řídicí a informační systémy. V objektech výrobních firem bývají propojeny systémy pro řízení výroby, s obráběcími stroji, s roboty, nebo manipulátory, s dopravním systémem. [1]

I distribuované systémy jsou založeny na komunikaci. Funkce, které tradičně provádí jeden řídicí systém, se realizuje souborem podsystémů (např. několika malými PLC). Každý z podsystémů je schopen samostatného řízení. Ostatním účastníkům jsou komunikační linkou zasílány informace pouze globálního charakteru. Distribuované systémy bývají řešeny víceúrovňově. Stále častěji se na nejnižší úrovni používají prvky, které byly doposud považovány za pasivní. Nyní jsou to inteligentní senzory, pohony atd. Pro jejich připojení se užívá různých průmyslových sběrnic (Profibus, CAN, ASI, ...). Standardní prvky se připojují pomocí komunikačních modulů. Přínosem distribuovanosti je blízkost podsystému a

jím řízené části procesu. Snižují se náklady na kabeláž, zvláště u systémů které překonávají velké vzdálenosti. [1]

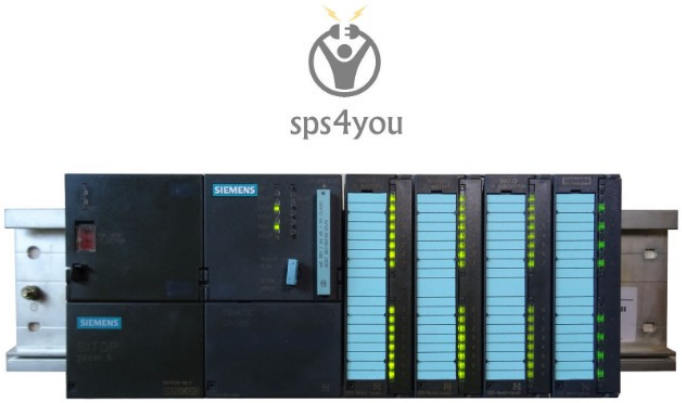
Čím více se automatizace rozšiřuje, tím více je třeba dbát na uživatelské rozhraní mezi člověkem a strojem. Každé pracoviště je jiné, má své předpisy a standardy, které zasahují do požadavků na obsluhu zařízení. U některých řízených systémů stačí ovládání několika tlačítky, u jiných je potřeba předat rozsáhlé informace o procesu. Celé rozhraní by mělo být odvislé od psychické zátěže obsluhy, chybovosti zásahů a celkové provozní spolehlivosti.

Ovládacímu panelu stroje dnes obvykle dominuje **operátorský panel**, v kombinaci s tradičními tlačítky. Na trhu je dostupný nespočet druhů operátorských panelů, které odlišuje jak velikost, tak i hardwarová výbava. Předávat jimi lze informace o stavech zařízení, diagnostice, lze je použít pro zadávání parametrů, ovládání jednotlivých částí. K tvorbě vizualizace se používají specializované vývojové programy. S řídicím systémem operátorský panel komunikuje pomocí průmyslových sběrnic, vše záleží na typu zakoupeného panelu. Nejpoužívanější prostředek ke komunikaci s operačním panelem je průmyslový ethernet - Profinet. [1]

Obr. 1: Operátorský dotykový panel [2]

Programovatelné automaty jsou určeny pro nasazení do podmínek průmyslového prostředí. Odpovídá tomu jejich konstrukce, robustnost, odolnost proti rušení. Původně byly automaty určeny pro řízení strojů, jako náhrada za reléovou logiku. Tomu odpovídají i první programovací jazyky, které vycházely z logických schémat, což bylo bližší elektrokonstruktérům. Dnes jsou programovací jazyky podstatně bohatší, vytvořilo se několik

variací, které sjednocuje mezinárodní norma IEC 61131-3. Postupem času se možnosti PLC rozšiřovaly a s jejich aplikacemi je možné se setkat ve všech oborech. Kromě tradičních aplikací ve výrobní činnosti se využívají v manipulačních technologiích, dopravní a skladové technice, nebo v energetice, např. regulace turbín, elektráren. [1]



Obr. 2: Programovatelný Automat [3]

PLC, jako systémy pro průmyslové aplikace jsou konstruovány jako maximálně spolehlivé a odolné proti vnějším vlivům. Jejich poruchovost je mnohonásobně nižší než poruchovost běžně využívaných periferii. Dnešním trendem je bezobslužný provoz. Řídicí systém tedy musí rozpoznat všechny chybové stavy a situace, tedy i ty, u kterých se spoléhalo na rozeznání obsluhou. Proto se stává neoddělitelnou součástí automatizační techniky technická **diagnostika** a zabezpečovací technika. Jejím cílem je testovat bezchybnou činnost řídicího systému a řízené technologie. Je schopná rozpoznávat hrozící závady, nebezpečné situace a reagovat na ně odpovídajícím způsobem. Diagnostické hlášení poskytuje účinnou pomoc při servisním zásahu. Ideálním případem by byl systém, který je odolný proti poruchám. [1]

Nejmenší a nejlevnější **mikro PLC** systémy jsou charakteristické pevným rozložením vstupů a výstupů a pevně stanovenou hardwarovou konfigurací, nedají se tedy dále rozšiřovat. Obvykle obsahují jen malé množství vstupně-výstupních komponent, které umožňují jen omezenou funkčnost. Jejich programová výbava je značně omezená, vše je redukováno na nezbytné minimum. Největší výhodou takovýchto systémů je jejich nízká cena a malé rozměry. Typickým využitím je realizace jednoduchých mechanismů, kde nahrazují pevnou reléovou logiku. [1]

Obr. 3: Mikro PLC [4]

Kompaktní PLC nabízí určitou možnost konfigurace, která je však také omezena svou variabilitou. Je možné k takovýmto automatům připojit několik přídavných modulů, ale vše jen z omezeného sortimentu a pevnou konfigurací. Některé z kompaktních systémů umožňují vnitřní modulárnost, dají se tedy sestavit osazením základní desky, pomocí jednoduchých násuvných modulů. Pro možnost rozšíření se používají podobné moduly jako u mikro PLC systémů, rozsah jejich variability je ale větší. Používají se binární vstupně-výstupní moduly, analogové moduly, komunikační moduly (RS232, PROFINET, ...), technologické moduly (rychlé čítače, ...), apod. Hardwarová výbava kompaktního automatu PLC je, ve srovnání s mikro PLC, robustní a softwarové nástroje pro tvorbu programu jsou navrženy i pro složité aplikace. Využívají se všude tam, kde je potřeba vyšší výpočetní výkon a nepředpokládají se budoucí změny v systému. [1]

Obr. 4: Kompaktní PLC [5]

Modulární PLC systémy poskytují nesrovnatelně větší volnost v konfiguraci použitého hardwaru. Místo jednoduchých rozšiřovacích modulů mohou být využity různé podsystémy připojené i na velkou vzdálenost. Lze tak vytvářet různě strukturované distribuované systémy. Sortiment rozšiřovacích modulů je rozsáhlý. Obsahují všechny možnosti rozšíření zmíněné u mikro PLC i u kompaktních systémů a spoustu dalších. To vše s nejvyšší možnou variabilitou ve výběru vlastností jednotlivých komponent. [1]

Obr. 5: Modulární PLC [6]

- Binární vstupy a výstupy - Všechny binární vstupy bývají galvanicky odděleny a uspořádány po 16, nebo 32 vstupech na modul. Vyrábějí se pro stejnosměrné i střídavé napětí. Nejčastěji se používají stejnosměrné, které mohou pracovat s napěťovými úrovněmi 5, 12, 24, 48 V (v praxi většinou 24 V). Existují speciální vstupní moduly jako např. bezjiskrové, vhodné do výbušných prostředí. Binární výstupy bývají také galvanicky odděleny, mohou být reléové , tranzistorové PNP i NPN. Sortiment těchto modulů vychází vstříc potřebám projektantů z různých oborů automatizační techniky.
- Analogové moduly - Sortiment analogových modulů také vyhovuje standardním i nadstandardním požadavkům a umožňuje připojení různých akčních členů. Specializované moduly jsou optimálně přizpůsobeny svému určení a nabízejí kvalitnější řešení. Galvanické oddělení zvyšuje odolnost proti rušení. Některé analogové inteligentní moduly umožňují modifikovat svou funkci vhodným osazením zásuvných modulů, nebo softwarovou konfigurací.
- Rychlé čítače - Mezi další používané moduly patří moduly pro rychlé čítání, moduly pro měření polohy a pohybu přírůstkovými nebo absolutními snímači. Mohou

vyhodnocovat rychlé sledy impulzů nezávisle na cyklech automatu. Zpravidla jde o vyhodnocení úhlů, otáček, pozic vyhodnocovaných enkodérem.

- Speciální inteligentní moduly - Komunikační moduly pro různá prostředí a typy přenosu. Paměťové moduly pro zálohování dat. Pneumatické moduly.
- Počítačové moduly - Do této skupiny patří moduly kompatibilní s PC. Tyto PC řeší aplikace, které nejsou typické pro PLC, jako jsou složité a rychlé výpočetní algoritmy, grafické úlohy, zpracování většího množství dat, využití standardních operačních systémů. [1]

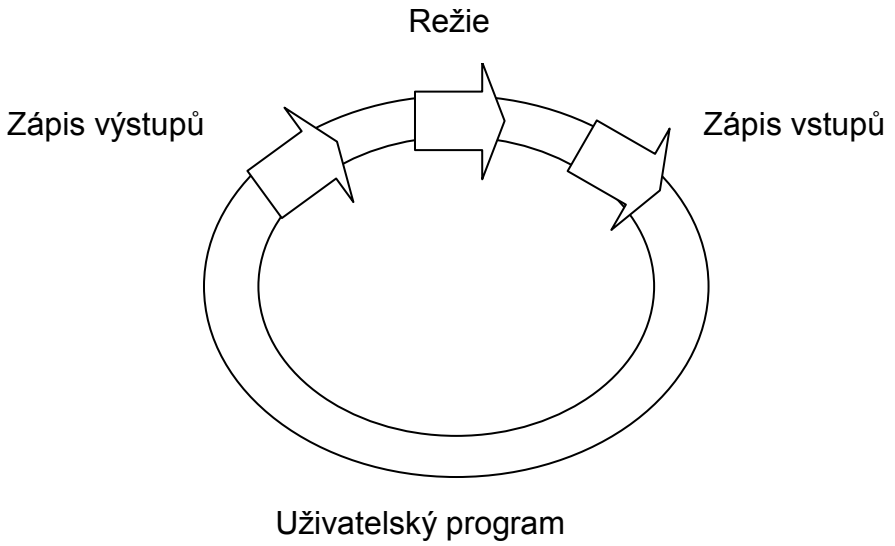
Centrální jednotka CPU je inteligencí celého automatizovaného systému. Realizuje soubor instrukcí a systémových služeb, zajišťuje i základní komunikační funkce s vlastními i vzdálenými moduly, s nadřazeným systémem as programovacím přístrojem. Paměťový prostor je rozdělen na prostor pro uživatelský program a operační prostor. V operačním prostoru jsou pracovní registry, čítače, časovače, obrazy vstupů a výstupů, komunikační data a systémové registry. [1]

Centrální jednotka se skládá z mikroprocesoru a mikrořadiče, zaměřeným na provádění instrukcí. Programem jsou realizovány všechny dostupné funkce. Protože byly automaty původně určeny k realizaci logických úloh na základě pevné logiky, nechybějí v žádném PLC instrukce pro základní logické operace (AND, OR, ..). Dnešní PLC nabízejí podstatně bohatší instrukční soubor. Obsahují např. aritmetické funkce, komunikační funkce, komplexní funkce pro práci s textem a pro přenos dat. Výkonnost programovatelného automatu se nejčastěji posuzuje podle doby vykonání instrukcí. Obvykle se to pohybuje v řádu jednotek až desítek mikrosekund. Používáním složitějších funkcí se může tato doba výrazně prodloužit. Celou tuto problematiku ovlivňuje druh převažujících funkcí a míra kvalifikace programátora. [1]

1.2 Vykonávání programu PLC

Programem PLC je posloupnost instrukcí programovacího jazyka. Program se vykonává cyklicky v programové smyčce, není tedy potřeba řešit, aby se po vykonání cyklu vrátil zpět na začátek, vše je zajištěno systémovým programem. Pokud by se programovou chybou stalo, že se program zacyklí (překročí limit pro délku cyklu) , systém skončí s chybou, zastaví cyklování a nahlásí překročení doby cyklu. Princip cyklování funguje tak, že po ukončení cyklu, po vykonání poslední instrukce, převezme řízení systémový program, ten dokončí otočku programu. Tam aktualizuje obrazy vstupů a výstupů, aktualizuje časové

údaje pro časovače a systémové registry. Jakmile dokončí zmíněné režie, předá řízení první instrukci programu. [1]



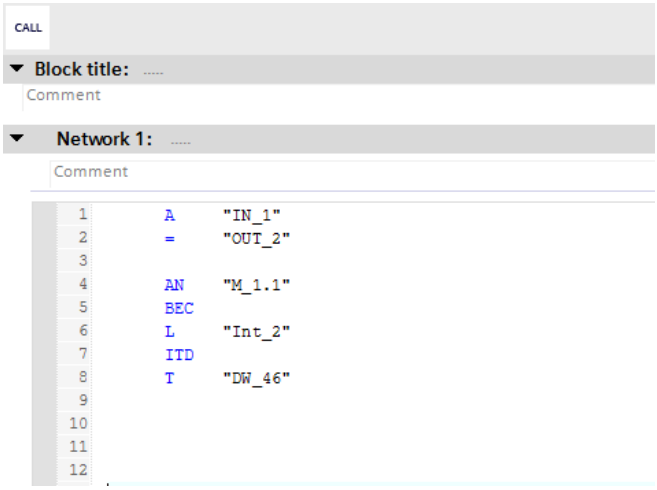
Obr. 6: Cyklus programu (zdroj: vlastní)

Pro vykonávání programu je typické, že nepracuje s aktuálními hodnotami vstupů a výstupů, ale s jejich obrazem, uloženým v paměti automatu. Zápis na fyzické výstupy a čtení z fyzických vstupů probíhá vždy při otočce cyklu, tedy jednou za cyklus programu. Je tím zajištěna synchronizace dat s průběhem programu a sníží se riziko chyb vzniklých nevhodným souběhem změn hodnot.

Automatizované řídicí systémy PLC nabízejí specializované **programovací jazyky**, které jsou navržené především pro účinnou realizaci logických funkcí. Programovací jazyky systémů různých výrobců bývají podobné, ne však stejné. Programovací jazyky sjednocuje mezinárodní norma IEC 61131-3. Norma udává podmínky nezávislosti PLC programu na hardware, definuje jednotný programátorský přístup a možnost ladění programu již ve fázi návrhu. Tímto podporuje kompatibilitu PLC programového vybavení od různých výrobců. Tato norma kodifikuje pět typů jazyků. [7]

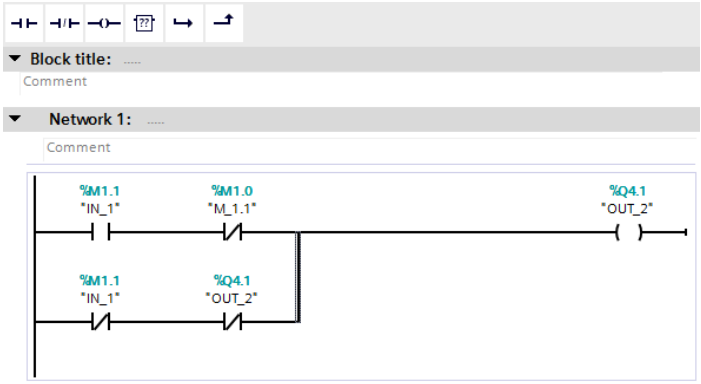
STL (jazyk mnemokódu), neboli "Statement List" je strojově orientovaný jazyk, který je obdobou assembleru. V principu každé instrukci odpovídá stejně pojmenovaný příkaz jazyka. Typické assemblerské prostředí poskytuje stejnou logiku programování, používání návěští, práci s registry. Jazyk mnemokódu bývá často používán zkušenými programátory,

protože dovoluje lépe přizpůsobit úlohy možnostem PLC a vytěžit maximum z jeho instrukčního souboru. [1]



Obr. 7: Jazyk mnemokódu (zdroj: vlastní)

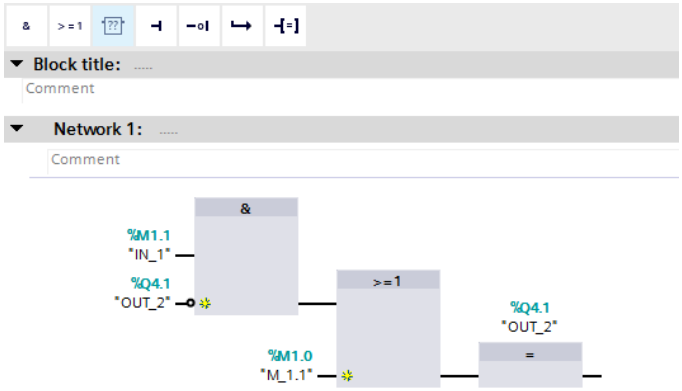
LAD (jazyk kontaktních schémat), neboli "Ladder Logic" je grafický jazyk žebříčkové logiky. Program základní logické operace zobrazuje ve formě obvyklé pro kreslení schémat při práci s reléovými a kontaktními prvky. Funkční bloky jsou kresleny jako obdélníkové značky. Jazyk je z pohledu programování uživatelsky přívětivý a vhodný pro programování jednodušších logických aplikací. Diagnostika programu je zde také jednoduchá a pochopitelná i pro uživatele s menšími zkušenostmi. Při využívání složitějších funkcí ztrácí svou přehlednost. [1]



Obr. 8: Jazyk kontaktních schémat (zdroj: vlastní)

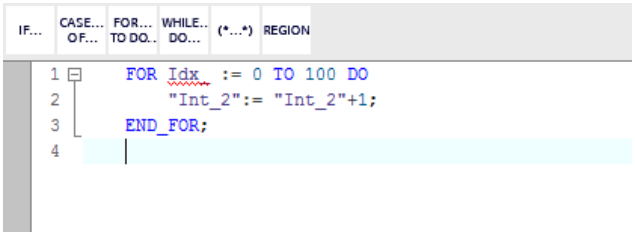
FBD (jazyk logických schémat), neboli "Function Block Diagram" jazyk funkčních bloků. Logické funkce a operace jsou znázorňovány obdélníkovými značkami. Každá značka

je označena svou logickou funkcí. Koncept programování vychází z principu kreslení logických schémat. [1]



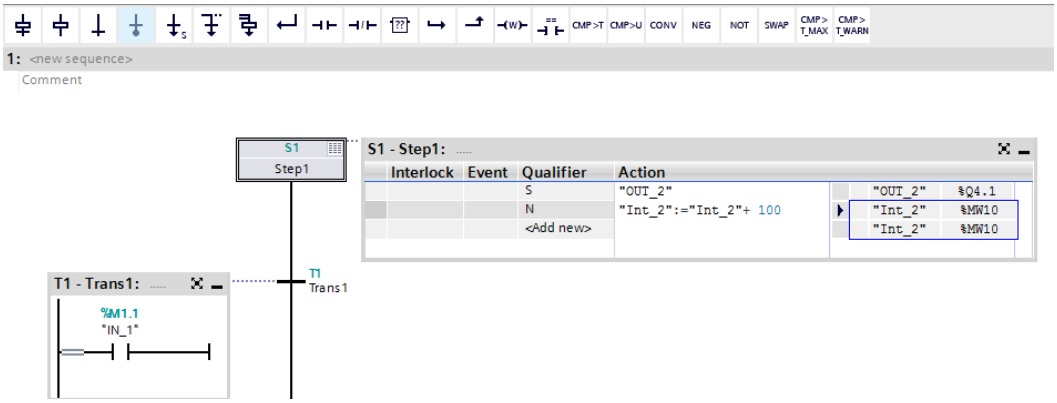
Obr. 9: Jazyk logických schémat (zdroj: vlastní)

SCL (jazyk strukturovaného textu), neboli "Structured Control Language" je obdobou vyšších programovacích jazyků. Je zde patrná podoba např. s jazykem PASCAL nebo C. U tohoto způsobu programování je předpoklad, že si najde své oblíbence u mladých absolventů, kteří se setkávají s takovýmto programováním již při studiu. [1]



Obr. 10: Jazyk strukturovaného textu (zdroj: vlastní)

GRAPH (jazyk sekvenčního programování), velmi přehledný jazyk, který podporuje systémový přístup k programování. K popisu struktury používá značky stavů, přechodů a větvení. Je srozumitelný a pochopitelný i pro méně zkušené programátory.



