

Návrh komunikačního rozhraní pro systém řízení výrobního toku v lakovně

Bc. Vojtěch Beran, DiS.

Diplomová práce
2014



Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

ZADÁNÍ DIPLOMOVÉ PRÁCE

(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení: **Bc. Vojtěch Beran, DiS.**
Osobní číslo: **A11474**
Studijní program: **N3902 Inženýrská informatika**
Studijní obor: **Informační technologie**
Forma studia: **kombinovaná**

Téma práce: **Návrh komunikačního rozhraní pro systém řízení výrobního toku v lakovně**
Téma anglicky: **Communication Interface Design for Paint Shop Product-Flow System**

Zásady pro vypracování:

1. **Popište funkci a účel jednotlivých řídicích prvků dopravníkové techniky v lakovně. Pro popis vnitřních i vnějších procesů použijte vhodný grafický modelovací jazyk.**
2. **Navrhněte vhodnou datovou strukturu pro řízení a výměnu dat.**
3. **Definujte požadavky na funkce systému nadřazeného řízení.**
4. **Navrhněte topologie toků dat na dostupné technologii.**
5. **Seznamte se s programovým vybavením, s možnostmi výměny dat pomocí dostupných komunikačních rozhraní a s integrovanými komunikačními funkcemi PLC Siemens SIMATIC S7-400.**
6. **V jazyku Step7 navrhněte a vytvořte komunikační rozhraní pro výměnu dat mezi PLC. Realizujte spojení mezi PLC.**
7. **Vytvořte prostředek pro demonstrační účely v systému Siemens SIMATIC WinCC.**

Rozsah diplomové práce:

Rozsah příloh:

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

Seznam odborné literatury:

1. BERGER, Von Hans. *Automatisieren mit STEP 7 in AWL: speicherprogrammierbare Steuerungen SIMATIC S7-300/400*. 2., wesentlich überarb. und erw. Aufl. Erlangen: Publicis-MCD-Verl, 1998. ISBN 38-957-8089-8.
2. MARTINÁSKOVÁ, Marie a Ladislav ŠMEJKAL. *Řízení programovatelnými automaty III: softwarové vybavení*. Vyd. 1. Praha: Vydavatelství ČVUT, 2003, 161 s. ISBN 80-010-2804-6.
3. ZEŽULKA, František. *Prostředky průmyslové automatizace*. 1. vyd. Brno: VUTUM, 2004, 176 s. ISBN 80-214-2610-1.
4. BERESFORD, Dillon. *Exploiting Siemens Simatic S7 PLCs*. In: *Black Hat USA 2011, Las Vegas [online]*. Las Vegas, 2011 [cit. 2014-01-16]. Dostupné z: https://media.blackhat.com/bh-us-11/Beresford/BH_US11_Beresford_S7_PLCs_WP.pdf
5. KABELOVÁ, Alena a Libor DOSTÁLEK. *Velký průvodce protokoly TCP/IP a systémem DNS*. 5., aktualiz. vyd. Brno: Computer Press, 2008, 488 s. ISBN 978-80-251-2236-5.
6. VLASÁK, Rudolf. *Základy projektování informačních systémů*. 1. vyd. Praha: Karolinum, 2003, 144 s. ISBN 80-246-0727-1.
7. FOWLER, Martin. *Destilované UML*. 1. vyd. Praha: Grada, 2009, 173 s. Knižovna programátora (Grada). ISBN 978-80-247-2062-3.

Vedoucí diplomové práce:

Ing. Radek Šilhavý, Ph.D.

Ústav počítačových a komunikačních systémů

Datum zadání diplomové práce:

25. července 2014

Termín odevzdání diplomové práce:

26. srpna 2014

Ve Zlíně dne 31. července 2014

doc. Mgr. Milan Adámek, Ph.D.
děkan



doc. Mgr. Roman Jašek, Ph.D.
ředitel ústavu

Prohlašuji, že

- beru na vědomí, že odevzdáním diplomové/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 diplomová/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 diplomovou/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 s předchozím písemným souhlasem Univerzity Tomáše Bati ve Zlíně, která je oprávněna v takovém případě ode mne požadovat přiměřený příspěvek na úhradu nákladů, které byly Univerzitou Tomáše Bati ve Zlíně na vytvoření díla vynaloženy (až do jejich skutečné výše);
- beru na vědomí, že pokud bylo k vypracování diplomové/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 diplomové/bakalářské práce využít ke komerčním účelům;
- beru na vědomí, že pokud je výstupem diplomové/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 diplomové práci pracoval samostatně a použitou literaturu jsem citoval. V případě publikace výsledků budu uveden jako spoluautor.
- Že odevzdaná verze diplomové/bakalářské práce a verze elektronická nahraná do IS/STAG jsou totožné.

Ve Zlíně

.....
podpis diplomanta

ABSTRAKT

Hlavním cílem diplomové práce je uvedení bezpečnostních a komunikačních problémů při použití PLC SIMATIC S7 společnosti Siemens. Tyto aspekty by měly být brány v potaz při nasazování a upgradování počítačových sítí v průmyslovém prostředí, kterou jsou tato zařízení hojně využívána. Také byla zvažena rizika používání starého TSAP protokolu. Ten byl navržen jako snadno implementovatelný, ale v době svého vzniku nebyly zvaženy hrozby zachycení paketů nebo dokonce cílených útoků.

Informace zde uvedené by měly sloužit technikům, kteří zřizují nová síťová spojení v továrnách, kde se PLC od společnosti Siemens používají.

Klíčová slova: PLC, SIMATIC, automatizace, STEP 7, WinCC, bezpečnost

ABSTRACT

The goal of this diploma work is the presentation of some security and communication issues of PLCs (programmable logical controllers) SIMATIC S7 by Siemens. These aspects should be taken into account by deploying or upgrading a computer network in an industrial environment where are these devices used. Risk of using an old TSAP protocol is also considered. It is designed as easy implementable, but at the time of its design, there were not considered threats of sniffing or even deliberate attacks.

The information mentioned here should serve technicians who are going to set up some new network connections with active network elements in production plants where PLCs by Siemens are used.

Keywords: PLC, SIMATIC, automation, STEP 7, WinCC, security

Děkuji panu Ing. Radku Šilhavému, Ph.D., za trpělivost, čas a metodické rady.

Děkuji panu Ing. Michalu Síthovi za poskytnutí zázemí pro studium.

Děkuji panu Štefanu Janíkovi za odborné konzultace a předání cenných zkušeností.