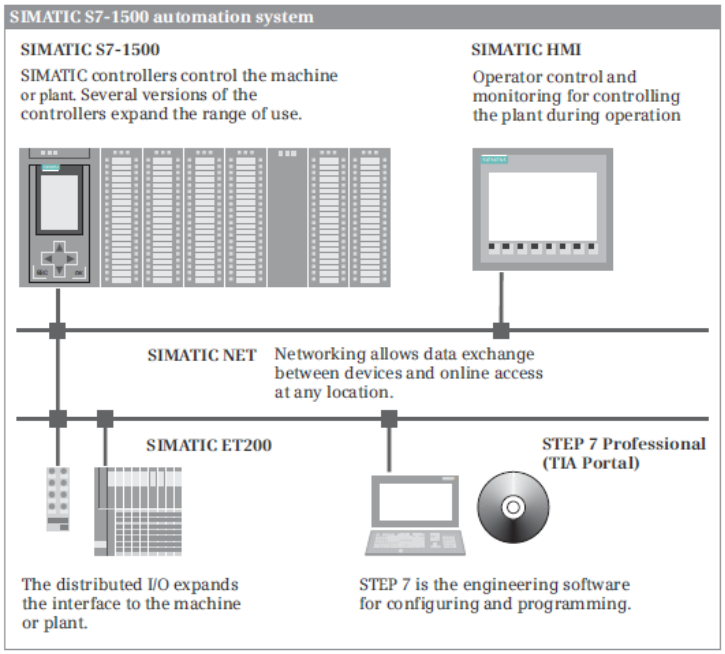
Obr. 11: Jazyk sekvenčního programování (zdroj: vlastní)

Vývojové prostředí podporuje práci s kombinačními funkcemi, i sekvenčními funkcemi. Logické kombinační funkce jsou funkce, jejichž výstupní proměnné jsou dány jednoznačnou kombinací vstupních proměnných. Sekvenční logické funkce jsou funkce, jejichž výstupní proměnné jsou závislé na vstupních proměnných a na stavu systému. Ten udává okamžitou situaci logického systému, nebo řízené sestavy. Je výsledkem dosavadního vývoje, nejčastěji posloupnosti (sekvence) vstupních hodnot. [8]

K programování, ladění a diagnostice logických automatů slouží **programovací nástroje**. V minulosti se k tomuto využívaly specializované přístroje, v současné době se používají výhradně počítače a potřebným softwarovým vybavením. Programovací software umožňuje zápis programu, jeho opravy, nahrávání do logického automatu, diagnostiku online. V některých případech je možné využít nástroj pro simulaci, který plnohodnotně zastoupí PLC při testování, nebo odlaďování programu. Programovací nástroje a vývojové systémy se různě liší svou přívětivostí, obsluhou a optimalizací pro vývoj. [1]

1.3 Automatizační systém SIMATIC

Automatizační systém SIMATIC od společnosti SIEMENS se skládá z mnoha součástí spolupracujících prostřednictvím konceptu "Totally Integrated Automation" (TIA). TIA koncept znamená automatizaci s integrovanou hardwarovou konfigurací, programováním, datovou správou a komunikační správou.



Obr. 12: SIMATIC automatizační systém [9]

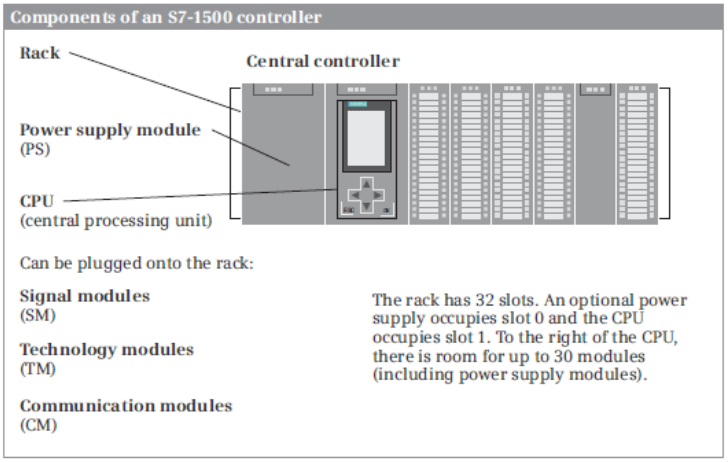
Základnu automatizovaného systému "Programmable Logic Controllers" (PLC) tvoří programovatelné automaty řady SIMATIC S7. Automaty řady SIMATIC S7-1200 jsou ideální pro jednoduché, autonomní úkoly s nízkým až středním výpočetním výkonem. Pokročilejší řada SIMATIC S7-1500 už zajistí maximální výpočetní výkon a maximální uživatelskou přívětivost pro střední až pokročilé aplikace v automatizaci strojů. U všech automatů je možné modulárně přidávat vstupně-výstupní signálové moduly, technologické moduly (rychlé čítače, ...) a komunikační moduly (PROFINET, RS232, ...). [9]

SIMATIC "Human Machine Interface" (HMI) znamená rozhraní člověk-stroj. Jedná se o operační panely SIMATIC v mnoha různých třídách výkonu, umožňující efektivní ovládání a parametrizaci stroje. Software HMI operačního panelu umožňuje vizualizaci stavu zařízení, události a poruchové zprávy. Řeší správu receptur, dat a je oporou při odstraňování problémů, servisu a údržbě. [9]

SIMATIC NET je nástroj, který zprostředkovává výměnu dat mezi různými sběrnicovými systémy, řadiči, vstup/výstupními zařízeními, zařízeními HMI a programovacími zařízeními. Programovacím zařízením se myslí osobní počítač, průmyslový počítač, nebo notebook. [9]

SIMATIC ET200 rozšíření systému o vstupy/výstupy a další dodatečné moduly, které mohou být k nadřazenému CPU připojeny pomocí PROFIBUS DP, nebo PROFINET IO. [9]

CPU obsahuje operační systém a uživatelský program, který je uložen na paměťové kartě. Vykonáván je tento program v pracovní paměti. Dle konkrétních typů CPU, může být řídicí jednotka opatřena malým intuitivním displejem s jednoduchou uživatelskou diagnostikou a možností nastavení některých parametrů. [9]



Obr. 13: S-1500 Sestava logického automatu [9]

- SIGNAL MODULES signálové moduly jsou odpovědné za připojení řízeného zařízení pomocí elementární signálové logiky. Tyto vstupní a výstupní moduly jsou k dispozici pro digitální a analogové signály s různými napětími a proudy, dle příslušných katalogů,
- TECHNOLOGY MODULES technologické moduly jsou moduly po inteligentní zpracování signálů, které se využívají nezávisle na CPU. Mohou být vráceny do procesu, nebo zpracovány CPU. Jsou zodpovědné za manipulaci s funkcemi, které CPU obvykle nemůže provádět dostatečně rychle, například počítání pulsů,
- COMMUNICATION MODULES komunikační moduly umožňují přenos dat nad rámec funkčnosti poskytované standardním CPU rozhraním. [9]

Pro práci se STEP 7 Professional, softwarový modul sloužící k programování CPU, je potřeba licence. Tyto jsou spravovány pomocí **Automation Licence Manager**, nástroje který je instalován společně se STEP 7 Professional. Licence, kterou je možno zakoupit u společnosti SIEMENS, se autorizuje pomocí softwarového klíče uloženého na pevném disku.

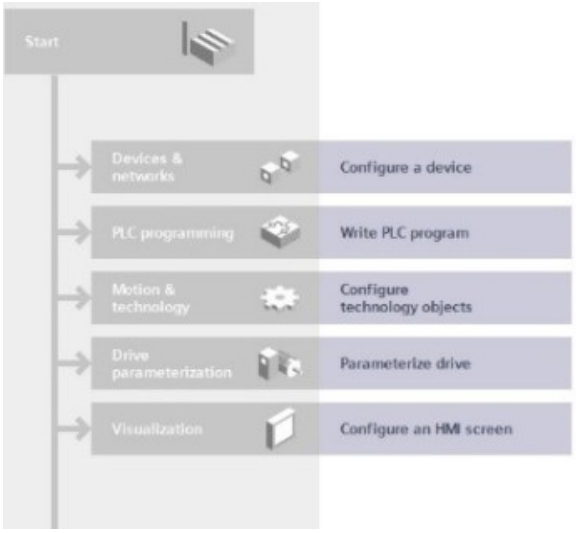
Existuje několik druhů licencí, které jsou rozděleny zpravidla dle délky užívání, nebo přenositelnosti.

Komunikační rozhraní **PROFINET** propojuje PLC s dalšími zařízeními prostřednictvím průmyslové ethernetové sítě. Toto rozhraní mohou podporovat programovací zařízení PLC, zařízením HMI nebo jiné PLC. Otevřená komunikace provádí výměnu dat mezi programovatelnými automaty. Rozhraní poskytuje přenosovou rychlost od 10 do 100 Mbit/s a je podporováno jak standardním ethernetovým kabelem, tak i kříženým kabelem. [10]

1.4 Práce v prostředí TIA Portal

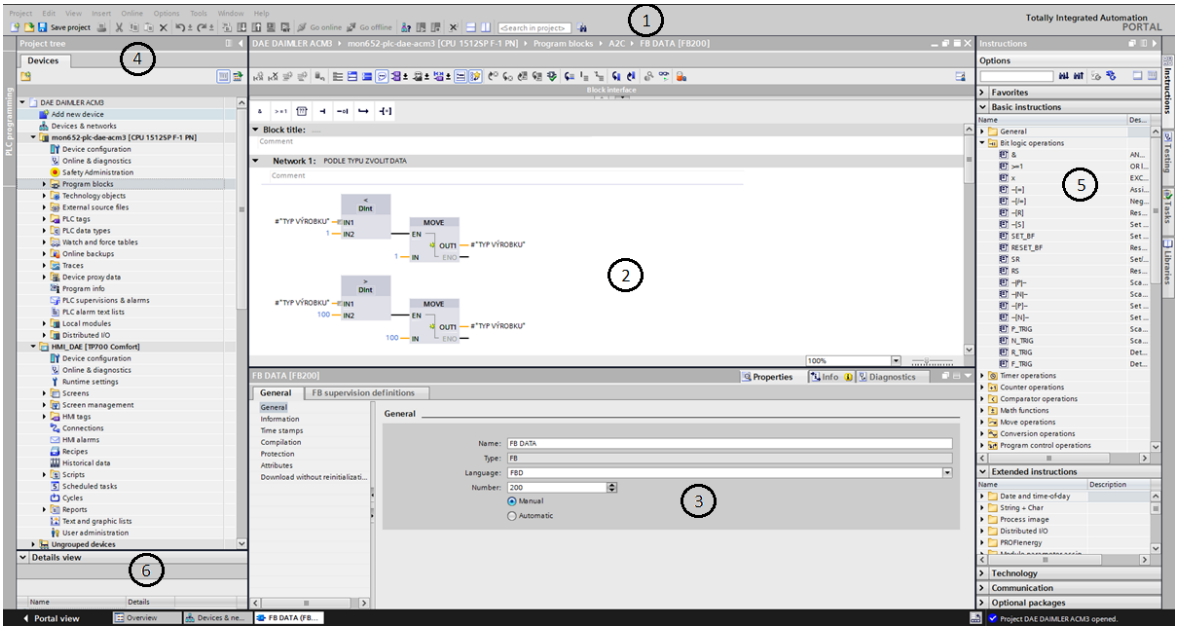
Po spuštění STEP 7 Professional se zobrazí Start Portal. Ten poskytuje všechny funkce a nástroje potřebné pro spuštění projektů. Rozsah funkcí a nástrojů Start Portalu závisí na nainstalovaných aplikacích.

- *Configure a device*, umožní spustit nástroj pro správu hardware, resp všech zařízení, které jsou v projektu obsaženy a nastavení komunikace a síťových valstností zářízení,
- *Write PLC programm*, spustí modul pro programování řídicího CPU,
- *Configure technology object*, spustí nástroj pro správu technologických objektů, které jsou v projekt využity,
- *Configure an HMI screen* , spustí nástroj pro správu operačních panelů HMI a tvorbu vizualizace,
- *Open the project view*, otevře okno Project view, prostředí s optimalizací pracovní plochy pro komplexní práci s projektem. [9]



Obr. 14: Start portal (zdroj: vlastní)

Project view je pro programátora, hlavní pracovní plochou, se kterou pracuje 99% projektového času. Je to komplexní pracovní prostředí, které umožňuje práci s hardwarovou konfigurací projektu, zprostředkovává nástroje pro práci s programem PLC a použitými periferiemi a zpřístupňuje prostředí pro návrh vizualizace projektu. Ve všech fázích projektového vývoje má uživatel možnost celý automatizační proces simulovat a ladit. Je to komplexní vývojové prostředí, které vyniká přehledností, optimalizací vývojového a pracovního procesu. Klade velký důraz na uživatelskou přívětivost. Pracovní plocha je rozdělena na 6 základních částí. [9]



Obr. 15: Project View (zdroj: vlastní)

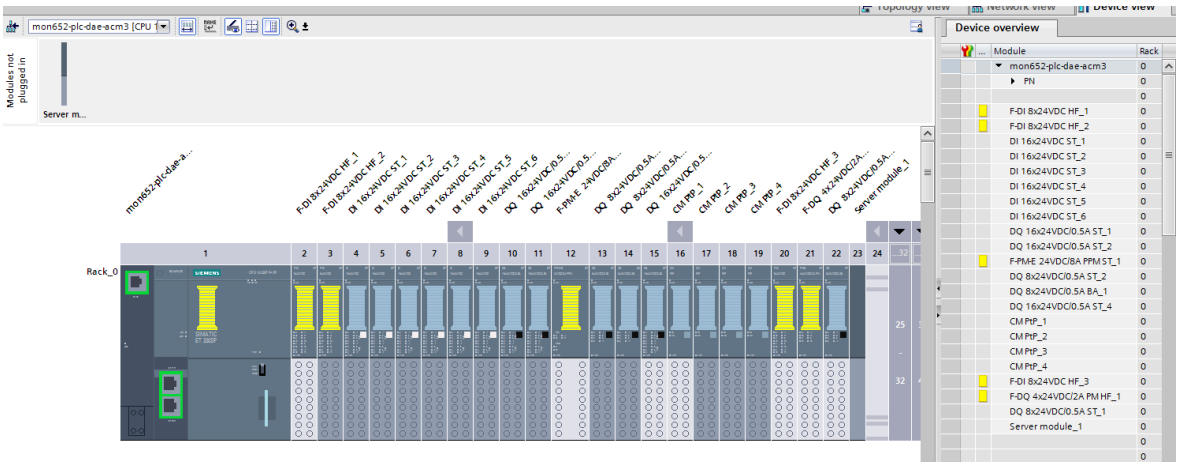
Popis jednotlivých části pracovní plochy Project view:

1. Main menu - Hlavní nabídka a panel nástrojů - hlavní nabídka se skládá z příkazů. Výběr příkazů závisí na označeném objektu. Z výběru jsou příkazy, které nelze vybrat zobrazeny šedě. Pod hlavní nabídkou je grafický panel nástrojů. Pomocí volby Přizpůsobit v hlavní nabídce je možné nastavit uživatelské rozhraní.
2. Working window -Pracovní plocha - pracovní okno se nachází uprostřed obrazovky. Obsah pracovního okna závisí na aktuálně používaném editoru. V případě konfigurace zařízení je okno rozděleno na objekty a stanice v horní části a formulář v dolní části. Pokud je zvoleno programování PLC, horní část obsahuje rozhraní a funkce, střed program v jednom z podporovaných programovacích jazyků a spodní část popis bloku. Pracovní okno lze oddělit od pracovní plochy a zobrazit samostatně.
3. Inspector window - okno, které pod pracovním oknem zobrazuje vlastnosti označeného objektu, sled akcí a poskytuje přehled připojených zařízení. Během konfigurace, nebo programování zde lze nastavovat adresy, datové typy a atributy funkcí.
4. Project tree - strom projektu. Je zobrazeno se stejným obsahem pro všechny editory. Hierarchická struktura obsahuje všechny údaje o projektu. Zobrazuje složky pro PLC, HMI, PC stanice obsažené v projektu a jejich obsah. Klikem na objekt se spustí příslušný editor.
5. Task window - napravo od pracovního okna je okno s úkoly. Obsahuje další objekty pro práci v pracovním okně. Obsah okna však závisí na aktivním editoru. V případě hardwarové konfigurace se zobrazí hardwarový katalog, pokud je aktivní programovací editor zpřístupní katalog programových prvků. Dále slouží např. pro práci s knihovnami a online diagnostikou.
6. Detail view - zobrazuje detailní informace o objektech, které jsou otevřeny v aktuálním projektu. [9]

Nabídka **Help** poskytuje uživateli komplexní informace a podporu při práci v prostředí TIA Portal. Rozsáhlá nápověda je rozdělena podle jednotlivých kroků realizace projektu - Konfigurace, parametrizování, nastavení sítí, strukturování a programování, vizualizace procesů a využití online diagnostických funkcí.

Hardwarová konfigurace je úvodní fází tvorby automatizačního projektu. V této fázi se definuje z jakých hardwarových částí se projekt skládá a jakým způsobem se jednotlivé části propojí, případně jak mezi sebou budou komunikovat.

Konfigurace v programovém nástroji probíhá offline. Uživatel má možnost vybrat si jakoukoliv komponentu z integrovaného hardwarového katalogu. Vybírat lze podle účelu, nebo podle katalogového čísla. Hardwarový katalog se automaticky aktualizuje. Vybrané komponenty se do sestavy vkládají tak, jako na fyzické sestavě.



Obr. 16: Hardwarová konfigurace (zdroj: vlastní)

Jednotlivým vybraným komponentám se v této pracovní ploše nastavují příslušné vlastnosti. Ke každé z nich je možné dohledat přesné hardwarové informace jako účel, napájení, přenosové rychlosti, firmware a další.

Výběr vlastností pro konfiguraci CPU:

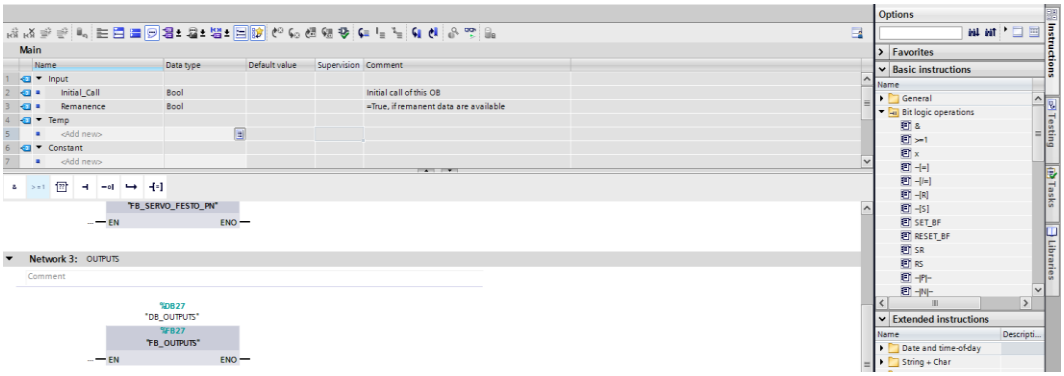
- PROFINET interface - souhrn nastavení pro možnost komunikace zařízení pomocí PROFINET, kompletní nastavení Ethernetové adresy, nastavení jednotlivých portů
- Protection&Security - zabezpečení přístupu k CPU, ochrana proti přepsání projektu, náhled do správy zabezpečovacích certifikátů
- Web Server - správa webového serveru
- Startup - volba režimu zapínání CPU
- Cycle - limity pro délku cyklu
- Overview of adresses - přehled použitých adres v sestavě CPU

Výběr vlastností pro konfiguraci vstupně-výstupní signálových modulů:

- Module parameters - nastavení prodlev signálu, využitého napěťového potenciálu, signálový status
- Inputs - nastavení rozsahu adres pro vstupní byte, možnost diagnostiky (přerušení)

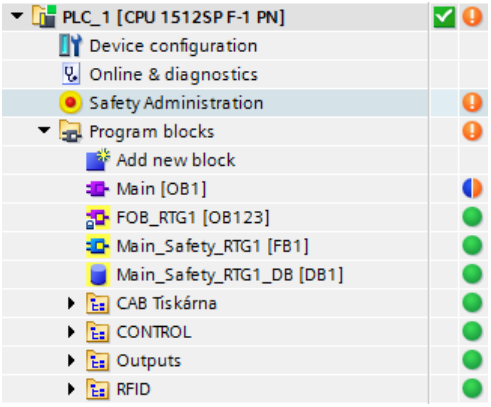
- Outputs - nastavení rozsahu adres pro výstupní byte, možnosti diagnostiky (přerušení, zkrat)

Programový editor slouží k tvorbě programu. Podporuje programování dle mezinárodní normy IEC 61131-3, která je standardem pro programovací jazyky PLC. Pokud je tento editor aktivní, napravo v Task Window je zpřístupněna nabídka základních funkcí sloužících k tvorbě programu. Obsahuje základní logické funkce, časovače, matematické funkce, funkce pro práci s textem a mnoho dalších. Dále má uživatel možnost pracovat s knihovnami, ať už standardními dodávanými spolu s vývojovým prostředím, nebo vlastními.



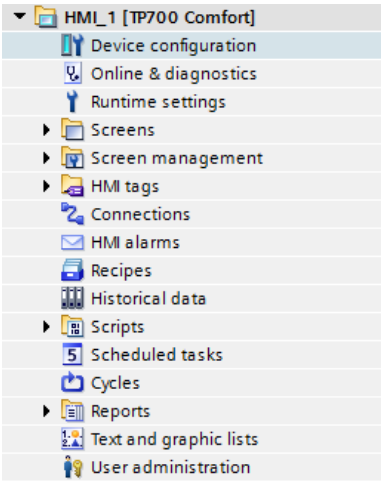
Obr. 17: Program Editor (zdroj: vlastní)

Práce v programovém editoru probíhá offline. Jakmile má uživatel projekt pro PLC připraven, může jej pomocí funkce "Download to device" nahrát do zařízení. Vývojové prostředí uživateli umožňuje sledovat činnost PLC a vykonávání programu online. To v praxi znamená, že je možné sledovat aktuální stav všech proměnných a každé vykonávané části programu. Aktivní části a probíhající logické souvislosti se zabarví zeleně. Při práci s online projektem je dále umožněno sledovat aktuální stav obsahu programu, tedy jestli programový obsah projektu otevřeného ve vývojovém prostředí TIA Portal se shoduje s obsahem nahraným v PLC. Zelená značka znamená shodu, modro-oranžová značí rozdílnou programovou část. V průběhu vývoje se zde mohou vyskytovat různé další značky, celý systém je velice intuitivní a přejetím kurzoru vypíše jednoduchou nápovědu.



Obr. 18: Porovnání online projektu PLC (zdroj: vlastní)

Do vývojového prostředí TIA Portal je implementována práce s vizualizací pro operátorské panely v projektu. Tato implementace je inovací, která usnadňuje práce s projektem a propojuje tyto dva systémy PLC a **HMI (Human Machine Interface)**. Umožňuje lépe a rychleji vytvářet spojení pro výměnu proměnných, předávání diagnostických stavů a ovládání PLC.



Obr. 19: Parametry pro nastavení HMI (zdroj: vlastní)

Uživateli je při práci na vizualizaci projektu umožněno pracovat na návrhu obrazovek, spravovat šablony a pozadí, pracovat na seznamu tagů (proměnných, které jsou napojeny na PLC), nastavit spojení s PLC systémem, řešit správu alarmů, spravovat jazykové mutace jednotlivých částí a spoustu dalších.

Hlavní částí práce na vizualizaci je tvorba obrazovek (Screenu). Tyto obrazovky je možné navrhovat a upravovat ve "Screen editoru". Tento editor umožňuje vkládat do navolených obrazovek objekty, jako jsou tlačítka, rolovátka, textová pole, obrázky, grafiku apod. Všem

takovýmto objektům je možné nastavit vlastnosti jako barvu, velikost, pozici, animační vlastnosti a akce. Animace objektů uživateli umožňuje pomocí nastaveného interface ovládat jednotlivé objekty obrazovek z PLC. V praxi to znamená, zabarvení tlačítek, zviditelnění obrázků apod. Naopak ovládat PLC pomocí vizualizace umožňuje nastavení akcí jednotlivým objektům. Tyto akce mohou, přepínat obrazovky, nastavovat bitovou logiku použitých proměnných a zpřístupní i jednoduché matematické operace.

Obr. 20: Vizualizace operátorského panelu (zdroj: vlastní)

Vizualizační rozhraní je dnes nedílnou součástí výrobní automatizace. Využití takovýchto operačních panelů se stává standardem, který vytváří plnohodnotné rozhraní uživatel - PLC. Funkce panelů určuje jejich zařazení, vyžití a cena. Vyšší řady HMI panelů Siemens, podporují pokročilé grafické objekty, internetový prohlížeč, videopřehrávač, vizualizaci grafů.

1.5 Webový server

Webový server je počítač, nebo počítačový program odpovědný za vyřizování HTTP požadavků. Požadavky přicházejí od klientů (např. webových prohlížečů). Takovéto požadavky server vyřídí a vrací odpověď klientovi, který požadavek odeslal. Odpověď bývá většinou jako HTML dokument, Odpověď webového serveru je ve tvaru http.

HTTP je internetový protokol určený k výměně hypertextových dokumentů formátu HTML. Používá se také s formátem XML pro spouštění aplikací, tím může zpřístupnit i další protokoly jako FTP. Vše funguje jako dotaz-odpověď.

HTML je programovací jazyk užívaný pro tvorbu webových stránek s využitím hypertextových odkazů. Pro stránky WorldWideWeb je hlavním programovacím jazykem.

Obr. 21: Program HTML (zdroj: vlastní)

Z hlediska bezpečnosti webových serverů je největší hrozbou útok **Man in the middle** (člověk uprostřed). Je to útok na kryptografii. Princip spočívá v odposlechu účastníků tak, že se útočník stane prostředníkem komunikace. Tuto problematiku může vyřešit HTTPS protokol.

HTTPS je protokol umožňující zabezpečenou komunikaci v síti. Tento protokol využívá HTTP protokolu a SSL protokolu. Tohoto zabezpečeného protokolu se využívá především při využití webového serveru a webového prohlížeče. Důležitou funkcí protokolu je zajištění autentizace. Ta se ověřuje pomocí asymetrické kryptografie, kde probíhá ověření identity webového serveru. Pro HTTPS protokol je důležitý veřejný klíč a X.509 digitální certifikát.

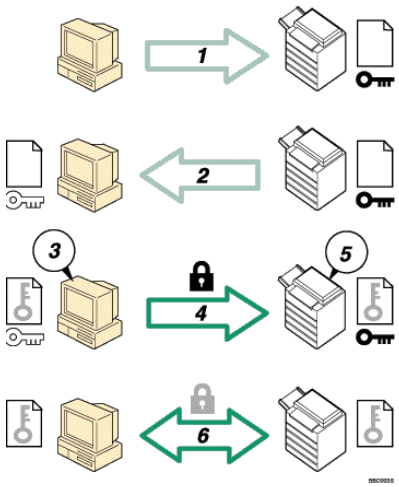
X.509 je standard pro systémy založené na veřejném klíči. Pomocí tohoto standardu se kontroluje digitální certifikát, který potvrzuje, že daný veřejný klíč patří uvedenému vlastníkovi. Takovéto certifikáty jsou vydávány certifikačními autoritami, což jsou organizace, které na základě důvěryhodnosti potvrzují pravdivost údajů, které jsou ve veřejném klíči uvedeny. Tímto ověřením ze strany webového prohlížeče probíhá autentizace webového serveru.

*„**SSL (Secure Sockets Layer)** je nekomerční otevřený protokol a v současné době jedna z nejvíce používaných metod pro zabezpečení datových přenosů v rámci internetu mezi serverem s webovou prezentací a prohlížečem (uživatelem).“* [11]

SSL protokol funguje jako asymetrická šifra. Každá strana má dva šifrovací klíče (veřejný a soukromý). Způsob šifrování probíhá následujícím způsobem:

1. Webový klient pošle webovému serveru požadavek na SSL připojení.

2. Server odpoví klientovi zprávou obsahující certifikát. Na jeho základě proběhne autentizace webového serveru.
3. Klient generuje základ šifrovacího klíče, který zašifruje veřejným klíčem.
4. Klient odesílá zašifrovaný sdílený klíč.
5. Server pomocí svého soukromého klíče zprávu rozšifruje. Z tohoto základu oba vygenerují hlavní šifrovací klíč.
6. Vzájemně si klient a server potvrdí komunikaci využitím tohoto klíče. Poté zasílají data. [12]



Obr. 22: Šifrování - SSL protokol [12]

Pro nastavení bezpečného spojení se využívá různých kryptografických algoritmů, při kterých se využívá i hašovacích funkcí. Pro šifrování klíčů se používají asymetrické šifry jako RSA, Diffie-Helman. Pro šifrování dat se užívají symetrické šifry jako IDEA, DES, 3DES, AES.

Hašovací funkce je matematická funkce, která slouží k převodu dat do malého čísla (haše, otisku). Většinou se používají pro rychlé prohledávání dat, porovnávání dat, hledání položek v databázích, hledání duplicitních dat. Hašovací funkci charakterizují čtyři základní pravidla:

1. jakákoliv velikost vstupu generuje stejně dlouhý otisk
2. z haše není možné rekonstruovat původní zprávu
3. malá změna vstupu znamená velkou změnu na výstupu
4. je velmi nepravděpodobné, že by byl dvěma různým zprávám generován stejný haš

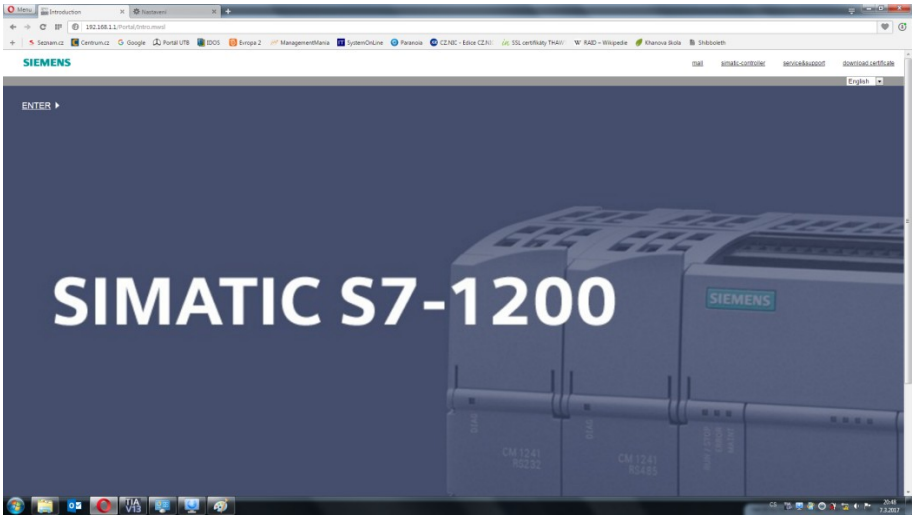
„*Každá HF musí být jednosměrná, tzn., že k ní neexistuje inverzní algoritmus. K otisku nelze v časově omezeném úseku, jednoznačně najít text, z kterého byl tento otisk vypočítán. Například certifikáty ke kvalifikovaným elektronickým podpisům jsou zpravidla vydávány s platností omezenou na rok či dva. To už je časově omezený úsek.*“ [13]

Řada s7-1200 má ve svém CPU integrovaný webový server, který může sloužit ke vzdálenému přístupu a výměně informací. Tento webový server může sloužit především jako zobrazování provozních a systémových hodnot, zapisování proměnných, nastavování parametrů a různým diagnostickým účelům. V určitých případech může nahradit vizualizaci operačním panelem HMI. Zajímavostí je možnost využití emailového klienta.

Je možné využít předem definované uživatelské rozhraní implementované vývojovým prostředím TIA Portal. Takový vytvořený HTML dokument obsahuje předem definované stránky s diagnostickými funkcemi a základními informacemi o CPU. Do tohoto dokumentu je možné jednoduše vložit další informace o projektu, proměnných a stavech programu, pomocí interního vývojového nástroje. To vše v předepsané šabloně.

Aby bylo možné využít vlastní HTML dokument implementovaný do šablony v PLC využít, je potřeba jej do projektu PLC systému nahrát. A aby byla zajištěna výměna a správnost dat, je nutné použít v programu PLC speciální funkci zajišťující tuto správu. Pomocí této funkce je možné specifikovat výměnu požadovaných dat a informací.

Hardwarová konfigurace uživateli umožní nastavit zabezpečení serveru, periodu načítání dat a přihlašovací údaje do HTML dokumentu. Jakmile je webový server v projektu PLC aktivován a celý tento projekt je do PLC nahrán, je server zpřístupněn. Aby však bylo možné využít zabezpečenou verzi, je potřeba použít digitální certifikát (veřejný klíč). Je možné certifikát získat od některé z certifikačních autorit, nebo využít certifikát dodavatele, společnosti SIEMENS, která jej má implementován ve svém vývojovém prostředí, resp. několik verzí digitálních certifikátů. Pro získání certifikátu je potřeba poprvé zobrazit HTML dokument základním protokolem HTTP, pomocí hypertextového odkazu na adresu http://192.168.1.1 v příkazovém řádku. Na úvodní stránce je zobrazena možnost stažení certifikátu. Pro správnou funkci je potřeba certifikát importovat do internetového prohlížeče.



Obr. 23: Hlavní strana webového serveru (zdroj: vlastní)

2 SÍTĚ

V praxi je využitelnost automatizačního systému bez vzájemného propojení podstatně omezená. Postupně se prolínají jednotlivé technologie pro zpracování a přenos dat. Takové technologie se většinou označují zkratkou ICT (Information and Communication Technology). Potřeba sdílení dat a umožnění komunikace vede k rozvíjení ICT technologií a potřebě komunikaci monitorovat a řídit. [14]

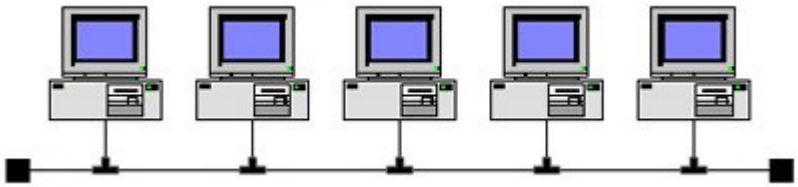
Počítačová síť je systém samostatných počítačů, které jsou propojeny mezi sebou a mohou vzájemně využívat své prostředky. Počítačové sítě jsou velice různorodé, dají se proto dělit podle různých aspektů. Kromě počítačů se do počítačových sítí připojuje celá řada technologických zařízení (stroje, měřicí přístroje, ...). Tyto kombinované sítě se stávají standardem automatizačních systémů. [14]

Sítě se mohou dělit dle rozsahu:

- LAN (Local Area Network) - řadí se mezi nejmenší, charakterizují ji spojení pouze několika počítačů řádově v desítkách (počítače v budově, komplexu, ...)
- MAN (Metropolitan Area Network) - řadí se mezi středně rozsáhlé sítě, typicky spojují několik menších LAN sítí (velký podnik, větší město, metropolitní síť, ...)
- WAN (Wide Area Network) - rozlehlá síť neomezené velikosti (internet), je tvořena soustavou propojených sítí, bez vlastníka, nebo správce
- PAN (Personal Area Network) - zvláštní kategorie osobních sítí, propojení na krátkou vzdálenost (Bluetooth). [14]

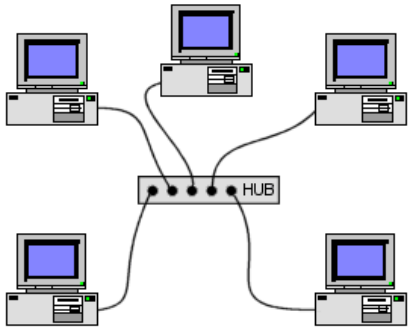
Dále se mohou sítě dělit dle topologie:

Sběrnicová topologie - zařízení v síti jsou navzájem propojeny kabelem. Tento kabel vede od jednoho zařízení k druhému a vytváří tak souvislou sběrnici. U této topologie nesmí dojít k uzavření sběrnice do smyčky. Na koncích sběrnice dochází k ukončení pomocí terminátoru. Nevyžaduje mnoho kabeláže. Při poruše, pokud dojde k přerušení kabelu, přestává sít fungovat. Takováto závada se diagnostikuje velice obtížně. Dále je v této síti omezen počet připojených uzlů a délka sběrnice. [14]



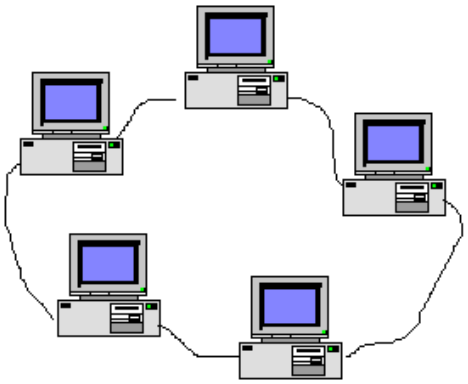
Obr. 24: Sběrnicová topologie [15]

Hvězdicová topologie - zařízení v síti jsou propojeny kabelem k centrálnímu aktivnímu prvku. Komunikace probíhá přes rozbočovač do všech zařízení v síti. U této topologie nehrozí narušení funkčnosti celé sítě v případě porušení kabeláže tak, jako u sběrnice. Opět platí pravidlo, že v síti nesmí vznikat smyčka. Hlavní výhodou této topologie je to, že pomocí více kaskádově zapojených rozbočovačů mohou vznikat rozlehlejší sítě než u topologie sběrnicové. [14]



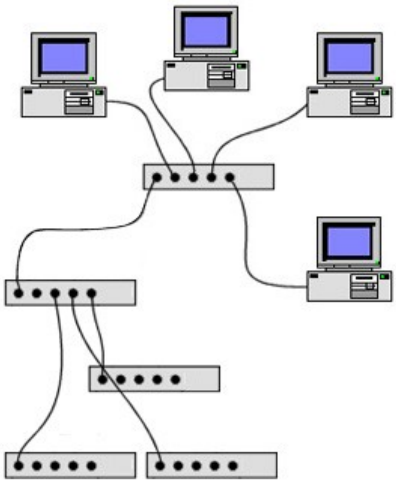
Obr. 25: Hvězdicová topologie [16]

Kruhová topologie - propojuje zařízení podobně jako topologie sběrnicová pomocí jednoho kabelu. Rozdíl je v tom, že je propojení realizováno do kruhu, jsou tedy vynechány terminátory a síť nemá konec ani začátek. Komunikace probíhá ve smyčce, v jednom směru a prochází všemi zařízeními. Každý prvek funguje jako opakovač. Zesiluje signál a posílá dalšímu prvku sítě. Selhání jednoho prvku, nebo narušení kabeláže má vliv na funkci celé sítě. [14]



Obr. 26: Kruhová topologie [17]

Stromová topologie - je kombinací vybraných topologií. Jde především o kombinaci sběrnicové a hvězdicové topologie, kdy je několik hvězdicových sítí propojeno navzájem. Vzniká rozvětvená struktura, jejíž základ se podobá sběrnici. [14]



Obr. 27: Stromová topologie [15]

Dělení podle architektury:

Klient - Server - u tohoto typu sítě jedno zařízení plní funkci serveru, poskytuje ostatním prvkům, klientům své prostředky a služby. Většinou tedy zařízení, které má větší výkon a bezchybný, nepřetržitý chod. Při výpadku serveru je omezena funkčnost celé sítě a práce klientů, které server využívají. Tato architektura oproti jednodušším architekturám dosahuje vyšších výkonů a umožňuje vytvářet rozsáhlé hierarchické sítě. [14]

Peer - to - peer - v této architektuře neexistuje nadřazené zařízení jako u předchozí architektury. Každý prvek v síti může zpřístupnit některý svůj prostředek ke sdílení ostatním.

Takováto architektura se používá u sítí malého rozsahu, kde není potřeba využívat prostředky na bázi klient-server. [14]

2.1 Aktivní prvky v síti

Aktivními prvky se rozumí jednotlivé počítače, nebo další síťová zařízení (např. tiskárny). Dále do této kategorie patří propojovací prvky (Hub, Switch, Router, Repeater). Rozdíl mezi nimi je ve funkčnosti prvku. Obecně se aktivní prvky používají v sítích se zapojením do hvězdy, k propojování sítí s různými parametry a technologiemi, nebo jako ochrana před útoky.

Mezi hlavní aktivní síťové prvky patří:

HUB (rozbočovač) - je základní aktivním prvkem, který umožňuje větvení sítě, elektrické oddělení do segmentů, nebo se může chovat jako repeater (opakovač). Tento síťový prvek data, která přijme na jednom z jeho portů, dále rozesílá na všechna připojená zařízení. Data obdrží i ta zařízení, kterým nebyla určena. Síť je v tomto případě zbytečně zatěžována daty, která jsou určena jen jednomu prvku. V praxi jsou Huby využívána jen zřídka a to u malých sítí. [14]

SWITCH (přepínač) - aktivní prvek propojující jednotlivé segmenty sítě, nebo připojená zařízení. Switch analyzuje procházející data a podle nich rozhoduje kam je poslat. Neprodukuje tak velké množství dat v síti jako Hub, síť tedy není tak zatížená. Kromě výkonu je přínosem i pro bezpečnost sítě. Pokud Switch přijme data směřující na neznámou adresu, chová se jako Hub a odešle je všem zařízením. Jakmile na ně příslušné neznámé zařízení na některém z portů zareaguje, uloží si Switch adresu k příslušnému portu a další komunikaci směruje tam. [14]

ROUTER (směrovač) - aktivní prvek, který se využívá ke spojení dvou sítí. Obecně takto může sloužit i jakýkoliv počítač. Zvláštním případem je router, který používá jen jedno rozhraní a směruje data ve virtuální LAN síti. Často je také využíván jako gateway (brána) pro připojení k vnější síti, např. internetu. V tomto případě počítače ve vnitřní síti skrývá pod svou vlastní adresu ve vnější síti. [14]

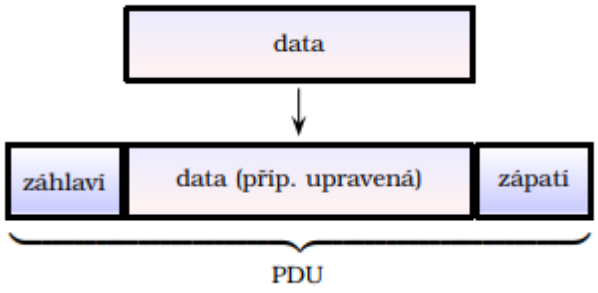
REPEATER (opakovač) - zařízení určené k prodloužení délky sítě. Přijme data od jednoho síťového zařízení, zesílí je a přepošle dál. [14]

2.2 Komunikace v LAN

V obecném pojetí je předpisem, který definuje způsob komunikace mezi síťovými zařízeními, **protokol**. Protokol definuje, jak musí komunikace začít, jak se dohodnout na parametrech komunikace, jak přenášet data, jak má druhé zařízení potvrdit příjem dat, nebo vyžádat jejich opětovné zaslání, nebo jak komunikaci ukončit. Většina protokolů je volně dostupná, aby byla zajištěna funkce síťových zařízení pro širší využití. V případně specifických technologií a druhů protokolů může být protokol poskytován formou nákupu licence.

Například protokol HTTP definuje, jakým způsobem komunikuje webový prohlížeč s webovým serverem. Tento protokol je implementován v operačním systému počítače, na kterém je spuštěn webový prohlížeč a v operačním systému webového serveru, který poskytuje data.