OBSAH

| | |
|--|-----------|
| ÚVOD | 9 |
| I TEORETICKÁ ČÁST | 10 |
| 1 PROGRAMOVATELNÉ ŘÍDICÍ JEDNOTKY | 11 |
| 1.1 STRUKTURA PROGRAMU PLC..... | 14 |
| 1.2 BĚH PROGRAMU PLC | 15 |
| 1.3 VÝVOJOVÉ PROSTŘEDÍ SIEMENS STEP7 | 16 |
| 2 POČÍTAČOVÉ SÍTĚ V PRŮMYSLVÉM PROSTŘEDÍ | 19 |
| 2.1 ETHERNET | 19 |
| 2.2 PRŮMYSLVÉ SÍTĚ A ETHERNET..... | 20 |
| 2.3 PROFINET..... | 22 |
| 3 BEZPEČNOST AUTOMATIZAČNÍCH SYSTÉMŮ | 23 |
| 3.1 SPOLEHLIVOST PŘENOSU DAT..... | 23 |
| 3.2 PROTOKOL ISO-TSAP | 25 |
| 3.3 BEZPEČNOSTNÍ SLABINY SYSTÉMU SIEMENS SIMATIC S7..... | 26 |
| 3.3.1 Odposlech sítě | 27 |
| 3.3.2 Replay Attack..... | 29 |
| 3.3.3 Server Session ID | 31 |
| 4 VIZUALIZAČNÍ SYSTÉMY SCADA | 32 |
| 4.1 SIEMENS SIMATIC WINCC | 33 |
| 5 PŘEHLED A VOLBA KOMUNIKAČNÍCH BLOKŮ | 34 |
| 5.1 PŘEHLED TYPŮ KOMUNIKAČNÍCH FUNKCÍ | 34 |
| 5.2 VOLBA VHODNÉHO GRAFICKÉHO VYJÁDŘENÍ..... | 36 |
| II PRAKTICKÁ ČÁST | 37 |
| 6 DEFINICE DATOVÝCH STRUKTUR | 38 |
| 6.1 POPIS DOPRAVNÍKOVÉ TECHNIKY | 38 |
| 6.2 TVORBA UŽIVATELSKÝCH DATOVÝCH TYPŮ (UDT)..... | 40 |
| 6.3 VOLBA JEDNOTNÉ DATOVÉ STRUKTURY | 41 |
| 7 INSTALACE A KONFIGURACE PROGRAMOVÉHO VYBAVENÍ | 43 |
| 7.1 SIEMENS SIMATIC STEP 7 PROFESSIONAL 2010 | 43 |
| 7.2 SIEMENS SIMATIC WINCC 6.0..... | 45 |
| 7.3 SIEMENS SIMATIC SOFTNET-S7 | 46 |
| 8 KONFIGURACE HARDWARE | 47 |
| 8.1 SÍŤOVÉ PROPOJENÍ..... | 47 |
| 9 PROGAM V JAZYKU STEP7 | 50 |
| 9.1 POPIS PROGRAMU | 50 |
| 9.2 NASAZENÍ PROGRAMU | 57 |
| 9.2.1 Konstanty, paměť a symbolické názvy | 57 |
| 9.2.2 Nastavení sítě | 60 |
| 9.3 SLEDOVÁNÍ A ANALÝZA DATOVÝCH PAKETŮ | 61 |

| | | |
|-----------|---|-----------|
| 10 | VIZUALIZACE DATOVÉHO SPOJENÍ VE WINCC..... | 64 |
| 10.1 | NOVÝ VIZUALIZAČNÍ PROJEKT | 64 |
| 10.2 | DEFINICE KOMUNIKAČNÍHO ROZHRANÍ A SPOJE | 65 |
| 10.3 | URČENÍ DATOVÝCH BODŮ | 68 |
| 10.4 | VIZUALIZAČNÍ SCHÉMA..... | 70 |
| 10.5 | UVEDENÍ DO PROVOZU | 71 |
| | ZÁVĚR | 72 |
| | SEZNAM POUŽITÉ LITERATURY..... | 73 |
| | SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK..... | 76 |
| | SEZNAM OBRÁZKŮ | 78 |
| | SEZNAM TABULEK..... | 80 |

ÚVOD

Cílem této diplomové práce je vytvořit funkční program v jazyku Step 7, který umožňuje výměnu dat mezi průmyslovými automaty Siemens SIMATIC S7. Výsledkem by mělo být především vytvoření postupu při výběru zvolených programových prostředků a objasnění chování zvoleného komunikačního procesu pomocí výpisu zdrojového kódu v nativních schématech FBD a LAD a znázornění procesu pomocí sekvenčního diagramu.

Měla by být nastíněna problematika volby komunikačních funkcí v závislosti na použitém hardware.

Po nastudování potřebných teoretických znalostí bude v prvním kroku provedena analýza vlastností dopravníkové techniky z hlediska datové reprezentace jednotlivých prvků v řídicím systému. Bude zhodnoceno, zda a jakou souvislost mají jednotlivé datové struktury z pohledu objemu dat. Existují-li kromě velikosti dat i další aspekty, se kterými je nutné počítat, bude cílem tyto problémy odhalit a stručně popsat.

Pokud bude shledáno, že existují skutečnosti, které naopak nemají na návrh komunikačního rozhraní větší vliv, budou tyto cíle také popsány.

Samostatnou kapitolou bude předložení některých bezpečnostních problémů PLC Siemens SIMATIC S7. Tyto aspekty by měly být zohledněny při návrhu, budování nebo modernizaci počítačové sítě v průmyslovém prostředí, kde se tato zařízení často používají.

Budou také zmíněna rizika používání některých komunikačních protokolů. Některé jsou navrženy jako lehce implementovatelné, ale v době svého vzniku se příliš neuvažovalo o hrozbách odposlechu nebo dokonce cíleného útoku. Bude uveden příklad útoku na základě zkušeností bezpečnostních expertů. Zmíním některé možné způsoby zneužití slabých míst radičů SIMATIC S7.

Pro základní vizualizaci vytvořeného komunikačního rozhraní bude použit vhodný nástroj SCADA.

Pro možnost detailní diagnostiky bude nastíněn postup, jak analyzovat datový provoz mezi dvěma PLC. Součástí práce by také měla být ukázka zachycení některých dat a popis jejich základní analýzy. V případě možnosti bude provedeno srovnání skutečně odeslaných dat a přijatých dat. Tato data by se měla shodovat s teoretickými předpoklady

I. TEORETICKÁ ČÁST

1 PROGRAMOVATELNÉ ŘÍDICÍ JEDNOTKY

PLC (anglicky Programmable Logic Controller), někdy též označovány jako SPS (německy Speicherprogrammierbare Steuerung) jsou řídicí jednotky, který jsou uzpůsobeny k řešení úloh typu logického řízení. Nahradily tak dřívější reléovou logiku. Užívají se dnes nejvíce pro regulace, monitorování a analogové měření. Jsou odpovědné za řízení procesů, jejichž existenci si člověk běžně ani neuvědomuje, přestože na nich často závisí důležité a kritické systémy, bez kterých by naše společnost měla zcela odlišnou kvalitu. I když to není vždy zřejmé, tato zařízení se používají v mnoha různých odvětvích. Modulární PLC se nacházejí v každém výrobním provozu, uvnitř elektráren, na ropných plošinách, v řídicích dopravních dispečincích (např. vlaková stanice). Technici se na tyto zařízení spoléhají, a protože jsou navrženy velmi robustně, předpokládá se u nich velká spolehlivost, odolnost, výkonnost a co nejvyšší maximální doba provozu (tzv. uptime).