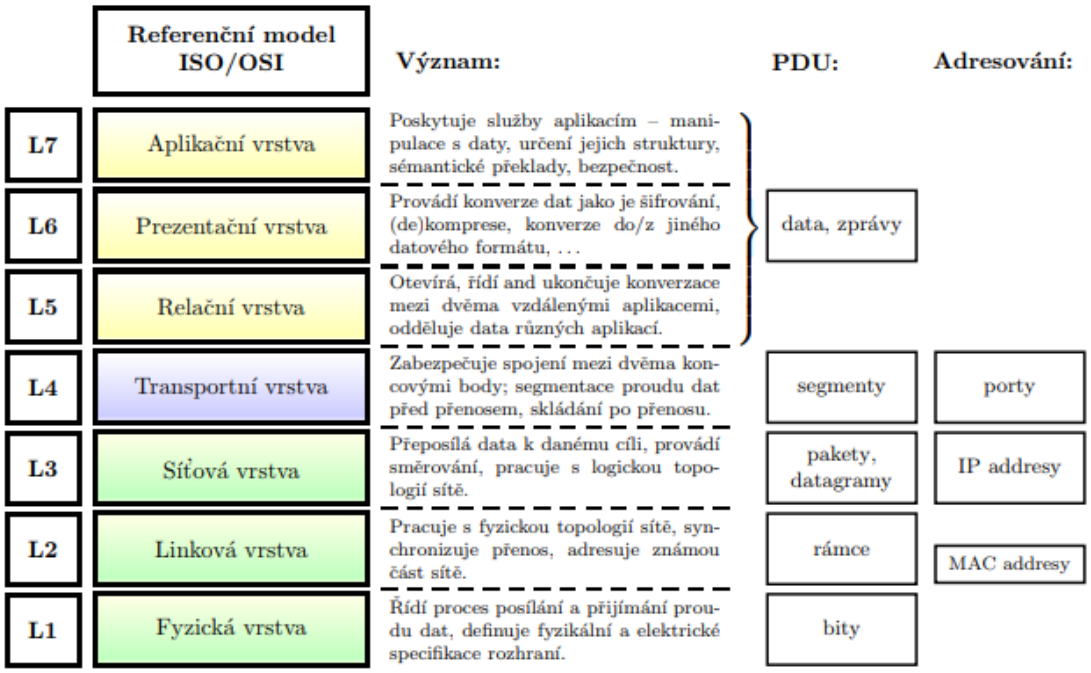
Protokolová datová jednotka (PDU, Protocol Data Unit) je soubor dat opatřený metadaty (informacemi o datech), která se vztahují ke konkrétnímu protokolu. Protokoly obdrží data, která zpracují (strukturují, rozdělí, zašifrují, přeloží, ...), přidají záhlaví s informacemi (délka, šifrovací algoritmus, adresa odesílatele a příjemce, ...). Některé protokoly přidávají i zápatí obsahující například kontrolní součet. [18]



Obr. 28: Protokolová datová jednotka [18]

2.3 Referenční model ISO/OSI

Mezi důležité standardy z oblasti počítačových sítí patří skupina standardů popisujících referenční model OSI (Open Systems Interconnection) publikovaných organizací ISO. Tento model ISO/OSI definuje sedm vrstev popisujících přesně stanovené funkce síťové komunikace. Díky tomuto je definováno, co se na dané vrstvě může dít. Účelem vytvoření modelu je rozdělit celek na menší části, snadněji popsat a určit vztahy těchto částí. [18]



Obr. 29: Referenční model ISO/OSI [18]

Vrstvy zobrazené zeleně jsou závislé na komunikačním médiu, modrá vrstva je přechodová a žlutě zobrazené vrstvy se na přenosu podílení jen nepřímo, připravují data a řeší komunikaci s aplikacemi.

Fyzická vrstva L1 - vrstva zprostředkovává fyzický přenos dat. Definuje přenosové médium (kabel, bezdrátová technologie,..), popisuje reprezentaci bitové logiky a kódování, síťové rozhraní. Vrstva přijímá data ve formě jedniček a nul a přetváří je na odesílaný signál. Pouze tuto vrstvu mají implementovány síťové zařízení jako huby a repeatery. Tyto zařízení pouze předávají přijatá data, která dále nezpracovávají. [18]

Linková vrstva L2 - v této vrstvě se určuje vztah mezi daty v bitové logice z fyzické vrstvy a konkrétním místem v síti. Zařízení s linkovou vrstvou vede přehled o připojených zařízeních v místní síti prostřednictvím tabulky fyzických adres (MAC adres). V této tabulce bývá i informace o portu, přes který je zařízení dostupné. Datové jednotky, se kterými pracují protokoly v této vrstvě jsou "rámce". Každý rámec vymezuje začátek a konec dat, fyzickou adresu příjemce a odesílatele. Další funkcí této vrstvy je například řízení rychlosti přenosu podle stavu příjmu datových jednotek. [18]

Síťová vrstva L3 - protokoly síťové vrstvy pracují s topologií sítě, stanovují cestu, určují adresu a směrují. Datové jednotky jsou pakety, nebo datagramy. Vzhledem k povaze své funkce je tato vrstva implementována na aktivních síťových prvcích zajišťujících směro-

vání, takovým zařízením je router. Router implementuje L1, L2 a L3. Vrstva pracuje se směrovací tabulkou, tam ukládá informace o tom, kam datová jednotka patří a do jaké sítě. [18]

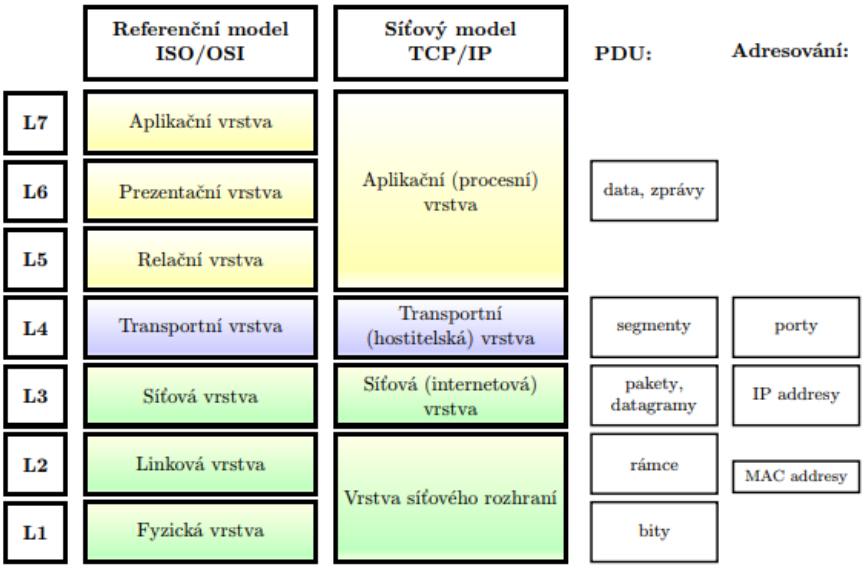
Transportní vrstva L4 - tato vrstva je přechodem mezi předchozími vrstvami, které jsou zaměřeny na přenos a dalšími, které jsou zaměřeny na aplikace. Směrem nahoru se využívá vazeb na protokol vyšší vrstvy. Taková vazba se nazývá port, je to číslo, které tvoří adresu. Datovou jednotkou transportní vrstvy je segment. Transportní vrstva je implementována především na koncových zařízeních. [18]

Relační vrstva L5 - v této vrstvě se oddělují a řídí data patřící různým aplikacím. Různé dvě aplikace, které spolu po síti přes tuto vrstvu komunikují, navazují relaci, v rámci níž se přenášejí data. Transportní vrstva navazuje spojení mezi dvěma zařízeními, relační vrstva mezi dvěma aplikacemi. [18]

Prezentační vrstva L6 - je to vrstva, která se stará o to, aby data vyšším vrstvám prezentovala ve formátu, kterému rozumí. Má zodpovědnost za konverzi dat, šifrování, kompresi, kódování. [18]

Aplikační vrstva L7 - na této vrstvě pracují protokoly, se kterými pracují aplikace. Například aplikační protokol HTTP využívající webový prohlížeč. Zajišťuje předání dat aplikacím. [18]

Nejpoužívanějším modelem definujícím síťovou komunikaci je **protokol TCP/IP** (Transmission Control Protocol/Internet Protocol). Jedná se o skupinu protokolů, pracujících na různých vrstvách. Je směrovatelný, může tedy pracovat ve velké skupině propojených sítí. Vychází ze síťového modelu ISO/OSI. [14]



Obr. 30: Síťový model TCP/IP [18]

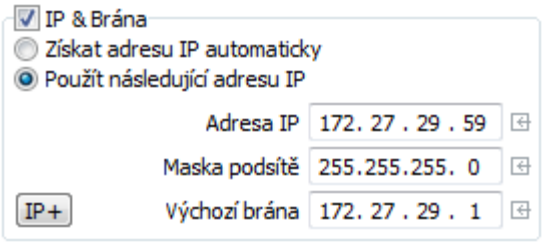
2.4 IP adresa

Síťová vrstva pracuje s topologií sítě. Tato vrstva zajišťuje síťové rozhraní a směrování. **Adresy síťové vrstvy** jsou softwarové adresy na rozdíl od fyzických adres linkové vrstvy. Na síťové vrstvě je nejdůležitějším protokolem protokol IP. V současné době existují dvě verze a to IPv4 a méně užívaný IPv6. IP adresy jsou hierarchické, dokážou tedy pracovat se složitou strukturou rozdělenou do skupin a podskupin.

IPv4 adresa je nejpoužívanějším standardem problematiky síťového adresování. Adresu tvoří unikátní číslo, které je přiděleno zařízení, které komunikuje pomocí internetového protokolu. U každého přenosu je potřeba znát adresu příjemce a odesílatele. Samotnou adresu tvoří 32 bitů zapisovaných po osmi bitech oddělených tečkou (v naprosté většině případů zapisováno v dekadickém tvaru).

Další adresa, která pomáhá určit rozdělení sítí a podsítí je maska sítě. Rozděluje IP adresu na síťovou část a hostující. „*Zápis je stejný jako u IP adresy, ale platné hodnoty jsou pouze ty, které mají v binárním tvaru zleva jedničky a zprava nuly (pokud se zleva na některé pozici objeví nula, dále již musí následovat pouze nuly). Jedničky v masce jsou tzv. network ID a je to část, která je pro daný subnet stále stejná. Nuly jsou tzv. host ID a tedy část, která je proměnná a určuje adresu hosta v daném subnetu. Příkladem jednoduché masky je 255.255.255.0, ta určuje, že prvních 24 bitů adresy je network ID a posledních 8 bitů je hostovská část.*“ [19]

Výchozí brána definuje adresu sítě a aktivního prvku (většinou routeru), který vytváří danou podsíť.



Obr. 31: Nastavení IP adresy (zdroj: vlastní)

3 SÍŤOVÁ BEZPEČNOST

Síťovou bezpečnost automatizace je potřeba vnímat jiným způsobem, než bezpečnost informační. A to z toho důvodu, že útok na automatizaci může mít odlišný motiv než útok na datovou síť. U automatizace je v naprosté většině případů motivem zastavení nějaké technologie, znemožnění komunikace v rámci sítě, jednoduše zastavení výrobního zařízení, nebo linky. Proto je možné se zde setkat s několika druhy síťových útoků.

Denial of service - DoS (odepření služby) je typ útoku na síťové služby, který se snaží cílovou službu znepřístupnit ostatním uživatelům. Může například dojít k přehlcení požadavky. Útočníkovi se nepodaří síťovou službu ovládnout, ale umožní mu ji rozbít. Existuje nespočet druhů útoků založených na DoS principu. [20]

Port scanning (skenování portů) je typ útoků, zaměřený na zjišťování otevřených síťových portů, což je činnost nežádoucí, protože vede k zjištění slabých míst a odhalení zranitelnosti síťového prvku. [21]

3.1 Firewall

Jedno z nejdůležitějších opatření pro řešení síťové bezpečnosti je **firewall**. Je to bezpečnostní brána, oddělující provoz mezi dvěma sítěmi, která data propouští jedním, nebo druhým směrem, podle předem definovaných pravidel. Tyto pravidla vždy identifikují cíle a zdroje dat. Definovaná pravidla mohou být orientována na IP adresy, MAC adresy (fyzické adresy), na různé druhy protokolů a portů. Existují tři základní druhy firewallu:

- paketové filtry - pravidla přesně uvádějí z jaké adresy a portu na jakou adresu a jaký port může být paket doručen, kontrola se provádí na L3 síťové a L4 transportní vrstvě síťového modelu ISO/OSI, výhodou je vysoká rychlost, nevýhodou je nízká úroveň kontroly a komplikace u složitějších protokolů,
- aplikační brány (proxy firewall) - zcela oddělí sítě, klient se připojí na aplikační bránu (proxy), ta připojení zpracuje a otevře nové spojení k serveru, kde sama brána vystupuje jako klient, kontrola probíhá na L7 aplikační vrstvě síťového modelu ISO/OSI, výhodou je vysoké zabezpečení známých protokolů, nevýhodou je vysoká náročnost na hardware,
- stavové paketové filtry - stejná kontrola jako jednoduché paketové filtry, navíc ale ukládají informace o povolených spojeních, které pak mohou využít při rozhodová-

ní, zda mohou být propuštěny, nebo má proběhnout nová kontrola, výhodou je vysoká rychlost, nevýhodou je nižší bezpečnost než poskytují aplikační brány. [22]

3.2 VPN - Virtuální privátní síť

Dalším bezpečnostním síťovým prostředkem využívaným ne jen v automatizaci, je VPN, která zabezpečuje bezpečné spojení několika počítačů, nebo síťových prvků, prostřednictvím nedůvěryhodné sítě, např. sítě Internet. Mezi prvky v síti se vytvoří šifrovaný tunel, kterým probíhá komunikace. Spojení vytvoří jednotnou zabezpečenou privátní síť. Navazování spojení je provázeno autentizací pomocí digitálního certifikátu a dále je veškerá komunikace šifrována.

IPsec (IP security) je bezpečnostní rozšíření IP protokolu, které je zaměřeno na autentizaci a šifrování každého IP datagramu. Je to zabezpečení probíhající na L3 síťové vrstvě síťového modelu ISO/OSI. Pro komunikaci vytváří logické kanály **Security Associations - bezpečnostní asociace**, což jsou atributy zabezpečení, které podporují zabezpečenou komunikaci (šifrovací algoritmus, režim, klíč šifrování provozu, ...). Pro distribuci těchto kanálů je nejčastěji používaným prostředkem protokol ze sady IPsec protokolů protokol **IKE (Internet Key Exchange)**. Tento protokol se skládá ze dvou fází:

1. v této fázi se vytvoří bezpečný otevřený komunikační kanál pro vytvoření sdíleného tajného klíče pro šifrování další komunikace,
2. během této fáze se bezpečným kanálem vytvořeným v první fázi nastaví bezpečnostní asociace, výsledkem je tedy výměna bezpečnostních asociací. [23]

Tvorbu a správu VPN využívající IPsec provází problematika šifrování, kterou se zabývá kryptografie.

3.3 Kryptografie

Kryptografie je věda, zabývající se utajením informace na zašifrovaný text. Hlavním tématem této metody je šifrování.

„*Šifrování neboli proces, při kterém se zpráva převádí z podoby otevřeného textu do podoby, kdy je čitelná pouze na základě nějaké speciální znalosti, tvoří významný bezpečnostní prvek v informačních systémech. Důvodem k šifrování je snaha ochránit důvěrné a osobní informace před nepovolanými osobami. Tato metoda je vhodná i jako ochrana před neo-*

právněným přístupem z řad administrátorů systémů, kteří k daným datům nepotřebují přístup.“ [24]

„*Opakem šifrování je dešifrování, které představuje postup, při kterém dochází k transformaci šifrovaných dat do jejich původní podoby. Oba postupy, jak šifrování, tak i dešifrování, vyžadují ke své funkci nějakou tajnou informaci. Obvykle je vyžadován klíč a použitá metoda. Klíč si můžeme představit jako heslo k počítači, které používáme dnes a denně, nebo jako klíč od auta. Klíč v tomto případě omezuje přístup k datům pouze pro oprávněné osoby. Jako klíč lze použít libovolný datový řetězec.“* [24]

Současné kryptografické prostředky umožňují jak zabezpečit předávané informace, tak i to, aby se vysílané informace do sítě dostaly pouze a jen k jednomu vybranému protějšku a aby jen on mohl informace zpracovat. Aby vše zmíněné mohlo fungovat, je potřeba zapojení kryptografických algoritmů.

Symetrické šifry k šifrování i dešifrování používají stejný klíč. Je to algoritmus, který je vzhledem k malým výpočetním nárokům velmi rychlý. Tyto šifry se využívají především k šifrování velkého množství dat. Mezi nejznámější symetrické šifry patří DES, 3DES, AES a IDEA.

DES - „*DES je šifra, která byla vybrána v roce 1976 jako Federal Information Processing Standart pro USA a poté úspěšně mezinárodně rozšířena. Algoritmus byl zpočátku nedokonalý s tajnými částmi, relativně krátkým klíčem a podle National Security Agency, podezřelý. DES se podrobil důkladnému akademickému zkoumání a umožnil porozumění bloku šifer a jeho analýze. V současné době je považována tato šifra za nejistou pro mnoho druhů aplikací. Je to hlavně proto, že jeho klíč je dlouhý pouze 56 bitů a pomocí Brutal Force Attack může být prolomen za méně než 24 hodin. Také se našlo několik analytických výsledků, které potvrzují slabost tohoto algoritmu. Přesto se považuje za relativně bezpečný ve formě Triple DES, na který jsou vyvinuty pouze teoretické útoky. V současné době byla tato šifra nahrazena metodou Advanced Encryption Standard (AES).“* [24]

3DES je šifra, která zvyšuje odolnost jednoduchého DES algoritmu. Šifra se aplikuje třikrát, není nutné přecházet na nový algoritmus. Postupem času se však stala nedostatečnou v porovnání s novými nastupujícími algoritmy.

AES - „*25 let po schválení šifry DES oznámil americký Národní úřad pro standardizaci (NIST) schválení šifry AES jako federální standard USA s platností od 26.5.2002. Rijnda-*

el je původní název algoritmu, který byl přijat jako standard pro šifrování v rámci amerických vládních úřadů. Jako většina šifrovacích algoritmů, i Rijndael odvozuje svůj název od jmen svých autorů: Joan Daemen a Vincent Rijmen. V praxi tedy názvy "Rijdael" a "AES" odkazují na totéž.“ [24]

„AES od tohoto dne oficiálně začala nahrazovat starý standard DES. AES znamená Advanced Encryption standard (Pokročilý šifrovací standard). U AES se očekává životnost minimálně 20 let, podle některých odhadů až 30 let. Šifře AES nehrozí útok hrubou silou (brute force) = vyzkoušení všech možných klíčů, jako třeba u DES pomocí DES Crackeru (viz časopis Chip 11/98). Momentálně se zdá, že je AES neprolomitelná. Výběr nového šifrovacího standardu trval více než čtyři roky, a tak se dá předpokládat, že v dohledné době by neměla být šifra prolomena.“ [24]

IDEA - symetrická bloková šifra. Poprvé byla využita v roce 1991, tehdy byla vytvořena jako náhrada DES. Pracuje s 64bitovými bloky a používá 128bitový klíč. Celý proces šifrování a dešifrování je podobný.

Asymetrickou šifrou je algoritmus, který využívá dva šifrovací klíče. Jeden je klíč veřejný a druhý soukromý. Navzájem od sebe tyto klíče nelze odvodit. Veřejný klíč je používán pro šifrování, soukromý klíč je pak ten, který jako jediný může dané informace dešifrovat do původní podoby. Nedůležitější u tohoto systému je zaručit ochranu soukromého klíče. Je důležité, aby jej měl vždy jen jeho vlastník. Nejznámější asymetrickou šifrou je

RSA - *„Algoritmus RSA publikovali v roce 1978 Ronald Rivest, Adi Shamir a Leonard Adleman. Jedná se o asymetrickou šifru, která je založena na Eulerově větě, a která je použitelná jak pro šifrování, tak pro podepisování dokumentů. Pokud tedy chceme poslat uživateli **A** zprávu takovým způsobem, aby ji nikdo kromě **A** nemohl přečíst, tak si seženeme jeho veřejný klíč $\boldsymbol{A}_{VK}$. Pomocí něj zprávu zašifrujeme a nakonec ji odešleme přes (nezabezpečenou) síť. Obsah zprávy zůstane všem případným útočníkům utajen, protože ji je schopen rozšifrovat pouze držitel odpovídajícího soukromého klíče – uživatel **A**.“* [25]

PRAKTICKÁ ČÁST

4 VÝROBNÍ LINKA NA PLATFORMĚ TIA-PORTAL

Cílem teoretické části je popsat práci ve vývojovém prostředí TIA Portal a tvorbu projektu od návrhu hardwaru, softwaru po vizualizaci. Ukázat možnosti tvorby webového serveru a jeho zabezpečení. Představit vybraný model zabezpečeného komunikačního modulu SCALANCE řady S od společnosti SIEMENS, popsat jeho možnosti a implementovat jeho hlavní zabezpečovací funkce včetně VPN.

Pro modelový návrh projektu automatizovaného zařízení s návrhem řídicí techniky a návrhem vizualizace HMI poslouží jednoúčelové montážní zařízení pro lisování vymezovacích kroužků na hřídele. Povahou procesu je montážní zařízení rozděleno do tří stanic (nasazení kroužku, lisování, kamerová kontrola), které jsou na sobě nezávislé. Z pohledu řízených technologií zařízení obsahuje servopohon FESTO, kamera SICK, čtečka DATAMAN, ventilový terminál FESTO CPX. Na řídicím CPU je zřízen zabezpečený webový server s informacemi o zařízení. Zařízení bude připojeno do sítě internet a zabezpečeno pomocí zabezpečovacího modulu SCALANCE S 623, na kterém je nastaveno VPN pro vzdálenou správu.

Celý projekt je postaven jako ukázka jednotlivých technologií a představení práce s vývojovým prostředím TIA Portal. Na každé zmíněné části jsou popsány vybrané body tak, aby pomohly objasnit problematiku tvorby automatizačního projektu.