PLC pomáhají automatizovat řadu úkolů, které zajišťují například řádný rozvod elektrické energie. U něčeho, co se zdá být tak zásadní a důležité pro náš způsob života, se zdá až nepředstavitelné, že by mohla být při vývoji PLC opomíjena bezpečnostní hlediska. Nejčastějším případem je absence bezpečnostních aktualizací zařízení, která nemusí být vždy jednoduchá. Je to ale jen otázka priorit provozovatelů. [1, s. 3]

Systémy PLC postupně nahradily centralizované systémy, které byly řízeny minipočítači. Nevýhodou systémů PLC byla nízká úroveň programátorského prostředí, mezi výhody se hned od počátku řadily spolehlivost, organizovanější struktura kabeláže a modularita. S tím souvisejí i další aspekty. Řídicí systémy umožnily zkrátit dobu instalace, oprav, údržby, snížit náklady na vývoj, kvalifikaci techniků a samotnou realizaci projektů.

Protože řídicí jednotky začaly postupně nahrazovat i průmyslové regulátory, bezkontaktní systémy a jiné zařízení, bylo nezbytné, aby se vyvinul vhodný programovací jazyk, který by obstál ve všech aplikacích průmyslové automatizace. Vyvinuly se tak jazyky podobné logickým schémátům (FBD, Functional Block Diagram; FUP, Funktionsplan), reléovým propojením (LAD, Ladder Diagram; KOP, Kontaktplan) a jazyku symbolických adres (STL, Statement List; AWL, Anweisungsliste). [2, s. 45]

Rozdíl mezi programovatelnou jednotkou a reléovým systémem je především v podstatě zapojení. V reléových systémech jsou obvody sestavovány pomocí propojování logických členů elektrickými vodiči, u PLC jsou jednotlivé funkční prvky navrhovány v podobě instrukcí programovacího jazyku. Spoje, kontakty a funkce jsou tedy naprogramovány.

Profesor Zezulka ve své publikaci Prostředky průmyslové automatizace uvádí srovnání výhod a nevýhod systémů PLC oproti systémům průmyslových PC (IPC):

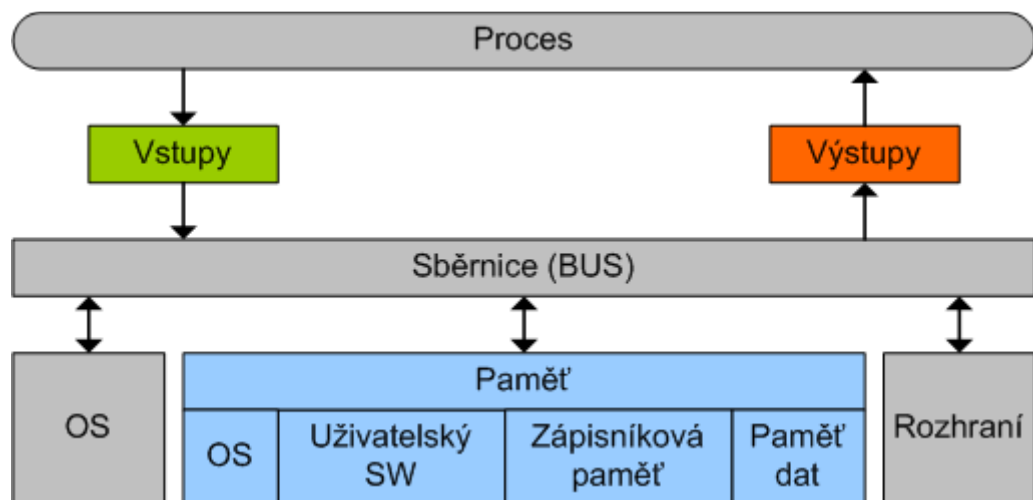
„A. Výhody:

- *Rychlé přeprogramování úlohy,*
- *malá varieta náhradních dílů,*
- *možnost vystavění velké hierarchické struktury dle potřeby,*
- *flexibilita (projektování na míru),*
- *modularita (možnost rozšíření),*
- *hospodárnost (levné velmi malé a malé kompaktní automaty),*
- *vestavěná diagnostika vlastního PLC,*
- *možnost tvorby diagnostiky vnější,*
- *jednoduché programování,*
- *možnost použití vyšších programovacích jazyků u nových automatů,*
- *jednoduchý a tím spolehlivý OS reálného času,*
- *velká nabídka kvalitních přístrojů různých výrobců.*

B. Nevýhody:

- *nižší programátorský komfort než u minipočítačů a IPC,*
- *vyšší cena než IPC ekvivalentního výkonu při nižším programátorském komfortu PLC,*
- *menší flexibilita ve srovnání s IPC,*
- *užití nedostatečně standardizovaných sériových komunikačních sběrnic pro propojení automatů do sítí,*
- *nezbytnost hierarchické architektury při propojování do větších celků.“ [2, s. 46]*

PLC se skládá zpravidla z CPU, systémové paměti a vstupních a výstupních rozhraní, pomocí kterých lze připojit řízený systém. Jedná se nejčastěji o výrobní zařízení, technologický proces nebo obsluhu výrobku. Další důležitou součástí jsou komunikační jednotky, které zajišťují spojení s nadřazenými a souřadnými systémy řízení. Propojení je označováno jako systémová sběrnice. [3, s. 3]



Obr. 1. Blokové schéma modulárního PLC

U starších PLC s bitově orientovanou architekturou (CPU, paměť dat) byly paměť dat a paměť programu odděleny. Dnešní PLC mají operační paměť společnou. V ní jsou vyhrazeny oblasti pro vstupní data, výstupní data, paměť pro program a vnitřní proměnné. Navíc jsou zde uloženy programové struktury, tzv. funkční bloky, uživatelské funkce a systémové funkce. Operační systém díky své jednoduchosti umožňuje režim reálného času. Základním způsobem zpracování úloh je tzv. cyklický režim. Kromě cyklického režimu je už i u malých PLC využíván systém přerušování, který je znám z mikropočítačů. Tento systém přerušování může být v uživatelském programu parametrizován. [2, s. 48]

Dále se budu zaměřovat výhradně na charakteristiku automatů Siemens SIMATIC S7. PLC Siemens SIMATIC S7 obsahuje operační paměť typu RAM, která je součástí CPU. Do operační paměti se ukládá programový kód i uživatelská data, která se po zapnutí napájecího napětí načítají z uživatelské paměti. Změny, které provádí uživatel pomocí vývojového software, probíhají pouze v operační paměti. Po restartu PLC se načítají původní uživatelská data. [4, s. 25]

Program zpracovává proměnné uložené v systémové oblasti. Tyto proměnné se dělí do skupin na vstupy (I), výstupy (Q), uživatelskou paměť (M), časovače (T), čítače (C) a lokální data (L). Vstupy a výstupy jsou obrazy skutečných hodnot fyzických digitálních vstupů a výstupů [4, s. 26]. Uživatelská paměť slouží k ukládání mezivýsledků [4, s. 27] a jsou obdobou globálních proměnných v programovacích jazycích.