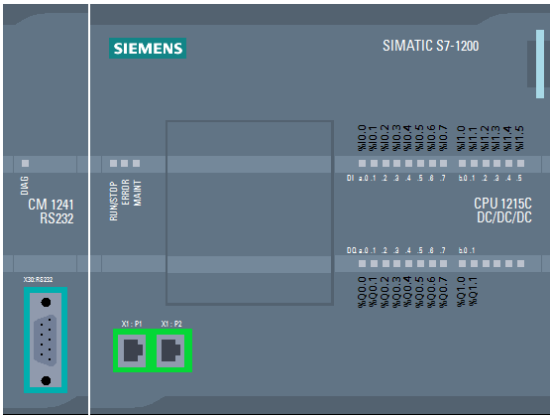
Obr. 32: Modelové zařízení [26]

4.1 Návrh řídicího systému

Pro řízení montážního zařízení je navrhnuto řídicí CPU 1215C, které je svým výkonem dostačující, má integrovány binární vstupy (14) a výstupy (10). Toto CPU je doplněno o komunikační rozhraní RS232 pro scanner DATAMAN. Komunikace s ostatními technologiemi probíhá pomocí průmyslové komunikační sběrnice PROFINET, která je postavena na TCP/IP protokolu.

Hardwarová sestava:

- CPU 1215C DC/DC/DC - Číslo výrobku: 6ES7 215-1AG31-0XB0
- CM 1241 (RS232) - Číslo výrobku: 6ES7 241-1AH32-0XB0

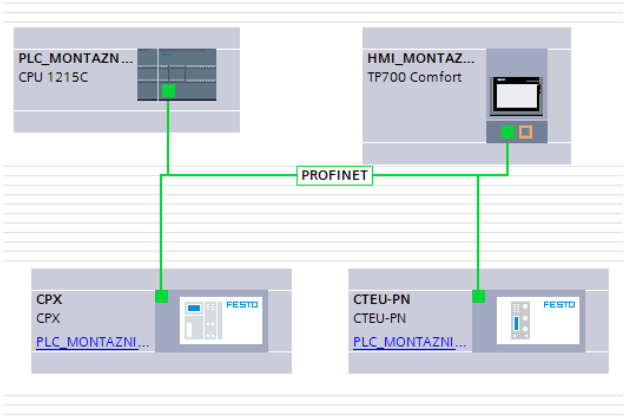


Obr. 33: Sestava řídicího systému (zdroj: vlastní)

Části CPU i CM po vložení do projektu jsou ihned připraveny a ve výchozím nastavení. Výchozí nastavení pro CPU znamená, že pokud uživatel nemá speciální požadavky na parametrizaci určitých řídicích částí, nemusí nic dalšího nastavovat. Nejčastěji upravovaným parametrem je např. adresa obrazu binárních vstupů a výstupů. Pro komunikační kartu CM je výchozí nastavení stavem, kdy je jednotka bez chybových hlášení, ale pro správnou komunikaci RS232 portu je potřeba nastavit parametry (rychlost, parita, stop bit, režim,atd.), které definují přenos telegramu. Nastavení musí být na obou stranách totožné, tedy jak na straně zařízení, tak na CPU.

Dalšími prvky, které řídí CPU a komunikuje s nimi pomocí sítě PROFINET jsou:

- HMI SIEMENS TP700 Comfort
- FESTO CPX ventilový terminál
- FESTO CMMO řízení servopohonu



Obr. 34: Základní síťová struktura (zdroj: vlastní)

HMI bylo zvoleno standardní vizualizační zařízení s dotykovým panelem řady Comfort.

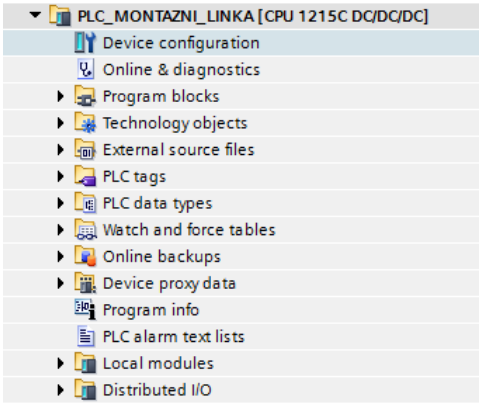
CPX ventilový terminál obsahuje dva vstupní 16b moduly a sadu 32 pneumatických ventilů, které jsou různé podle potřeby a funkce. Doplnění tohoto technologického celku je zprostředkováno pomocí GSD souboru, což je soubor obsahující konfigurační data pro definování komunikace s tímto konkrétním zařízením. Tento GSD soubor je nutné získat od výrobce, v tomto případě byl stažen z oficiálních stránek společnost FESTO.

CTEU - PN je zařízení ze skupiny servořízení nadefinováno jako model CMMO. Doplnění zařízení je zprostředkováno opět GSD souborem.

4.2 Program PLC a vizualizace

S vložením zařízení do projektu se v části Project Tree vytvořily záložky pro správu zařízení CPU a HMI. Vývojové prostředí TIA Portal zahrnuje správu řídicích systémů i vizualizace. Další obsažená zařízení od společnosti FESTO jsou implementovány jako externí.

Záložka PLC v části Project Tree obsahuje veškeré informace hardwarovém nastavení CPU, které jsou zpřístupněny prostřednictvím Device Configuration a informace týkající se programové části.



Obr. 35: Prostředky správy CPU (zdroj: vlastní)

Nejdůležitější částí je složka Program blocks. V této složce je celý program vykonávaný CPU. Výchozí nastavení obsahuje organizační blok s názvem Main. Tento blok je volán v každém cyklu PLC. V tomto bloku se volají všechny funkce obsažené v projektu.

Jako programovací jazyk napříč celým vytvořeným projektem byl zvolen jazyk FBD (jazyk logických schémat), protože je přehlednější i pro složitější funkce a pochopitelnější pro toho, kdo se v problematice neorientuje.

Jelikož je zařízení procesně rozděleno do tří nezávislých stanic, které si pouze přesunují výrobek mezi sebou, je pro řízení režimů, stavů a alarmů použita funkce FB_STEP_CONTROL. Je to funkce, která s využitím dalších dvou funkcí FC_STEP a FC_STEP_DELAY přináší řešení efektivním řízením sekvence.

FB_STEP_CONTROL je funkce, která řídí volbu režimů a funkci sekvence. Dostupnými režimy jsou - manuální režim, automatický režim a reset zařízení. Splněním určitých podmínek lze mezi režimy přepínat.

Vstupy funkce:

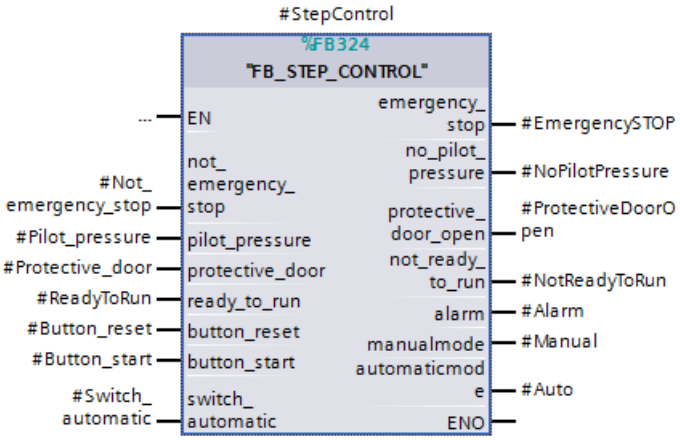
- not_emergency_stop - signál pro stav, kdy není spuštěn nouzový stop
- pilot_pressure - signál pro kontrolu tlaku v zařízení
- protective_door - signál pro kontrolu zavření ochranných dveří
- ready_to_run - uživatelsky definovaný signál
- button_reset - signál z tlačítka reset
- button_start - signál z tlačítka start
- switch_automatic - signál z přepínače manuál/automat

Výstupy funkce:

- emergency_stop - signál pro chybu nouzového zastavení
- no_pilot_pressure - signál pro chybu tlaku
- protective_door_open - signál pro otevření ochranných dveří
- not_ready_to_run - signál pro uživatelsky definovanou chybu
- alarm - obecné chyby, je aktivní vždy, když chybí některý ze vstupních signálů - not_emergency_stop, pilot_pressure, protective_door, ready_to_run
- manualmode - signál spuštění manuálního režimu
- automaticmode - signál spuštění automatického režimu

Důležité statické proměnné:

- step - číslo, které charakterizuje vykonávaný krok
- release - uvolnění vykonávání sekvence, podmíněno nevyvoláním alarmu
- break - zastavení sekvence
- reset_done - příznak ukončení resetu



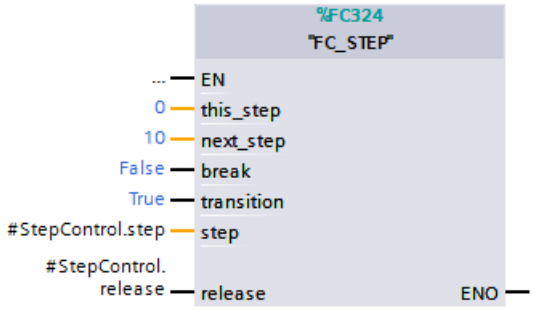
Obr. 36: Funkce Step Control (zdroj: vlastní)

FC_STEP je funkce, která při využití FB_STEP_CONTROL pomáhá řešit problematiku řízení sekvence. Dokáže pracovat s řízením kroků, které je ovládáno pomocí speciálních příznaků. Každé volání této funkce vytváří jeden krok sekvence.

Vstupy funkce:

- this_step - číslo kroku, který funkce definuje
- next_step - číslo dalšího kroku

- break - signál pro zastavení kroku
- transition - signál pro přesun na další krok
- step - číslo aktuálního kroku
- release - uvolnění provádění sekvence

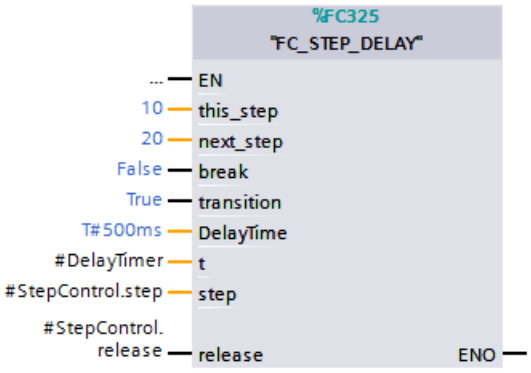


Obr. 37: Funkce Step (zdroj: vlastní)

FC_STEP_DELAY je obdobná funkce jako FC_STEP jen s tím rozdílen, že využívá časového zpoždění pro přesun do dalšího kroku.

Vstupy funkce:

- this_step - číslo kroku, který funkce definuje
- next_step - číslo dalšího kroku
- break - signál pro zastavení kroku
- transition - signál pro přesun na další krok
- delaytime - časová prodleva pro přesun do dalšího kroku
- t - časovač využívaný pro časovou prodlevu
- step - číslo aktuálního kroku
- release - uvolnění provádění sekvence



Obr. 38: Funkce Step Delay (zdroj: vlastní)

V **sekvenci** znázorněné v příloze č.1 je vložena funkce FB_STEP_CONTROL, které byla vytvořena instance StepControl. Vstupům a výstupům funkce byly přiřazeny statické proměnné se stejným názvem. Jejich význam byl zmíněn výše v popisu funkcí.
Krokování je prováděno pomocí číselné proměnné Step instance StepControl, která udává aktuální číslo kroku.
Funkce FC_STEP i FC_STEP_DELAY se chovají tak, že vykonávají určitý krok sekvence, resp. aktivují výstupní signál ENO do stavu TRUE vždy, když jsou splněny tyto podmínky:

- step = this_step - tedy instance StepControl.Step je stejná se zadaným vstupem this_step,
- release = TRUE - uvolnění pro vykonávání sekvence, podmíněno neaktivním alarmem,
- break = FALSE - není aktivní signál pro zastavení sekvence.

Tedy vždy, když proměnná StepControl.Step (aktuální krok) odpovídá vstupu funkce this_step a pokud je sekvence aktivní a není aktivní blokování sekvence, vykoná se obsah kódu závislý na výstupu ENO. Tento kód se vykoná vždy alespoň jednou, dokud nejsou splněny podmínky pro vstupní signál transition. Jakmile dojde ke stavu, kdy je vstupní signál transition = TRUE, do proměnné StepControl.Step se uloží hodnota zadaná do vstupu funkce next_step, čímž dochází k přesunu na další krok.

Tak jak je znázorněno v příloze č.1, je pomocí výše zmíněných funkcí vytvořena řízená sekvence, tedy posloupnost vykonávání kroků. FB_STEP_CONTROL dokáže pracovat ve třech režimech:

- Resetovací režim - vytváří posloupnost kroků, které je potřeba splnit, aby bylo zařízení uvedeno do výchozího stavu (základní pozice), tento režim se využívá vždy při servisu zařízení, nebo po zapnutí, v rámci tohoto režimu je zpřístupněno manuální ovládání zařízení (pneumatických ventilů, servo pohonů, atd.),
- Manuální režim - je režim, kdy je zařízení uvedeno do výchozí pozice, má splněny všechny podmínky pro možnost uvedení do automatického režimu, v rámci tohoto režimu je rovněž zpřístupněno manuální ovládání zařízení,
- Automatický režim - je režim, ve kterém je následující část sekvence prováděna automaticky, v případě přepnutí, nebo vyvolání alarmu je sekvence zastavena v kroku,

který se zrovna vykonával, dalšímu vyvolání tohoto režimu musí předcházet resetovací režim.

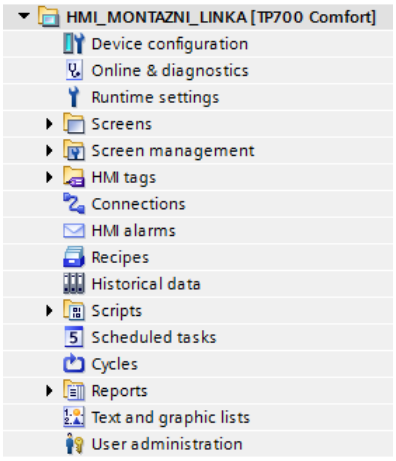
Pro spuštění automatického režimu je potřeba dodržet posloupnost jednoduchých logických úkonů:

1. Je potřeba provést reset zařízení, uvést zařízení do výchozího stavu. Pro spuštění resetovacího režimu je potřeba dodržet určité vstupní podmínky. Přepínač manuál/automat musí být přepnut na manuál, tedy na vstupním signálu funkce FB_STEP_CONTROL switch_automatic musí být hodnota FALSE. Dále musí být splněny kritické bezpečnostní podmínky prezentovány splněním aktivním vstupním signálem na vstupech not_emergency_stop, pilot_pressure, protective_door, ready_to_run. Pokud jsou tyto podmínky splněny a není aktivní alarm, je možné spustit resetovací režim.
2. V další kroku je potřeba stisknout tlačítko reset a tím uvést vstup buton_reset do aktivního stavu. Náběžnou hranou tohoto signálu je spuštěna sekvence vyhrazená pro reset. Splní se všechny kroky až do kroku 100. Tento krok je zvolen jako krok, ve kterém je dosaženo výchozí pozice. Proto je při dosažení tohoto kroku aktivována statická proměnná reset_done, která zastavuje pokračování sekvence. Bylo dosaženo manuálního režimu.
3. Aktivovat automatický režim je možné až v tuto chvíli a to tím, že se přepne přepínač manuál/automat do stavu automat, což aktivuje vstup switch_automatic a stiskne se tlačítko start, tedy uvedeme vstup button_start do stavu TRUE. Tímto je spuštěn automatický režim.

K signalizaci aktivního režimu slouží výstupy funkce manualmode, automaticmode. Automatický režim lze kdykoliv přerušit přepnutím přepínače manuál/automat na manuál, tedy switch_automatic = FALSE a tím sekvenci přerušit. K uvedení do provozu je potřeba opět dodržet předepsaný postup.

Využití těchto funkcí pro řízení sekvence vede ke zvýšení přehlednosti díky jednoduché práci s krokováním, zjednodušují se možnosti diagnostiky, nebo dohledávání v sekvenci. Přidávání kroků do sekvence, nebo úpravy jsou pro přehlednější a rychlejší. Celý tento systém je lépe pochopitelný i pro neznalé uživatele.

Záložka HMI v části Project Tree obsahuje veškeré informace o hardwarovém nastavení operačního panelu a informace týkající se vizualizační části.



Obr. 39: Prostředky správy HMI (zdroj: vlastní)

Protože tento operační panel je hlavně vizualizačním nástrojem, stává se nejdůležitější částí správa obrazovek a práce s nimi. Obrazovka je ve vývojovém prostředí TIA Portal značena jako Screen.

Do obrazovek je možné vkládat objekty dle jejich zařazení do tří hlavních skupin:

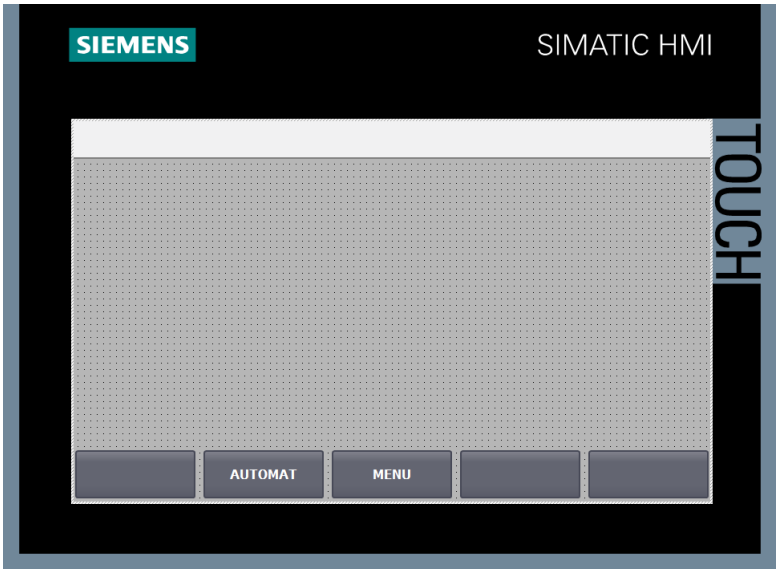
- základní objekty: čáry, grafické objekty - čtverce, obdélníky, polygony, kružnice, textové pole, grafické pole
- funkční objekty: vstupní a výstupní textová pole, tlačítka, rozevírací seznam, přepínače, grafy, posuvníky
- speciální objekty: objektová pole, složité grafy, přehrávač videí, PDF prohlížeč, prohlížeče PLC kódu

Všem objektům lze nastavit širokou škálu vlastností. Je možné nastavovat velikost, barvy, tloušťky čar, grafické přechody a další. Navíc je možné každému objektu vytvořit možnost řízených animací, což jsou určité akce (změna podbarvení, změna pozice, viditelnost), které je možné propojit s proměnnými, nebo daty z řídicího CPU. V praxi je tedy možné, například v případě spuštění některého ventilu, podbarvit tlačítka pro manuální ovládání. Nejčastěji používané objekty a jejich využití je předvedeno v další části ve vypracovaných funkčních obrazovkách.

Při návrhu kompletní vizualizace je potřeba se zamyslet nad využitelností a optimalizací. Jelikož se obrazovky dají přizpůsobit napříč celým vizualizačním projektem, je vhodné

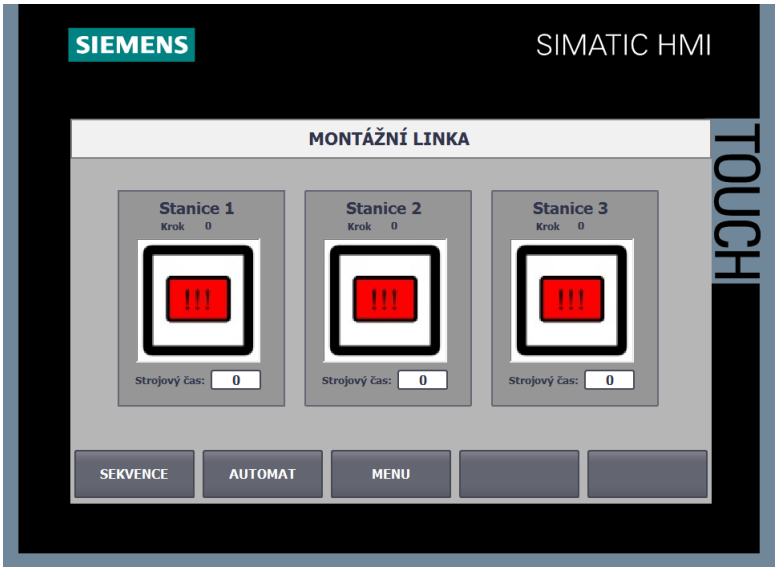
uvažovat o možnosti využití šablony, která bude pro každou obrazovku stejná, případně s malými odchylkami. Celý projekt pak působí celistvě a druhořadým výsledkem je i efektivnější práce při návrhu jednotlivých obrazovek.

Šablona vytvořeného projektu, která tvoří základ jednotlivých obrazovek je navrhnuta tak, aby vymezovala dostatečný prostor pro doplnění vizualizačních prvků jednotlivým účelově orientovaným obrazovkám a zároveň aby splňovala pomyslný funkční standard pro volání dalších obrazovek. Navíc je po vizuální stránce uživatelsky přívětivá. Obsahuje pět jednoduchých tlačítek, které se obsazují podle potřeby. Určitá tlačítka si však svůj účel ponechávají napříč celým projektem. Je to například tlačítko AUTOMAT, které aktivuje výchozí obrazovku AUTOMAT a tlačítko MENU, které aktivuje tlačítko menu.