1.1 Struktura programu PLC

Jednotlivé programy se skládají z jednotlivých modulů, které se nazývají bloky. Uživatelské bloky (OB, FB, FC a DB) obsahují sled instrukcí anebo pracují s daty. Tyto bloky lze volat cyklicky nebo pouze při volání některé speciální obsluhy.

Systemové bloky (SFB a SFC) jsou naprogramovány výrobcem PLC, jsou součástí operačního systému a v uživatelské paměti nezabírají žádné místo. Jsou předem otestované a jsou určeny pro řešení dílčích problémů jako je komunikace, kopírování dat a jiných standardních úloh. Jejich zdrojový kód není uživateli dostupný, ale jejich výhodou je vzájemná přenositelnost mezi systémy Siemens SIMATIC S7-300 a S7-400. SFC není nutné nahrávat do uživatelské datové oblasti.

Organizační bloky (OB) vytvářejí uživatelské rozhraní mezi operačním systémem a programem. Jsou rozčleněny do tzv. tříd priorit. Základním organizačním blokem je OB1, který je vyhledán a spuštěn za začátku každého cyklu činnosti PLC. Tento blok nelze spustit z uživatelského programu. Základní rozdělení je na časově řízené bloky a událostmi řízené bloky. Dalším důležitým blokem je OB100, který se spouští při restartu PLC, a používá se zejména pro inicializaci proměnných a parametrizaci programových struktur v projektu. Další bloky slouží k obsluze událostí nebo se spouštějí v případě výskytu nějaké chyby. Ne všechny OB jsou k dispozici ve všech CPU.

Funkční blok (FB) je modul, kterému je přiřazena oblast dat (DB), do které může ukládat své proměnné. Tato paměť je v PLC uložena v podobě datového bloku (DB), který je v tomto případě označován jako instanční datový blok. Údaje v tomto bloku se zachovávají do dalšího spuštění. Proměnné, které byly uloženy do zásobníku lokálních dat, se po ukončení zpracování bloku ztrácejí.

Funkce (FC) je logický modul podobný funkčnímu bloku, avšak nedisponuje vlastní instanční pamětí. Dočasné hodnoty proměnných se stejně jako u FB po zpracování bloku ztrácejí. Funkce po ukončení své činnosti vrací návratovou hodnotu do volacího bloku.

Datové bloky (DB), jak již bylo uvedeno, slouží k ukládání uživatelských dat, která lze v programu kdykoliv zapisovat a číst. Tyto bloky lze také pomocí PG zálohovat. Speciálním případem datového bloku je tzv. instanční datový blok, který je vždy svojí strukturou svázán s příslušným funkčním blokem. Pokud v programu voláme stejný funkční blok vícekrát, ale vždy se jeho volání vztahuje na jiný objekt, používáme vždy stejný FB, ale rozdílné DB. Tyto datové bloky se neliší velikostí ani strukturou, rozdílná jsou pouze v nich uložená data.

„K programování nabízejí PLC systémy specializované jazyky, původně navržené pro snadnou, názornou a účinnou realizaci logických funkcí. Jazyky systémů různých výrobců jsou podobné, nikoliv však stejné. Přímá přenositelnost programů mezi PLC různých výrobců není možná, daří se to obvykle jen mezi systémy téhož výrobce. Mezinárodní norma IEC 61131 se snaží jazyky a zvyklosti různých výrobců PLC alespoň co nejvíce sblížit. Ustálily se i třídy jazyků pro programování PLC.“ [3, s. 46]

Mezinárodní norma IEC 61131 byla převzata členskými státy EU jako harmonizovaná evropská norma EN 61131, a stala se tak i součástí českých technických norem pod označením ČSN EN 61131. ČSN EN 61131-3 ed. 2 z října 2013 specifikuje syntaxi a sémantiku jazyků, které jsou navrženy pro programování řídicích jednotek PLC [5]. Zaměřuje se zejména tyto problémy: Architektura, komunikace, programování, datové typy, proměnné, datové bloky, textové jazyky (Instruction List IL a Structured Text ST) a grafické programovací jazyky (Ladder Diagram LD a Function Block Diagram FBD).

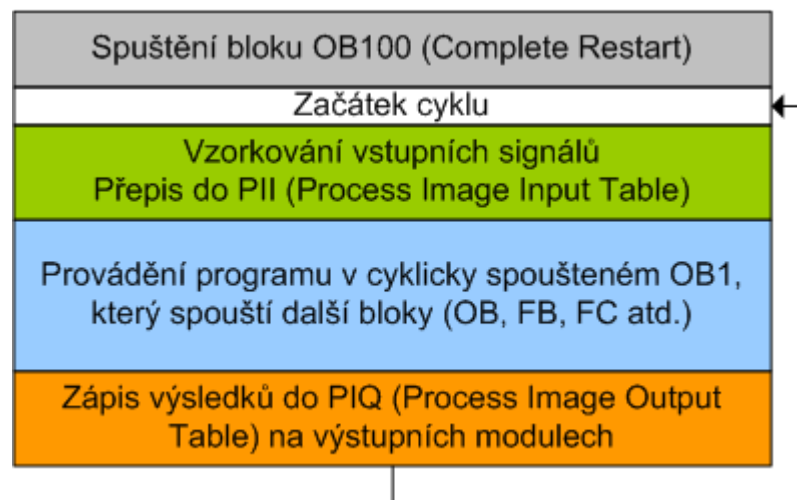
1.2 Běh programu PLC

Pokud je program přeložen (zkompilován) a uložen do paměti PLC, procesor pak cyklicky zpracovává programovou smyčku pomocí funkce OB1 (Obr. 3). [2, s. 53]

V okamžiku zapnutí nebo přepnutí z režimu STOP do režimu RUN (nebo RUN-P), dojde k události nazvané Complete Restrat (kompletní restart), která je obsluhována organizačním blokem OB100. PLC vynuluje paměť, čítače, časovače a zásobníkovou paměť.

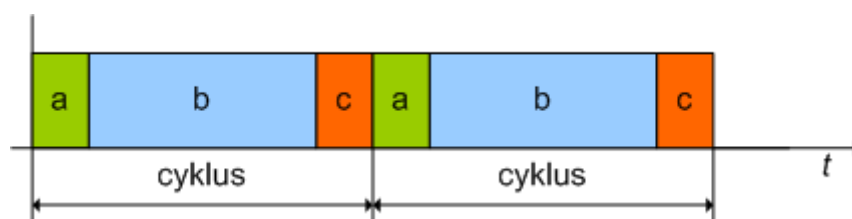
Cyklický program probíhá tak, že CPU vzorkuje stavy signálů na vstupu a aktualizuje jejich obraz ve vstupních vyrovnávacích pamětech PPI (Process Image Input Table). Dále je prováděn program voláním nadřazeného organizačního bloku OB1. Nakonec CPU zaznamená obrazy hodnot ve výstupních vyrovnávacích pamětech PIQ (Process Image Input Table) do výstupních zařízení.