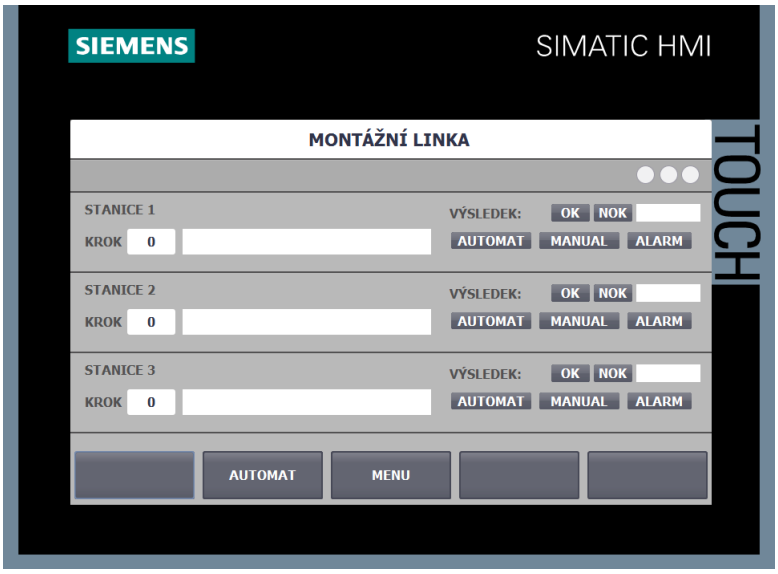
Obr. 40: Šablona HMI (zdroj: vlastní)

Hlavní obrazovka, která je nastavena jako výchozí je obrazovka **AUTOMAT**. Ta je optimalizována tak, aby byla dostatečně srozumitelná pro obsluhu. Pomocí grafického pole zobrazuje pracovní postup jednotlivých stanic, signalizuje případné poruchy, při kterých se dále zobrazí objektové okno s alarmy a jejich popisem. Doplňkem je zobrazení strojového času jednotlivých stanic, tedy doby cyklu zpracování jedné operace na výrobku. Navíc obsahuje tlačítko SEKVENCE pro zobrazení obrazovky sekvence.



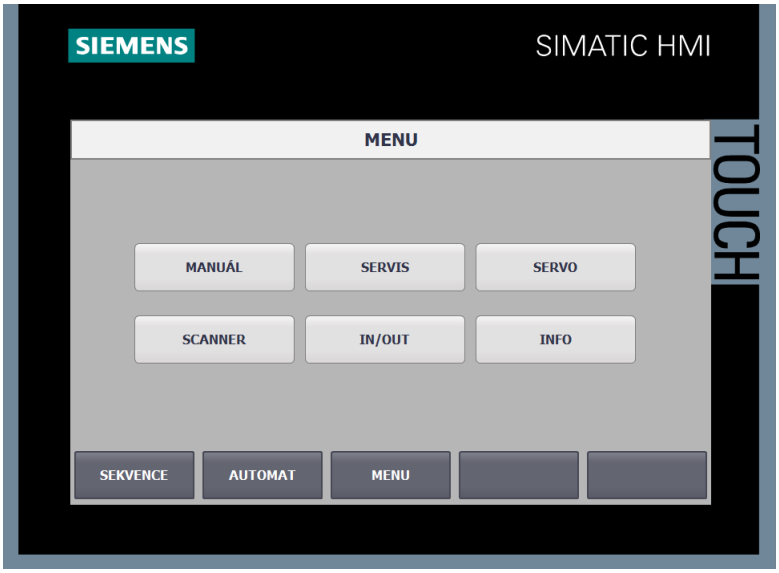
Obr. 41: Obrazovka AUTOMAT (zdroj: vlastní)

Obrazovka **SEKVENCE** zobrazuje aktuální stav sekvencí jednotlivých stanic. Ke každé stanici zobrazuje základní, ale dostačující informace o stavu, čísle kroku, popisu kroku, režimu a výsledku operace.



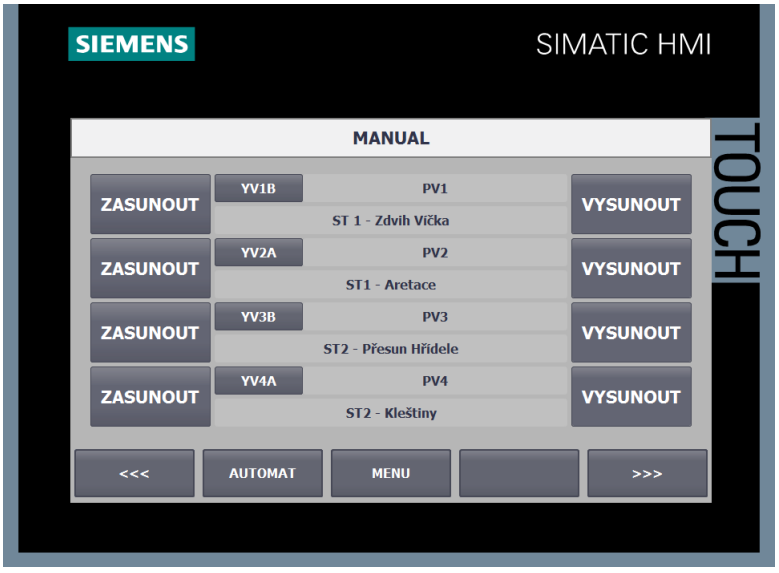
Obr. 42: Obrazovka SEKVENCE (zdroj: vlastní)

Obrazovka **MENU** obsahuje odkazy na další obrazovky důležité pro správu zařízení.



Obr. 43: Obrazovka MENU (zdroj: vlastní)

Obrazovka **MANUAL** umožňuje ovládání pneumatických ventilů, resp. pneumatických pohonů, v manuálním režimu. Jednoduchými tlačítky se změnou podbarvení v závislosti na stavu ventilů a senzoriky vzniká přehledná a univerzální ovládací struktura.



Obr. 44: Obrazovka MANUAL (zdroj: vlastní)

Tvorba vizualizace napříč projektem je ve vývojovém prostředí TIA Portal poměrně přehledná a jednoduchá. Tím, na co je potřeba klást důraz, je optimální návrh šablon a provázání obrazovek.

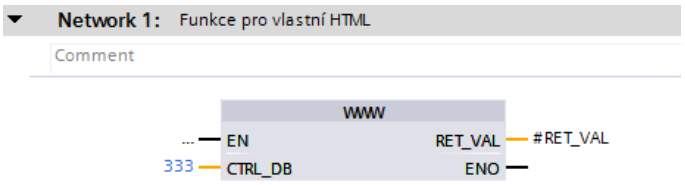
Zajímavým doplňkem vývojového prostředí je volba jazykových mutací. Ta funguje napříč celým projektem, ale nejvíce se využívá u vizualizace. Je tedy možné si v základním na-

stavení projektu nastavit jaké jazyky se budou využívat a systém vygeneruje tabulku textů, do které můžeme doplnit překlady jednotlivých popisků. Přepínání lze ovládat přímo z vizualizace.

4.3 Webový server

Jak již bylo zmíněno, CPU řady S7-1200 má ve své výbavě i **webový server**. Ten slouží k jednoduchému získávání informací z řídicího CPU. Informace mohou být různorodé a budou podrobněji vysvětleny v další části, ale zpravidla jde o informace o hardware, informace o stavu CPU, alarmové hlášení apod.

HTML dokument webového serveru PLC vychází z implementované šablony. Do této šablony je možné vložit i vlastní tvorbu, tedy vlastní dílčí webové stránky, kterými můžou být např. vizualizace, a přistupovat k datům, která jsou zpřístupněna pomocí systémové funkce SFC99 (WWW) v PLC programu. Tato funkce odkazuje na data z definovaného datového bloku.



Obr. 45: Funkce pro správu HTML (zdroj: vlastní)

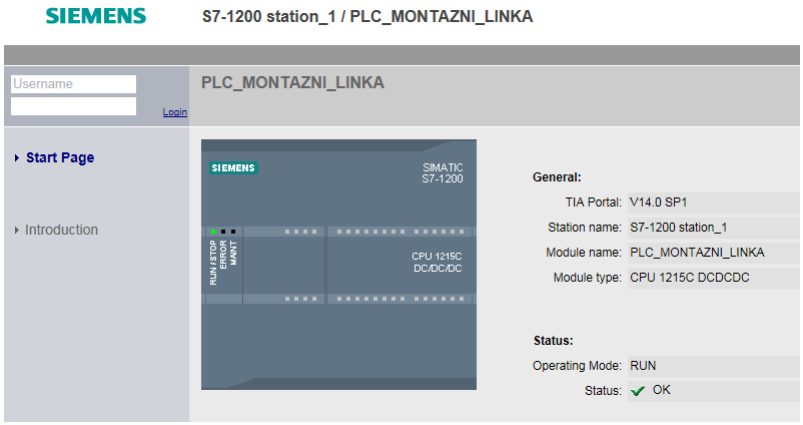
V tomto modelovém projektu je využita pouze implementovaná šablona. Ta umožňuje spravovat uživatele přistupující k webovému serveru. Administrace uživatele spočívá ve volbě jména, vytvoření hesla a definování přístupů k jednotlivým parametrům, nebo informacím. Po přihlášení do webového serveru se prohlížeč přizpůsobí vybraným uživatelským datům.

Hlavní uživatelská přístupová práva:

- read tags - čtení proměnných,
- write tags - zápis proměnných,
- open user-defined web pages - otevření uživatelsky definovaných webových stránek,
- write in user-defined web pages - zápis do uživatelsky definovaných webových stránek,

- change operating mode - změna operačního módu (RUN, STOP, MRES),
- acknowledge alarms - potvrzení alarmů.

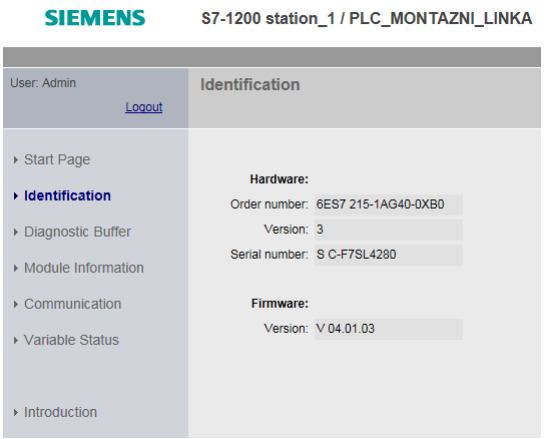
Po otevření hlavní webové stránky se zobrazí základní informace o CPU a možnost přihlášení uživatele. Základní zobrazené informace jsou typ CPU, operační režim a status.



Obr. 46: Webový server PLC - startovací obrazovka (zdroj: vlastní)

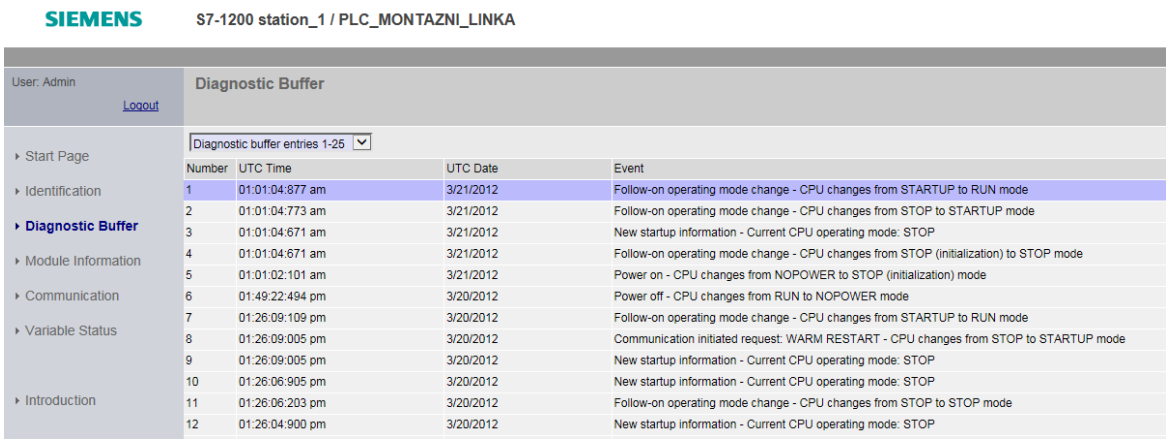
Pro vytvořený uživatelský účet Admin jsou zpřístupněna všechna přístupová práva. Po přihlášení profilu se zobrazí záložky odkazující na definované uživatelské informace.

Záložka **Identification** zobrazuje konkrétní informace o CPU a to katalogové číslo, sériové číslo a verzi firmware.



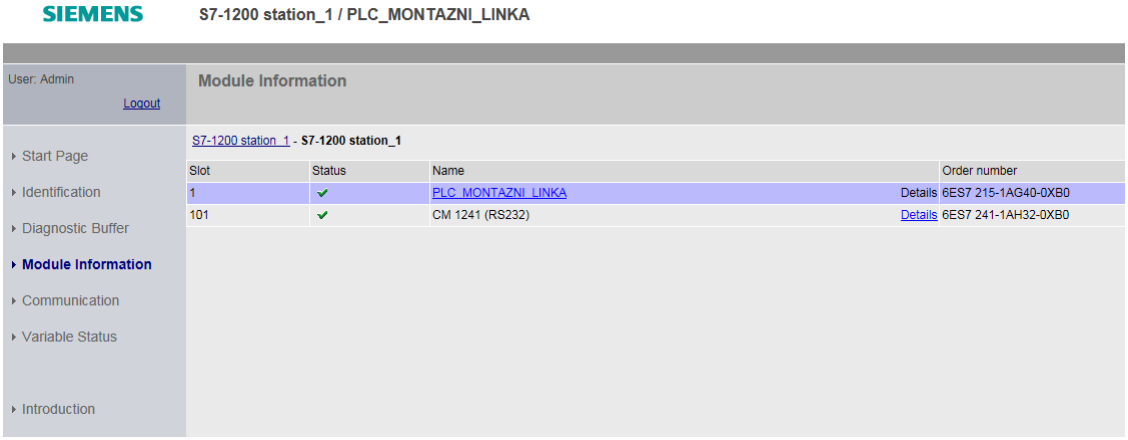
Obr. 47: Webový server PLC - obrazovka Identification (zdroj: vlastní)

Záložka **Diagnostic Buffer** zobrazuje historii diagnostiky CPU. Zde jsou zobrazeny všechny chyby a stavy dotýkající se operačních stavů PLC. Tedy jaká chyba vedla k zastavení CPU, stavové hlášení po obnovení režimu, nebo resetu.



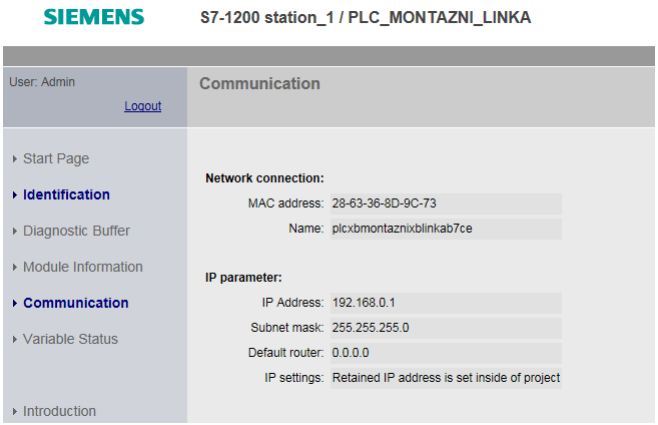
Obr. 48: Webový server PLC - obrazovka Diagnostic Buffer (zdroj: vlastní)

Záložka **Module Information** umožňuje získat informace o hardwarové konfiguraci a stavu jednotlivých prvků.



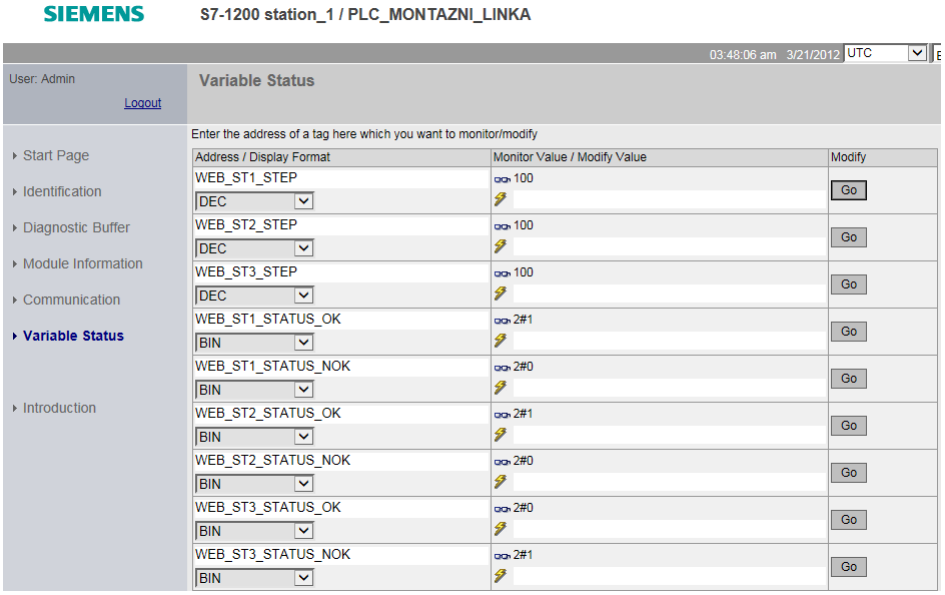
Obr. 49: Webový server PLC - obrazovka Module Information (zdroj: vlastní)

Záložka **Communication** zobrazuje nastavení sítě řídicího CPU.



Obr. 50: Webový server PLC - obrazovka Communication (zdroj: vlastní)

Záložka **Variable Status** je záložka, která umožňuje sledovat a měnit definované proměnné.

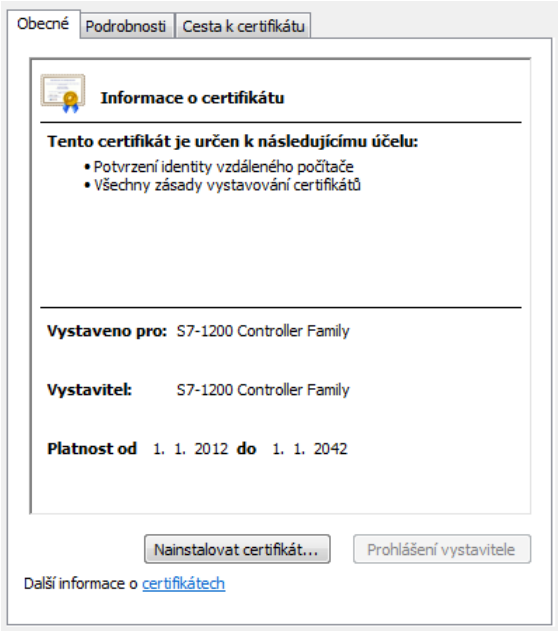


Obr. 51: Webový server PLC - obrazovka Variable Status (zdroj: vlastní)

Webový server umožňuje zabezpečenou komunikaci protokolem HTTPS, který je popsán v teoretické části. Tento protokol zajišťuje autentizaci, důvěryhodnost dat a jejich integritu. Navíc pomáhá bojovat s **Man InThe Middle** útokem, zmíněným v teoretické části, což je v informatice útok formou odposlouchávání. Díky tomuto by se útočník mohl dostat k citlivým informacím včetně hesla.

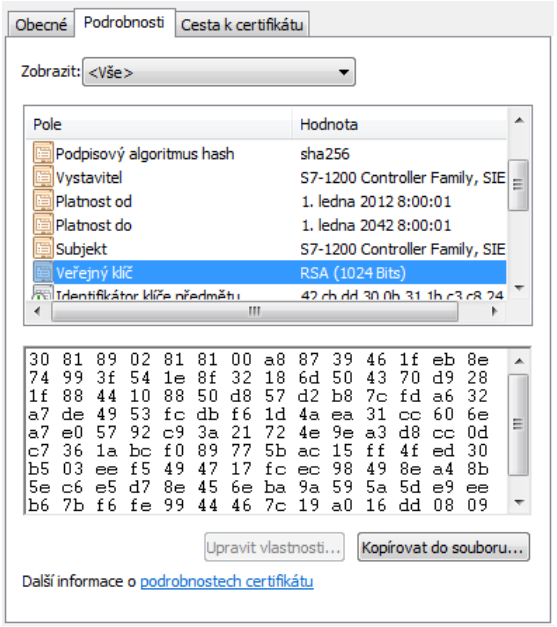
Možnost nastavení HTTPS protokolu ve vývojovém prostředí TIA Portal je v hardwarové konfiguraci řídicího CPU. Společnost SIEMENS k zabezpečení používá svůj digitální

certifikát, čímž se stává vlastní certifikační autoritou. Certifikát je implementován přímo do webového serveru.



Obr. 52: Digitální certifikát (zdroj: vlastní)

Digitální certifikát používá pro šifrování veřejného klíče asymetrickou šifru RSA s délkou klíče 1024 b, což v kombinaci s podpisovým algoritmem hashem sha256 vytváří dostatečně robustní formu zabezpečení.



Obr. 53: Vlastnosti digitálního certifikátu (zdroj: vlastní)

Certifikát je dostupný přímo z úvodní webové stránky po aktivaci HTTPS protokolu v hardwarové konfiguraci CPU. Z této stránky stačí certifikát stáhnout a nainstalovat. Automaticky se zařadí do důvěryhodných kořenových certifikátů a po obnovení stránek již prohlížeč využívá této zabezpečené komunikace.