Jedna programová smyčka se nazývá cyklus. Délka tohoto cyklu se pohybuje řádově v desítkách milisekund. Jedná se o velmi důležitou hodnotu pro určování rychlosti PLC, ale také pro vyhodnocování efektivity programu či analýzu rychlosti zpracování událostí.



Obr. 2. Programová smyčka PLC

Na obrázku (Obr. 3) je znázorněn časový diagram běhu PLC. Nejdříve (a) dochází ke vzorkování vstupních dat automatu (např. z periferií) a zápisu do vstupních pamětí PLC. Poté dochází ke zpracování programu (b), při kterém vždy dochází i k zápisu do vnitřních pamětí. Nakonec (c) nastane uvolnění výstupních pamětí a aktivace výstupů automatu.



Obr. 3. Časový diagram základní funkce PLC

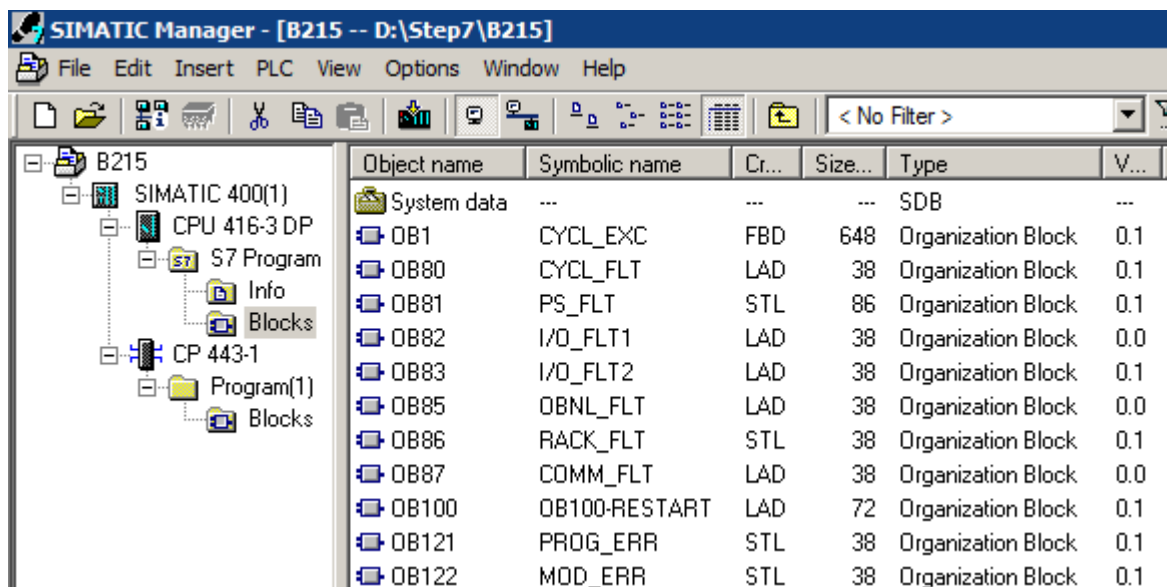
1.3 Vývojové prostředí Siemens Step7

Vývojové prostředí Step7 je určeno pro návrh, ladění a programování softwaru PLC Siemens SIMATIC S7. Prostředí podporuje výše uvedenou normu IEC 61131-3 a v rámci jednoho projektu je možné přepínat mezi jednotlivými programovými schématy. Je také možné provádět diagnostiku a konfiguraci hardwaru. Symbol Editor je určen k definování globálních proměnných. NetPro je nástroj pro konfiguraci síťových rozhraní a definování síťových rozhraní PLC systémů. Hardware Configuration definuje konfiguraci jednotlivých hardwarových komponent, které lze sestavovat na základě katalogu dostupných pro-

duktů. Hardwarová diagnostika sleduje aktuální stav PLC či jednotlivá poruchová hlášení. Program Simatic Manager tyto všechny nástroje zastřešuje a lze je odtud spustit. [6, s. 144]

Ke konfiguraci, návrhu a programování PLC řady SIMATIC S7 se používá vývojový software SIMATIC STEP 7, který umožňuje uživateli navrhovat a spravovat tyto oblasti:

- Hardwarová konfigurace modulárního systému Simatic S7,
- komunikace (např. Profibus, Profinet, Industrial Ethernet aj.),
- programování řídicího programu v podobě LAD, FBD nebo STL
- a diagnostika a testování (on-line sledování, diagnostické nástroje).



Obr. 4. SIMATIC Manager STEP 7

Program je možné zapisovat v jakémkoliv ze tří nabízených schémat, která vycházejí z mezinárodní normy IEC 61131-3.

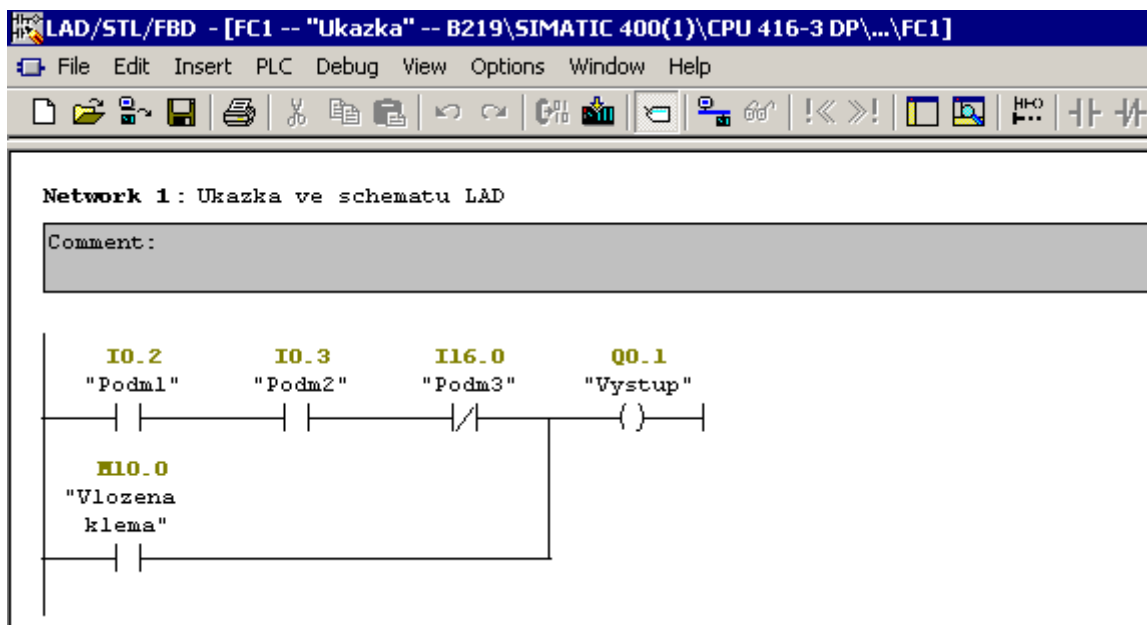
LAD (Ladder Diagram) je grafické programovací schéma, které je založeno na pomyslném elektrickém obvodu sestaveném ze vzájemně propojených relé. Tento typ zápisu je nejprůhlednější, proto se také nejvíce užívá.