4.4 Komunikační modul SCALANCE

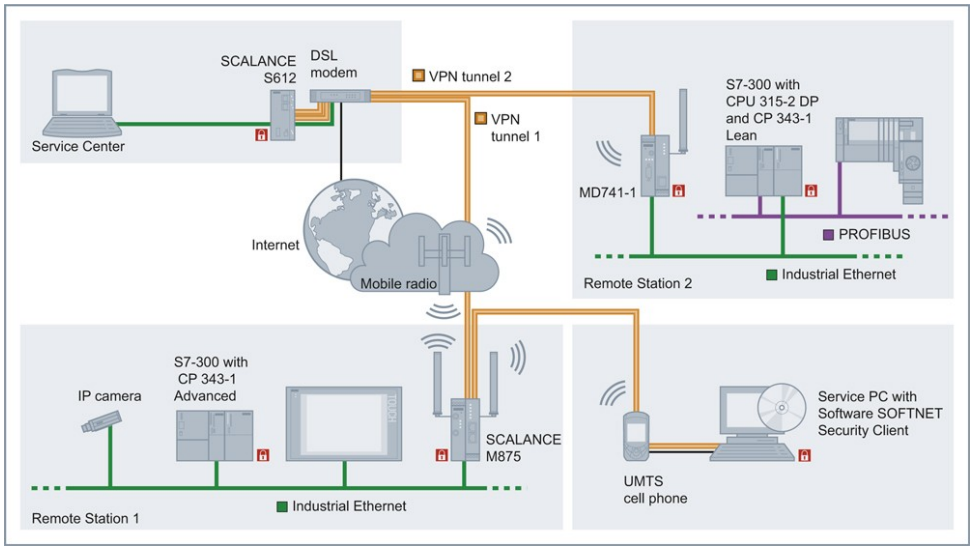
Zařízení je v modelovém projektu zabezpečeno pomocí zabezpečovacích komunikačních modulů SCALANCE řady S od společnosti SIEMENS.

Zařízení pro průmyslové zabezpečení **SCALANCE S** podporuje koncepci "Defense in depth", což je koncepce využití více vrstev bezpečnostních kontrol (využití nadbytečnosti v případě selhání zabezpečení). Zabezpečuje sítě automatizace a bezproblémově se dokáže připojit do struktury kancelářské sítě, nebo i sítě Internet. Umožňuje efektivně řešit segmentování sítí a ochranu datové komunikace pomocí firewallu a VPN (virtuální privátní sít). Zařízení poskytují ochranu automatizace především v sítí diskrétní výroby a procesního průmyslu. Předností je i robustní průmyslové provedení. Všechny modely řady S umožňují správu zařízení z vývojového prostředí TIA Portal.

Obr. 54: SCALANCE S612 [27]

Vybraný **model S612** je vhodnou alternativou pro zabezpečení v jednoduché průmyslové síti. Charakteristickou vlastností tohoto modelu, na kterou se tento projekt zaměřuje, je podpora VPN a firewallu. Dále podporuje router a bridge režim, DHCP server, NAT (překlad síťových adres), NAPT (překlad portů), umožňuje archivaci událostí z provozu na Syslog server, zálohování konfigurace na paměťové médium C-plug.

Využití tohoto komunikačního modulu je patrné z obrázku č. 55. Zde je komunikační modul využíván pro spojení bezpečného servisního centra a průmyslové automatizace využitím VPN tunelu v síti internet. Na straně automatizace jsou využity další komunikační zařízení z produktů řady SCALANCE, které ji chrání, a se kterými je vytvářen VPN tunel. Pokud by nešlo o bezdrátové připojení do sítě internet, pak by mohl všechny tyto moduly nahradit SCALANCE S612.



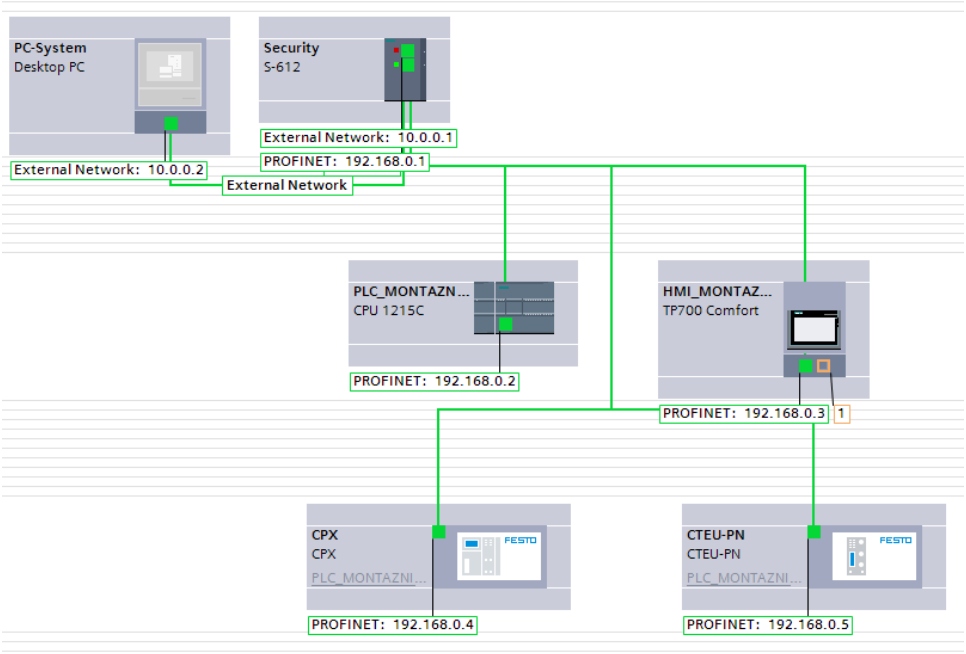
Obr. 55: Využití komunikačních modulů SCALANCE [28]

Do stávajícího modelového projektu je vložen modul SCALANCE S612 spolu s blíže nespecifikovaným počítačovým systémem, který slouží pouze pro ukázku nastavení. Vložením zabezpečovacího modulu je v prostředí TIA Portal v části Project Tree aktivována nabídka pro správu zabezpečovacích funkcí a globálních zabezpečovacích pravidel.

Obr. 56: Globální zabezpečovací pravidla (zdroj: vlastní)

Struktura vnitřní a vnější sítě je zobrazena na obrázku č. 57. Vnitřní síť je tvořená PLC řídicím systémem, operačním panelem, ventilovým terminálem CPX a řídicím systémem servopohonu. Tato síť obsahuje IP adresy v rozsahu 192.168.0.1 - 192.168.0.5. Vnější síť je zobrazena pouze jako spojení komunikačního modulu s počítačovým systémem s IP

adresovým rozsahem 10.0.0.1-10.0.0.2. Ve vnější síti je možné si představit jakékoli další zařízení, nebo spojení se sítí internet.



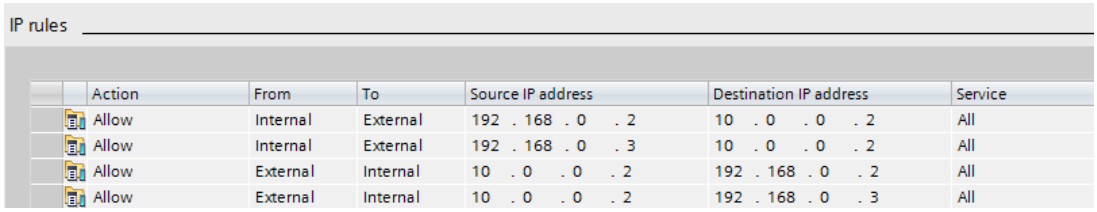
Obr. 57: Struktura sítě (zdroj: vlastní)

4.5 Firewall

Pro zabezpečení automatizace, v tomto případě výrobní linky, nebo výrobního zařízení, je nejdůležitějším opatřením zabránění přístupu do vnitřní sítě s PLC, aby nemohlo dojít k manipulaci se softwarem, protože to je v naprosté většině případů, u zabezpečení automatizace, největší hrozba při napadení. Proto zde hraje hlavní roli firewall. Jak již bylo popsáno Firewall slouží k řízení síťového provozu a definuje pravidla komunikace mezi sítěmi. U tohoto modelu firewall umožňuje vybrat určité druhy protokolů, které mohou mezi sítěmi procházet v jednom, nebo druhém směru. Mezi takové protokoly patří:

- HTTP/HTTPS
- FTP/FTPS
- S7 protokol
- DNS
- NTP
- DHCP
- IP komunikace

Pokud, je ale potřeba definovat konkrétní spojení, vývojové prostředí TIA Portal nabízí řešení. Řešení je buď to formou nastavení globálních pravidel, která se nastavují v Global security setting záložce Firewall, nebo přímo v konkrétním komunikačním modulu. Pravidla mohou být nastavená jako paketový filtr pro konkrétní IP, nebo MAC (fyzické) adresy.

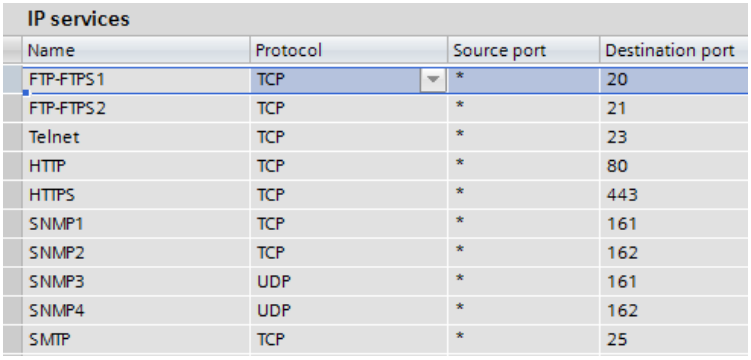


IP rules

	Action	From	To	Source IP address	Destination IP address	Service
	Allow	Internal	External	192 . 168 . 0 . 2	10 . 0 . 0 . 2	All
	Allow	Internal	External	192 . 168 . 0 . 3	10 . 0 . 0 . 2	All
	Allow	External	Internal	10 . 0 . 0 . 2	192 . 168 . 0 . 2	All
	Allow	External	Internal	10 . 0 . 0 . 2	192 . 168 . 0 . 3	All

Obr. 58: Nastaveni IP pravidel firewallu (zdroj: vlastní)

Možné je i nastavení pravidla pro konkrétní podporovaný protokol s definovaným portem.



IP services

Name	Protocol	Source port	Destination port
FTP-FTPS1	TCP	*	20
FTP-FTPS2	TCP	*	21
Telnet	TCP	*	23
HTTP	TCP	*	80
HTTPS	TCP	*	443
SNMP1	TCP	*	161
SNMP2	TCP	*	162
SNMP3	UDP	*	161
SNMP4	UDP	*	162
SMTP	TCP	*	25

Obr. 59: Nastavení protokolů (zdroj: vlastní)

Pro modelový projekt výše uvedené nastavení znamená, že s některými prvky vnitřní sítě může komunikovat pouze počítačový systém s IP adresou 10.0.0.2. Ten má nastavená pravidla pro komunikaci dovnitř i ven se dvěma zařízeními, které jsou řídicí PLC a operační panel. Komunikace v těchto případech není nijak omezena, v případě potřeby je možné ji omezit například jen pro práci s webovým serverem HTTP/HTTPS, pro vzdálenou správu pomocí Telnet protokolu, nebo vytvořením skupiny libovolných protokolů. Veškeré další pokusy o komunikaci z vnější sítě nejsou přijímány.

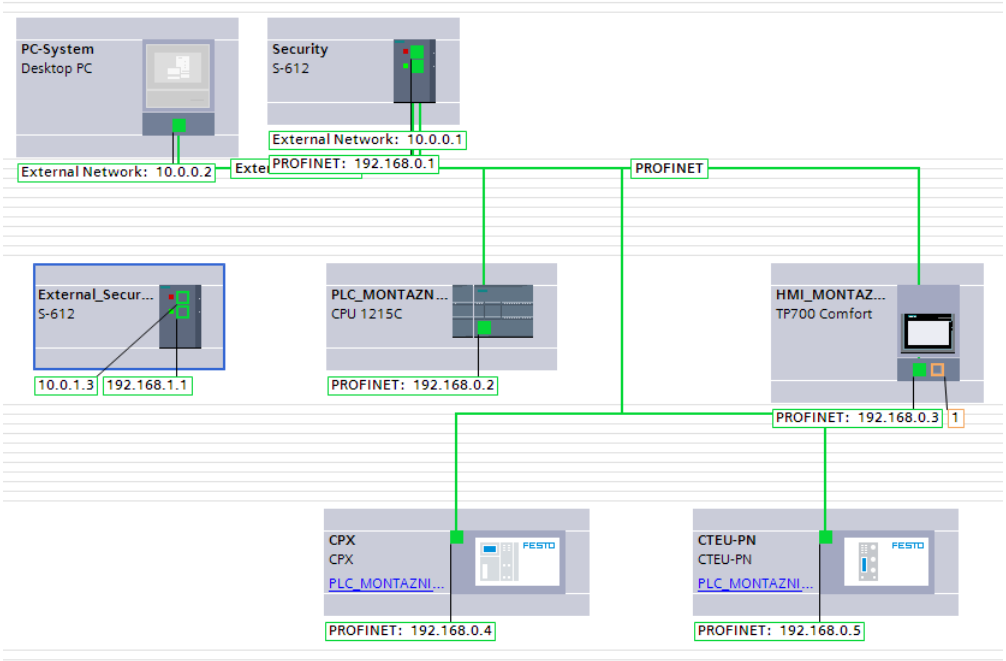
4.6 VPN

Druhým charakteristickým prvkem komunikačního modulu SCALANCE S612 je možnost zřízení VPN, tedy zabezpečeného spojení síťových prvků, v nezabezpečené, nebo nedůvěryhodné síti. Tohoto spojení se u automatizace využívá především pro vzdálenou správu

projektu PLC, tedy při servisu, přístupu k datům, nebo úpravách řídicího softwaru. Mezi síťovými prvky se vytvoří šifrovaný tunel, který udržuje bezpečné spojení.

V modelovém projektu je nejdříve ukázka vytvoření VPN mezi dvěma síťovými prvky a následně ukázka vytvoření VPN mezi síťovým prvkem a klientem pro připojení do VPN pomocí software SOFTNET Security Client, který slouží k vytvoření tunelu z osobního počítače, nebo notebooku.

Do výchozího nastavení sítě v projektu, ve kterém je síť rozdělena komunikačním modulem SCALANCE S612, je přidán další komunikační modul, který bude sloužit jako druhý síťový prvek pro vytvoření VPN. Zmíněný komunikační modul byl označen jako External_Security.

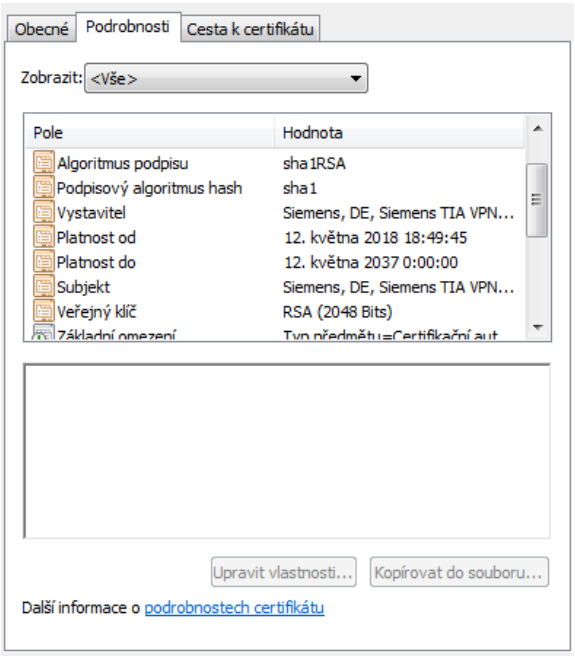


Obr. 60: Struktura sítě se dvěma komunikačními moduly (zdroj: vlastní)

VPN je možné nastavit v sekci Global security settings, záložce VPN skupina. Zde je potřeba vytvořit VPN skupinu, která vytyčí bezpečnostní pravidla a přijme společné nastavení pro vybraná síťová zařízení.

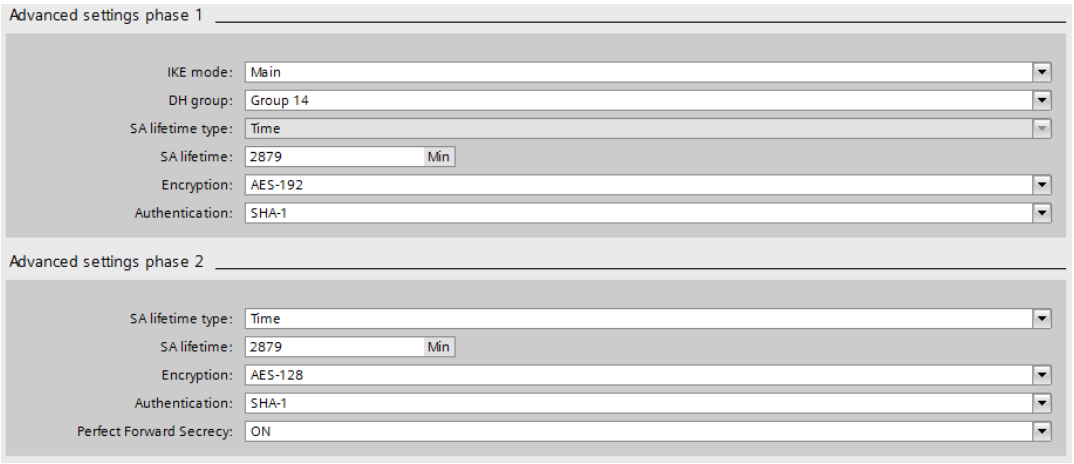
Při tvorbě VPN je potřeba definovat nastavení virtuální sítě. Jako první definovatelná vlastnost se nabízí volba způsobu autentizace mezi přednastaveným klíčem a digitálním certifikátem. U volby využití digitálního certifikátu je potřeba požadovaný certifikát vygenerovat přímo ve vývojovém prostředí TIA Portal. Tímto způsobem se vygeneruje digitální

certifikát s platností na 20 let. Pro modelový projekt byl zvolen digitální certifikát, viz obrázek č. 61.



Obr. 61: Vlastnosti digitálního certifikátu (zdroj: vlastní)

Pro nastavení způsobu autentizace mezi síťovými prvky, je dále potřeba nastavit a definovat **IKE (výměna internetového klíče)**. Tato výměna probíhá ve dvou fázích, kde každá má určité nastavitelné vlastnosti. Ve vývojovém prostředí je možnost nastavení jednotlivých parametrů omezena na možnosti a vlastnosti jednotlivých síťových prvků vložených do skupiny.

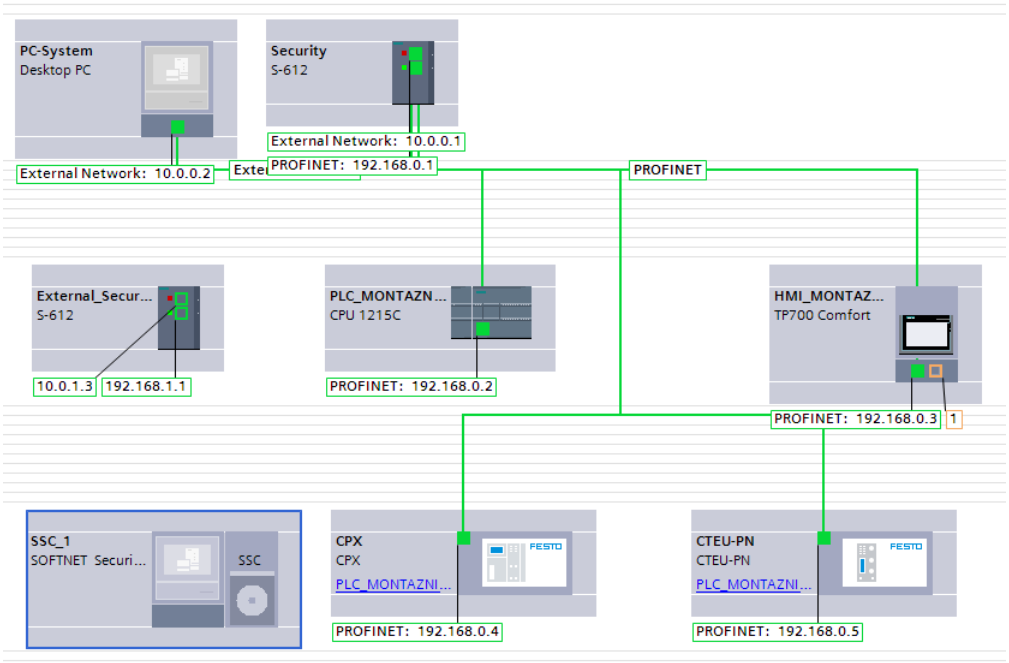


Obr. 62: Nastavení IKE (zdroj: vlastní)

Na obrázku č. 62 je zobrazeno jakým způsobem je možné nastavit parametry obou fází, aby vyhovovaly možnostem komunikačního modulu SCALANCE S612. IKE mód je nastaven na Main, což je mód, který chrání identitu komunikujících stran. DH group (Diffie-Helman protokol) je nastavení kryptografického protokolu, který umožňuje nezabezpečeným kanálem vytvořit šifrované spojení. Dále je zobrazen čas, po který je možné udržet spojení, šifrování a autentizace hashem.