Dalšími schématy jsou FBD (Functional Block Diagram), který je složen z logických hradel, a STL (Statement List), což je příkazové schéma, které nápadně připomíná jazyk symbolických adres. STL má oproti předchozím dvěma schématům neomezené možnosti programování v rámci daného PLC.

Ve všech třech schématech lze přepnout zobrazení do on-line režimu, kde je možné sledovat aktuální hodnoty proměnných a průběhy signálů na jednotlivých pomyslných vodičích (FBD a LAD), což je velmi užitečné při diagnostice a ladění programu.

STEP 7 TIA Portal podporuje širokou škálu produktů řady SIMATIC, jmenovitě S7-300, S7-400 a S7-1200. V praxi se ještě hojně používá starší vývojové prostředí STEP 7, protože některé projekty nelze jednoduše převést do nové verze. Problém často nastává v interpretaci datových typů (například záměna datových typů WORD a INT).

Většinu diagramů FBD a LAD lze mezi sebou interaktivně přepínat, ale pokud dané schéma neumožňuje zobrazení některého prvku, zobrazí se programový kód kombinovaně ve formě STL. Kód STL lze jen velmi výjimečně převést do FBD či LAD.



Obr. 5. STEP 7: LAD/STL/FBD editor

2 POČÍTAČOVÉ SÍTĚ V PRŮMYSLOVÉM PROSTŘEDÍ

V posledních letech došlo k velkému rozvoji komunikačních rozhraní pro řídicí jednotky. Staré kompaktní systémy byly nahrazeny modulárními, které ke komunikaci využívají volitelné síťové rozhraní odpovídající běžným síťovým standardům, např. IEEE 802.3 Ethernet a IEEE 802.11 Wi-Fi. Nové komunikační protokoly podporují vyšší přenosové rychlosti a zlepšené zpracování signálů. V současnosti nejvíce nasazovanou síťovou technologií je PROFINET, kterou PLC Siemens SIAMTIC S7 také podporují.

2.1 Ethernet

Ethernet je síťová komunikační sběrnice vyvinutá společnostmi Xerox, Intel a DEL, později byl standardizován pod označením IEEE 802.3 Ethernet (též ISO 8802-3). Definiuje fyzickou a linkovou vrstvu. Důležité jsou zejména podvrstvy MAC (Medium Access Control), která popisuje metody přístupu k přenosovému médiumu, a LLC (Logical Link Control), která řídí logický spoj. Původní protokol označovaný jako Ethernet II se od IEEE 802.3 liší zejména v položce Length/Type [7, s. 111].

Tab. 1. Struktura rámce protokolu IEEE 802.3-2012

| Velikost | Název pole | Popis |
|-------------------|---------------|--|
| 7 B | Preamble | 7 bajtů rovných hodnotě 10101010_2 , 55_{16} |
| 1 B | SFD | Start Frame Delimiter; 10101011_2 , $D5_{16}$ |
| 6 B | Destination | MAC adresa adresáta |
| 6 B | Source | MAC adresa zdroje |
| 4 B | IEEE 802.1Q | VLAN tag, volitelný |
| 2 B | Length | Délka (u Ethernet II typ protokolu) |
| 46(42)– 1500 B | Payload | Data |
| 4 B | CRC | kontrolní součet |

Dvoubajtové pole Payload/Length, v tabulce (Tab. 1) je vyznačeno tučně, způsobuje největší rozdíl mezi protokoly Ethernet II a IEEE 802.3. Rámec protokolu IEEE 802.3 neobsahuje identifikaci protokolu, ale k záměně nemůže dojít, protože specifikace protokolů

Ethernet II jsou vyjádřeny čísly vyššími než 1500. K takové maximální délce nemůže dojít. Sítě tak mohou spolu bez problémů koexistovat [8, s. 15].

Ačkoliv původní Ethernet II popisuje pouze variantu s přenosovou rychlostí 10 Mb/s, fyzická vrstva Ethernetu (IEEE 802.3) zahrnuje realizace spojení pomocí koaxiálních kabelů, kroucených dvojlinek a optických médií od rychlosti 10 Mb/s až po 100 Gb/st. Mezi nejčastější používané jsou 10BASE-T, 100BASE-TX (Fast Ethernet) a 1000BASE-T (Gigabit Ethernet). V případě kroucených dvojlinek jsou nejčastěji využívány modulární konektory 8P8C. Pro ty jsou nejběžnější rychlosti 10 Mb/s, 100 Mb/s a 1 Gb/s. Sítě realizované pomocí optického vlákna využívají rychlosti 100 Mb/s a 1 Gb/s.

2.2 Průmyslové sítě a Ethernet

Profesor Zezulka je skeptický k myšlence, že by mělo v nejbližších letech dojít k vytlačení průmyslových sítí Ethernetem. Uvádí několik výhod, ve kterých má Ethernet oproti zavedeným průmyslovým sítím navrch:

- „Dlouhodobě otevřené technologie (Ethernet, TCP/IP, http, ftp),
- kompatibilita s dalšími lokálními sítěmi (LAN) a s Intranetem a Internetem,
- vyšší přenosová rychlost ve srovnání s průmyslovými sítěmi (Profibus, Device Net),
- při použití přepínaného Ethernetu možnost duplexního režimu, de facto zdvojnásobení přenosové rychlosti,
- jednoduché a levné připojení na PC, Internet/Intranet,
- masová výroba síťových komponent se odráží v nízké ceně,
- vývojoví pracovníci většinou mají s technologií TCP/IP již značné zkušenosti.

Mezi nevýhody Ethernetu ve srovnání s průmyslovými sítěmi je možné uvést:

- Nedeterministický přístup k médiu. To je způsobeno použitím přístupové metody CSMA/CD. Pokud zařízení při přístupu na sběrnici detekuje kolizi, čeká náhodný časový interval, než se pokusí o přístup znovu.
- Délka datového pole není přizpůsobena potřebám průmyslové komunikace.

- *Použití aktivních prvků (swithe, routery, ...) v síťové technologii. Oproti jiným sítím využívajícím pasivní sběrnice je toto řešení dražší a z principu náchylnější na poruchu.*
- *Neukončený vývoj (protokolů) a tím další náklady na vývoj.*
- *Nutnost vyvinout průmyslové verze konektorů, kabelů a dalších síťových prvků. Je nutné mít k dispozici prvky vhodné pro vyšší rozsahy teplot, větší úrovně rušení a zajišťující vysokou spolehlivost provozu (redundance).*
- *Není vhodný pro připojení jednoduchých (levných) sensorů a aktorů. Cena připojení jednoho čidla k Ethernutu je v současné době vysoká v porovnání s jinými sběrnici. Také se ještě nevyrábějí dostatečně integrované prvky umožňující splnit prostorové omezení.“ [2, s. 124]*

V případě informačních technologií, kde nejsou kladeny vysoké nároky na správné načasování přenosu dat, přístupové metody CSMA/CD postačují. V průmyslovém prostředí je však kladen důraz na deterministické řízení přenosu dat, což služby sítě Ethernet neposkytují. Zařízení, která vyžadují přesné načasování toku dat, např. kvůli vzorkování, nemohou v takových sítích fungovat spolehlivě. Kde se nachází mnoho účastníků a dochází také k častým kolizím.