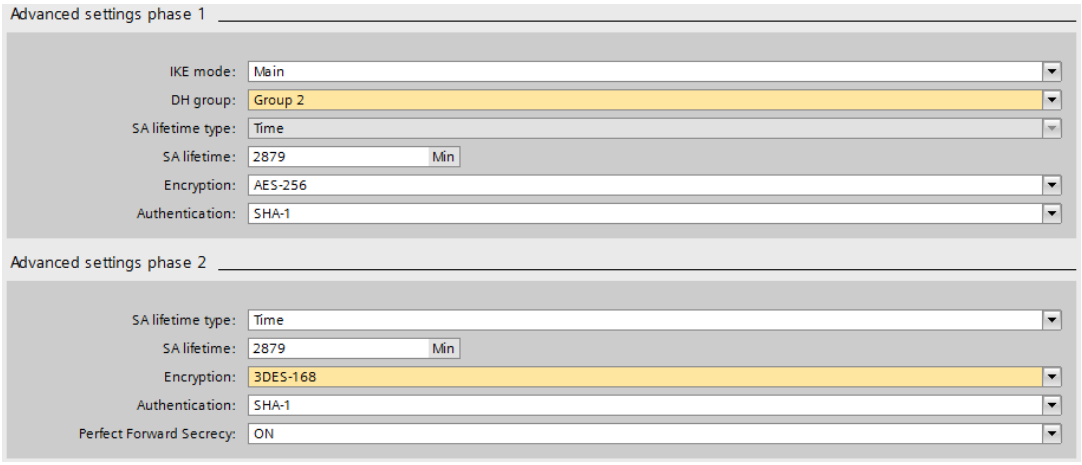
Další nastavení potřebné pro vytvoření VPN je poměrně jednoduché. Výše popsané nastavení je potřeba pouze potvrdit v hardwarové konfiguraci jednotlivých síťových prvků a ID sítě, která je pro VPN tunel zpřístupněna. V nastavení firewallu je nutné vytvořit jednoduchou podmínku pro přístup z VPN tunelu.

Pokud je třeba vyřešit vzdálenou správu automatizace je možné vytvořit VPN tunel pomocí softwaru **SOFTNET Security Client**.



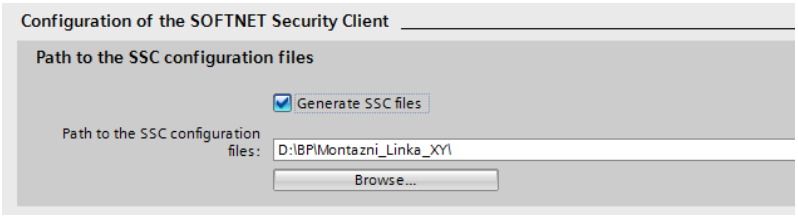
Obr. 63: Struktura sítě s využitím SOFTNET Security Client (zdroj: vlastní)

Celé nastavení ve vývojovém prostředí TIA Portal je stejné jako v předchozím případě, jen s tím rozdílem, že pro kombinaci síťového prvku a software SOFTNET Security Client ve VPN skupině padne změna na nastavení IKE patrná z obrázku č. 64.



Obr. 64: Nastavení IKE - SOFTNET Security Client (zdroj: vlastní)

Změna nastala v nastavení Diffie-Helman protokolu a způsobu šifrování. Ze strany software SOFTNET Security Client je také potřeba nastavit spojení. To však probíhá pomocí importu konfiguračního souboru generovaného v hardwarovém nastavení tohoto softwarového prvku, který byl do projektu vložen stejným způsobem, jako ostatní fyzické prvky.



Obr. 65: Generování konfiguračního souboru (zdroj: vlastní)

Po výše popsaném nastavení je PLC systém i se zvolenými síťovými prvky připraven k provozu.

Možnosti **síťových útoků**, které byly zmíněny v teoretické části (skupina DoS útoků a Port scanning), byly nastaveným opatřením značně omezeny.

- Dos útoky (skupina útoků zaměřených na síťovou službu) - možnosti takovéhoto druhu útoku se pomocí nastavených pravidel firewallu razantně snížily, ale protože nelze úplně zablokovat síťový port, nemůže být absolutně účinný,
- Port scanning - firewall umožňuje pokusy o spojení některých portů blokovat, dokáže dokonce skenování rozpoznat a další komunikaci zablokovat, čili je opatřením i pro takovýto druh útoku.

V souhrnu se správným nastavením pravidel firewallu podařilo snížit riziko napadení uvedenými druhy útoků, které se zaměřují na zablokování sítě, nebo některé její služby. A pomocí zabezpečené virtuální privátní sítě se podařilo vytvořit bezpečný síťový systém uvedeného zařízení, nebo výrobní linky. Opatřením bylo dosaženo vysokého stupně zabezpečení jak pro redundantní zabezpečení v rozsáhlé firemní síti, tak pro přímé připojení do sítě Internet.

ZÁVĚR

Cílem bakalářské práce bylo vytvoření projektu výrobní linky na platformě TIA Portal a zabezpečení připojení do sítě Internet, spolu se zabezpečením vytvořeného webového serveru.

První část bakalářské práce popsala problematiku automatizační techniky. Představila práci s vývojovým prostředím TIA Portal, tvorbu programu a způsob programování včetně vizualizace. Popsala možnosti webového serveru integrovaného do řídicího systému a serverového zabezpečení. Byla popsána síťová problematika, hlavní možnosti síťového zabezpečení a funkce VPN.

V druhé, praktické části se bakalářská práce věnovala návrhu konkrétního zabezpečovaného zařízení. Byl vytvořen projekt s vybraným PLC systémem a vizualizačním zařízením. V rámci softwarového vybavení byla vytvořena ukázka tvorby programové sekvence a tvorby vizualizace. V PLC byl aktivován webový server, nastaven a zabezpečen. Do vytvořené sítě byl vložen komunikační modul, který pomocí nastavení zabezpečil síťové připojení do vnější sítě. Pro vzdálenou správu byla vytvořena VPN.

Síťovým zabezpečením použitou technologií se snížilo riziko napadení vnitřní sítě. Podařilo se vytvořit bezpečný síťový systém pro vytvořenou automatizovanou linku. Díky integraci síťových technologií do vývojového prostředí TIA Portal se zvyšuje uživatelský komfort a podpora síťového řízení a zabezpečení pro oblast automatizační techniky.

SEZNAM POUŽITÉ LITERATURY

[1] ŠMEJKAL, Ladislav a Marie MARTINÁSKOVÁ. PLC a automatizace. Praha: BEN - technická literatura, 1999. s.6-45. ISBN 9788086056586.

[2] JORK SPOL s.r.o. In: *Operátorský panel SIMATIC HMI TP700 COMFORT - 7″* [online]. 2015 [cit. 2018-05-10]. Dostupné z: http://www.jork.shop/produkt/automatizacni-systemy/vizualizace-panely/6av2124-0gc01-0ax0-85938.htm

[3] Ebay. In: *Siemens Simatic S7 300 CPU 315-2dp Di Do AI AO Complete Profibus PLC SPS Analog* [online]. [cit. 2018-05-10]. Dostupné z: https://www.ebay.co.uk/p/Siemens-Simatic-S7-300-CPU-315-2dp-Di-Do-AI-AO-Complete-Profibus-PLC-SPS-Analog/1411698764

[4] Information technology intelligent software. In: *RS facilita il passaggio a LOGO! 8* [online]. [cit. 2018-05-09]. Dostupné z: https://www.itismagazine.it/news/14543/rs-facilita-passaggio-logo-8/

[5] TME Electronic Components. In: *SIEMENS 6ES7211-0BA23-0XB0*[online]. [cit. 2018-05-09]. Dostupné z: https://www.tme.eu/sk/details/6es7211-0ba23/riadiace-cleny-plc/siemens/6es7211-0ba23-0xb0/

[6] GRUPS Automation. In: *Siemens Plc S7 1500* [online]. [cit. 2018-05-09]. Dostupné z: http://www.plccontrolpanel.com/siemens-plc-s7-1500.html

[7] HRUŠKA, František a Ladislav ŠMEJKAL. Technické prostředky informatiky a automatizace: (úvod, popis funkce, konstrukce a aplikace). Vyd. 1. Ve Zlíně: Univerzita Tomáše Bati, 2007, s.53. ISBN 978-807-3185-350.

[8] ŠMEJKAL, Ladislav. PLC a automatizace 2. Praha: BEN - technická literatura, 2005. s.22-23. ISBN 80-7300-087-3.

[9] BERGER, Hans. *Automating with SIMATIC S7-1500 Configuring, Programming, Motion Control and Security inside TIA Portal*. Erlangen: PUBLICIS, 2013. s.22-32. ISBN 978-389-5784-040.

[10] BERGER, Hans. *Automating with SIMATIC: Hardware and Software, Configuration and Programming, Data Communication, Operator Control and Monitoring*. 2016. s.25. ISBN 978-3-89578-459-0..

[11] Thawte it's a trust thing. *Co je to SSL* [online]. [cit. 2018-05-12]. Dostupné z: http://www.ssl-thawte.cz/ssl/co-je-to-ssl/

[12] Support Ricoh. In: *Konfigurace šifrování SSL* [online]. [cit. 2018-05-09]. Dostupné z: http://support.ricoh.com/bb_v1oi/pub_e/oi_view/0001035/0001035712/view/software/unv/0341.htm

[13] Kryptografie.wz.cz. *HASHOVACÍ FUNKCE* [online]. [cit. 2018-05-17]. Dostupné z: http://www.kryptografie.wz.cz/data/hash2.htm

[14] VÁŇA, Vladimír. *Počítačové sítě*. Praha: Střední průmyslová škola elektrotechnická, Ječná 30, Praha 2, s.2-9. 2010.

[15] Geo-info-mat. In: *Uspořádání sítě* [online]. [cit. 2018-05-09]. Dostupné z: http://www.geo-info-mat.cz/ict_internet_sit.php

[16] Site.the.cz. In: *Počítačové sítě - Topologie sítí - Hvězdicová topologie (strom)* [online]. [cit. 2018-05-09]. Dostupné z: http://site.the.cz/index.php?id=17

[17] Maturita z vyt. In: *POČÍTAČOVÁ KOMUNIKACE A SÍTĚ* [online]. [cit. 2018-05-09]. Dostupné z: http://maturita-vyt.buchtic.net/17.php

[18] VAVREČKOVÁ, Šárka. *Počítačová síť a internet* [online]. Filozoficko-přírodovědecká fakulta v Opavě, Slezská univerzita v Opavě, 2017 [cit. 2018-05-10]. s.18-27. ISBN 978-80-7510-245-4. Dostupné z: http://vavreckova.zam.slu.cz/pocsit.html

[19] Www.Samuraj-cz.com. *IP adresa - IP address* [online]. [cit. 2018-05-17]. Dostupné z: https://www.samuraj-cz.com/clanek/tcpip-adresy-masky-subnety-a-vypocty/

[20] Wikipedie. *Denial of service* [online]. [cit. 2018-05-17]. Dostupné z: https://cs.wikipedia.org/wiki/Denial_of_service

[21] Wikipedie. *Skenování portů* [online]. [cit. 2018-05-17]. Dostupné z: https://cs.wikipedia.org/wiki/Skenov%C3%A1n%C3%AD_port%C5%AF

[22] Home.czu.cz. *Firewall* [online]. [cit. 2018-05-17]. Dostupné z: http://home.zcu.cz/~afrouzov/

[23] Wikipedie. *Internet Key Exchange* [online]. [cit. 2018-05-17]. Dostupné z: https://en.wikipedia.org/wiki/Internet_Key_Exchange

[24] JAŠEK, Roman a David MALANÍK. *BEZPEČNOST INFORMAČNÍCH SYSTÉMŮ*. Zlín, 2013. s.20-32. ISBN 978-80-7454-312-8.

[25] Algoritmy.net. *Algoritmus RSA* [online]. [cit. 2018-05-17]. Dostupné z: https://www.algoritmy.net/article/4033/RSA

[26] EPO MACHINERY. In: *M503 – TESTER HLADINOVÝCH SENZORŮ AdBlue* [online]. [cit. 2018-05-09]. Dostupné z: http://www.epomachinery.cz/cs/stranka/jednoucelove-stroje

[27] SIEMENS. In: *Restricted Delivery Release for SCALANCE S602 V3 and S612 V3* [online]. [cit. 2018-05-09]. Dostupné z: https://support.industry.siemens.com/cs/document/63111939/restricted-delivery-release-for-scalance-s602-v3-and-s612-v3?dti=0&lc=en-WW

[28] SIEMENS. In: *Virtual private networks (VPN)* [online]. [cit. 2018-05-09]. Dostupné z: https://w3.siemens.com/topics/mea/en/industrial-security/products/pages/network-components.aspx

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

3DES 3 Data Encryption Standard, bloková šifra sloužící pro symetrické šifrování.

AES Advanced Encryption Standard, bloková šifra sloužící pro symetrické šifrování.

CM Comunication Module, komunikační rozšiřovací modul.

CPU Central Processing Unit, centrální procesorová jednotka provádějící strojové instrukce.

DES Data Encryption Standard, bloková šifra sloužící pro symetrické šifrování.

DHCP Dynamic Host Configuration Protokol, protokol se skupiny TCP/IP sloužící pro automatickou konfiguraci počítačů připojených do počítačové sítě.

DNS Domain Name System, systém doménových jmen realizován DNS servery.

FBD Function Block Diagram, jazyk funkčních bloků používaný pro programováni PLC.

FTP File Transfer Protocol, protokol pro přenos souborů v počítačové síti.

FTPS File Transfer Protocol Secure, zabezpečený protokol pro přenos souborů v počítačové síti.

GSD General Station Description, soubor popisující hardwarové nastavení zařízení.

HF Hashovací Funkce, hašovací funkce.

HMI Human Machine Interface, rozhraní mezi strojem a člověkem, vizualizace.

HTML HyperText Markup Language, programovací jazyk pro tvorbu webových stránek.

HTTP Hypertext Transfer Protocol, protokol určený pro výměnu hypertextových dokumentů ve formátu HTML.

HTTPS Hypertext Transfer Protocol Secure, zabezpečený HTTP protokol.

ICT Information and Communication Technologies, informační a komunikační technologie.

IDEA International Data Encryption Algorithm, bloková šifra sloužící pro symetrické šifrování.

IKE Internet Key Exchange, protokol sloužící při šifrování VPN.

IP Internet Protocol, protokol sloužící pro síťovou komunikaci.

LAD Ladder Diagram, jazyk kontaktních schémat používaný pro programováni PLC.

LAN Local Area Network, lokální počítačová síť (domácnosti, malé firmy).

MAC Media Access Control, jednoznačný identifikátor síťového zařízení.

MAN Metropolitan Area Network, rozlehlá počítačová síť (města).

NAPT Network Address and Port Translation, změna jednoho IP adresního prostoru a portu, do druhého.

NAT Network Address Translation, změna jednoho IP adresního prostoru, do druhého.

PAN Personal Area Network, osobní síť (mezi samotnými zařizeními).

PC Personal Computer, osobní počítač.

PDU Protocol Data Unit, data opatřená metadaty vztahující se ke konkrétnímu protokolu.

PLC Programmable Logic Controller, programovatelný logický automat.

SCL Structured Control Language, jazyk strukturovaného textu používaný pro programováni PLC.

SSL Secure Sockets Layer, protokol poskytující zabezpečení komunikace šifrováním a autentizací.

STL Statement List, jazyk mnemokódu, strojově orientovaný jazyk používaný pro programováni PLC.

TCP/IP Transmission Control Protocol/Internet Protocol, sada protokolů pro komunikaci v počítačové síti.

TIA Totally Integrated Automation, koncept plně integrovaného automatizačního prostředí.

VPN Virtual Private Network, virtuální privátní síť.

WAN Wide Area Network, rozsáhlá síť (okres, stát).

SEZNAM OBRÁZKŮ

SEZNAM PŘÍLOH

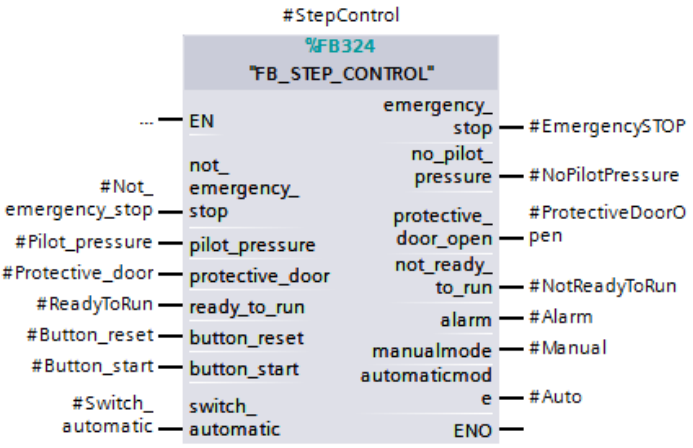
PŘÍLOHA 1: SEKVENCE

Block title: UKÁZKA SEKVENCE

Comment

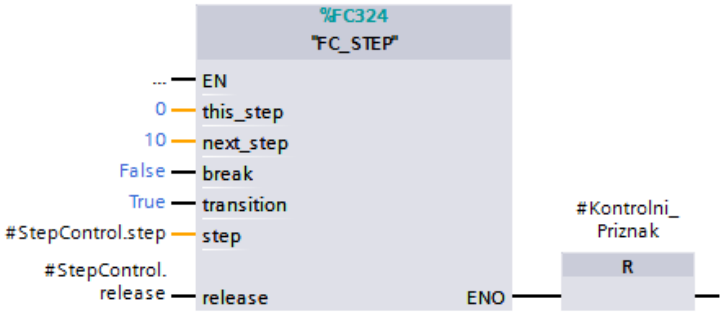
Network 1: STEP CONTROL

Comment



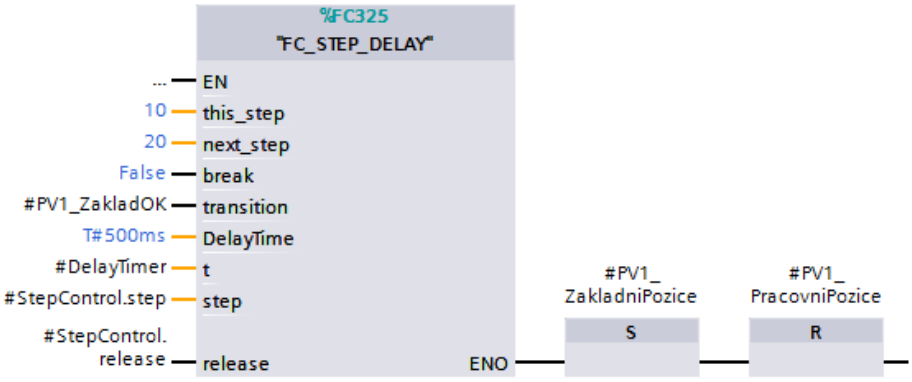
Network 2: STEP 0 - RESET

Comment



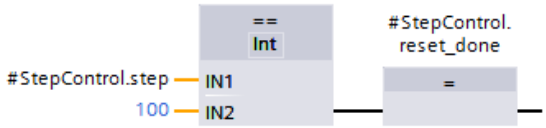
Network 3: STEP 10 - RESET

Comment



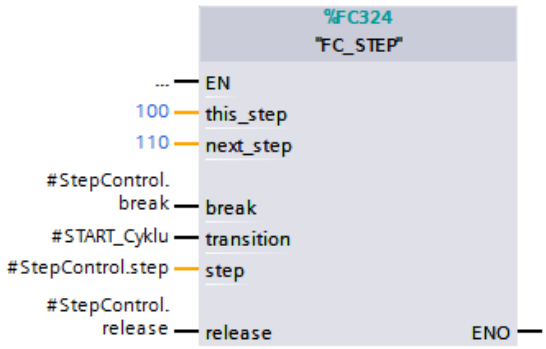
Network 4: STEP CONTROL - RESET DONE

Comment



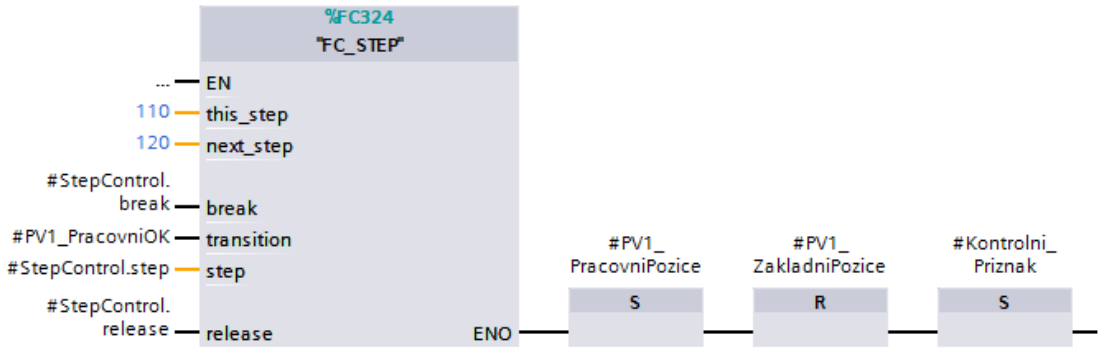
Network 5: STEP 100 - START CYKLU

Comment



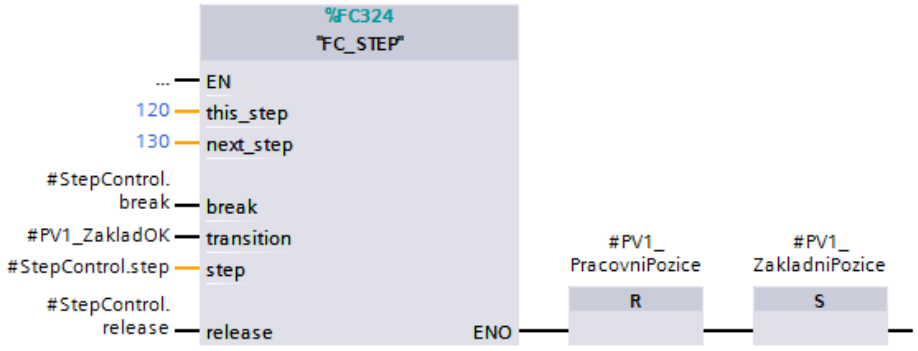
Network 6: STEP 110 - CYKLUS

Comment



Network 7: STEP 120 - CYKLUS

Comment



Network 8: STEP 130 - CYKLUS

Comment