Řešením může být rozdělení sítě do menších segmentů (kolizních domén), kde lze očekávat menší pravděpodobnost vzniku kolize. Pravděpodobnost kolize se zvyšuje při zvyšujícím se počtu účastníků a při velkém objemu přenášených dat. Většinu těchto problémů tedy vyřeší síťový přepínač, který směřuje pakety jen do určitých částí sítě.

Při nízkém objemu dat se může spolehlivostí sítě Ethernet (100 Mb/s) blížit systémům pracujícím v reálném čase. [2, s. 124]

Ethernet vychází z normy IEEE 802.3, která definuje fyzickou a linkovou vrstvu referenčního modelu ISO/OSI. Tyto vrstvy neposkytují jistotu doručení dat adresátovi. Pro tyto účely jsou definovány další síťové vrstvy. V současnosti bezesporu nejpoužívanější rodinou protokolů je TCP/IP. Protokol IP (Internet Protocol) tvoří síťovou vrstvu modelu ISO/OSI a TCP (Transmission Control Protocol) zajišťuje doručování zpráv na úrovni transportní vrstvy. Nad těmito vrstvami je aplikační vrstva, která je tvořena rozličnou škálou služeb.

2.3 PROFINET

Jedná se o otevřený transparentní standard sjednocující standardní průmyslové sběrnice Profibus a Ethernet TCP/IP. Vývoj řídí organizace PROFIBUS International. Standard PROFINET byl navržen tak, aby vytvořil skutečně otevřené a dostupné propojovací prostředí mezi prvky průmyslové automatizace přes společné síťové standardy a protokoly. Myšlenkou bylo usnadnit jedné osobě nebo malému týmu správu stovek nebo tisíců zařízení PLC rozmístěných po celém výrobním podniku.

Možnost spravovat zařízení připojených do více sítí z jednoho místa je velmi výhodné, levné a efektivní. PROFINET nyní podporuje technologie Ethernet, Industrial Ethernet (dříve používaný protokol SINEC H1), HART, ISA 100 a Wi-Fi. Také podporuje standardní sběrnice starších zařízení (PLC-5 a SLC-500 – Allen-Bradley, Ge Fanuc Series 90, Mitsubishi PLC Series A/Q), což odstraňuje nutnost nahradit stávající systémy, a tím přispívá k dalšímu snížení nákladů na zavedení. [2, s. 128]

PROFINET v současnosti zahrnuje tyto protokoly:

- TCP/IP s reakční dobou řádově 100 ms,
- RT (Real-Time) protokol s maximální dobou cyklu 10 ms,
- IRT (Isochronous Real-Time) pro řízení pohonů s cyklem menším než 1 ms.

Celkový počet instalovaných zařízení PROFINET se na konci roku 2013 odhadoval celosvětově odhadoval na 7,6 milionů zařízení, i když přesný počet není znám. O prudkém růstu počtu instalací svědčí odhady z předcházejících let, kdy na konci roku 2012 se tento počet odhadoval na 5,8 milionů a na konci roku 2011 na 4,3 milionů. Značný počet těchto zařízení jsou systémy Siemens SIMATIC S7 PLC. [9]

Specifikace, podrobné popisy, případy užití, možnosti implementace a jiné informace lze nalézt na internetové adrese <http://www.profibus.com/technology/profinet/>.

PROFINET je mnoha odborníky považován za nejspolehlivější sběrníkový standard současnosti [1, s. 4].

3 BEZPEČNOST AUTOMATIZAČNÍCH SYSTÉMŮ

V této kapitole popíšu některé problémy, se kterými je možné setkat při posuzování bezpečnosti počítačových sítí v průmyslovém prostředí. Síťové protokoly byly vždy navrhovány jako jednoduché, snadno implementovatelné, s minimální režii. V době návrhu nebyly bezpečnostní aspekty brány v potaz. Bezpečnost služeb v sítích může být chápána samostatně jako souhrn několika dílčích problémů.

Prvním je zamezení před únikem informací: V případě odposlechu by měl útočník získat nečitelná data. Tento typ bezpečnosti je nazýván jako důvěrnost a utajení dat. Dalším problémem je ověření totožnost komunikujících stran. Autentizací se v této práci nebudu zabývat. Třetí složka bezpečnosti se nazývá integrita. Pokud zpráva vyslaná informačním kanálem zůstane neporušená a v okamžiku doručení je identická se zprávou odeslanou, zachovala si svoji integritu [10, s. 487]. Minimalizací počtu zranitelných míst sítě se její bezpečnost zvyšuje.

3.1 Spolehlivost přenosu dat

Komunikační procesory Siemens SIMATIC CP x43-1 pro průmyslový Ethernet umožňují volbu z několika komunikačních režimů. Správná volba režimu má zásadní vliv na spolehlivost přenosu dat.

Procesory disponují funkcemi autonegotiation a autosensing, které zajišťují automatickou identifikaci přenosové rychlosti, zpravidla 10 Mb/s či 100 Mb/s, a volbu provozního režimu (full-duplex, half-duplex).

Oba duplexní režimy jsou určeny pro obousměrnou komunikaci. Full-duplex umožňuje oběma uživatelům vysílat nezávisle na sobě, half-duplex umožňuje pouze jeden transport v daný časový okamžik, a to pouze jedním směrem, přenos dat mezi dvěma účastníky tedy musí probíhat střídavě.

Výše uvedené mechanismy (autonegotiation a autosensing) se používají pro automatické určení nejefektivnějšího provozního režimu mezi dvěma komunikačními partnery. Výrobce doporučuje využívat vždy ten nejpokročilejší mód, který je k dispozici. [11]

Tab. 2. CP-x43-1: Přehled dostupných komunikačních režimů

| Přenosová rychlost | Režim komunikace |
|------------------------|------------------|
| 10 Mb·s ⁻¹ | half-duplex |
| 10 Mb·s ⁻¹ | full-duplex |
| 100 Mb·s ⁻¹ | half-duplex |
| 100 Mb·s ⁻¹ | full-duplex |

Od srpna 2001 byl výrobcem stanoven jednotný algoritmus funkce autonegotiation (tzv. verze 2). Do té doby platil algoritmus verze 1:

Po zapnutí komunikačního procesoru se provede automatická konfigurace. Pokud je to možné, aktivuje se nejvyšší možný provozní režim, tedy 100 Mb/s full-duplex, v ostatních případech se CP modul přepne do režimu autoswitching, tedy do režimu 10 Mb/s half-duplex. Pokud není po zapnutí k dispozici žádný komunikační partner, výchozí nastavení zůstane aktivní a v případě, že partner odpoví později, bude zprvu vytvořen link 10 Mb/s a až poté funkce autonegotiation zahájí vyhledávání optimálnějšího spojení, protože komunikační partneři mohou podporovat kvalitnější typ spojení než 10 Mb/s.

Pokud komunikační partner podporuje pouze link 100 Mb/s full-duplex (může to být například optický media konvertor), je nutné brát v potaz následující dvě situace: V případě, že jsou při zapnutí CP oba komunikační partneři propojeni, dojde ke spojení v režimu 100 Mb/s full-duplex, a při následném autonegotiation dojde k potvrzení tohoto režimu. Je-li však rychlejší zařízení (100 Mb/s) připojeno později, komunikační procesor je již v režimu autoswitching. To má za následek neúspěšné spojení, protože optický media konvertor nepodporuje režim 10 Mb/s. V tomto případě nebude spojení nikdy navázáno. Dotčené komunikační procesory jsou zejména CP 343-1 do verze v1.0.3 a CP 443-1 do verze v1.1.0. [11, tabulka 3].

Jak již bylo uvedeno, od roku 2001 byla zavedena úprava, která způsobuje cyklické přepínání režimů mezi autoswitching a autonegotiation (a to vždy po startu a při ztrátě linku). Tímto způsobem je zajištěno spojení komunikačních partnerů za každých okolností. Činnost této funkce lze detekovat pomalým blikáním kontrolky FAST. Protože v tomto případě nelze předem určit režim navázaného linku, okamžiku detekce spojení dojde ještě jednou k aktivaci funkce autonegotiation, aby byla zajištěna co nejvyšší rychlost spojení.

Pokud bude přednastaven režim 100 Mb/s full-duplex, může docházet ke sporadické ztrátě telegramů. Tento problém se týká pouze případů, kdy dochází k vysoké zátěži CP, například při zpracování větších objemů dat. Je ovšem také nutné zmínit, že se tento problém týká i těch CP, které mají nastaveny velký počet partnerských stanic. Tento problém se týká především komunikačních procesorů CP 443-1 do verze v1.1.0. [11, tabulka 4].

Problém se projevuje se v občasných výpadcích komunikace. Při ztrátě telegramu totiž partnerská stanice čeká na potvrzovací telegram, který nedorazí. Asi za 1 s stanice opakuje zaslání posledního telegramu a komunikace pokračuje dál. Z tohoto důvodu dochází ke snižování výkonu komunikačního kanálu. Spojení se ani neukončí a ani nedojde k žádné ztrátě telegramu, protože transportní vrstva zajistí opakování telegramů.

Aby nedocházelo k výpadkům komunikace, výrobce doporučuje na síťových prvcích nastavit jiný režim než 100 Mb/s full-duplex, což způsobí, že nedojde k automatické konfiguraci. Toto chování se nevztahuje na novější verze firmware komunikačních procesorů, kde v žádném z provozních režimů nedochází ke ztrátám dat. [11]

3.2 Protokol ISO-TSAP

Tento protokol byl navržen v roce 1986 (RFC 983), o rok později upraven (RFC 1006) a v roce 1997 aktualizován (RFC 2126), jako snaha poskytnout rozhraní pro transportní vrstvu mezi referenčním modelem ISO/OSI a velmi se rozmáhajícím protokolem TCP, který vznikl v tehdejší komunitě vývojářů prostředí ARPA/Internet. Od TCP se v zásadních aspektech liší pouze tím, že TCP spravuje nepřetržitý proud dat bez ohraničení. Při přenosu pomocí TCP se pakety po doručení sestavují tak, aby vznikl souvislý blok dat, ale standardní OSI/ISO Layer 4 definuje hranici mezi pakety, což je hlavním rozdílem mezi těmito protokoly. Protože je nutné znát délku platných dat, norma ISO-TSAP přidává do každého balíčku 4 bajty, tak, aby aplikace mohly ohraničení datového bloku rozpoznat. Hlavní rozdílem mezi ISO-TSAP a TCP je přidání záhlaví do každého balíčku (Tab. 3).

Další odlišností je existence portu relace, tzv. TSAP ID. Jedná se o obdobu TCP portu, ale seznam vyhrazených ISO TSAP ID nebyl nikdy jasně publikován. V prostoru komunikace pomocí TCP je protokolu TSAP vyhrazen jeden port 102.

Tab. 3. ISO-TSAP: Struktura hlavičky paketu

| Bajt | Bit | Název pole | Popis |
|-------|----------|---------------|--|
| 0 | 0 až 7 | vrsn | všechny bity jsou jedničky |
| 1 | 8 až 15 | reserved | vyhrazené pole, není použito |
| 2 a 3 | 16 až 31 | packet length | délka paketu (minimum 8, maximum 65535) |
| od 4 | od 32 | TPDU | transport protocol data units (tj. data) |

ISO TSAP má symetrické chování, tj. nejedná se explicitně o model klient-server. Namísto TCP serveru, který naslouchá na známém portu, transportní služba protokolu TSAP vytváří indikaci událostí, které nastávají u jednotlivých účastníků, kteří jsou ve výchozím stavu v klidovém režimu, dokud se nevytvoří požadavek na vysílání nebo příjem dat.

Tento protokol je díky snadnosti jeho implementace používán v průmyslových řídicích systémech Siemens (PLC, SCADA) již mnoho let, a možná právě kvůli snadnosti implementace a možnosti zpětné kompatibility průmyslových zařízení nebyl nikdy přehodnocen důraz na bezpečnost. Za posledních 20 let doznaly koncepty kybernetické bezpečnosti radikální změn, avšak komunikační standardy nebyly nijak zásadně dotčeny. [1]

3.3 Bezpečnostní slabiny systému Siemens SIMATIC S7

Dne 8. července 2011 uvedl na konferenci Black Hat USA+2011 v Las Vegas bezpečnostní technik společnosti NSS Labs Dillon Beresford přednášku, ve které bylo popsáno několik bezpečnostních slabin PLC systému Siemens SIMATIC S7. Sám přednášející uvedl, že všechny jím odhalené slabiny již dříve zaslal společnosti Siemens AG. [1]

O nedostatečné bezpečnosti PLC se dlouhou dobu nehovořilo, dokud nezaútočil počítačový červ Stuxnet. Od té doby se o kyberkriminalitě v průmyslovém prostředí hovoří více, avšak chybí představa, jakými prostředky je tato ilegální činnost provozována, a která zařízení jsou cílem těchto útoků. Až analýza chování červu Stuxnet ukázala na nesmírnou obšířlost tohoto problému. [1]

Spolu s nasazením řídicích systémů, kde je kladen důraz na kontinuitu vývoje a zpětnou kompatibilitu, roste riziko použití zastaralých komunikačních protokolů, které byly navrženy pro snadnou implementaci a spolehlivý přenos dat. V době svého vzniku nebylo bráno v potaz riziko jejich napadení. K těmto protokolům patří například protokol ISO-TSAP

(TCP port 102), který byl poprvé navržen v roce 1986. V minulosti byly požadavky na průmyslové komunikační systémy pouze funkčnost, výkon a spolehlivost. Také dnes, při nasazení či modernizaci průmyslových komunikačních technologií, není obvyklé, aby zákazník požadoval v první řadě zabezpečení systému proti hrozbě útoku.

V oblasti průmyslových řídicích systémů je nedostatek síťových komunikačních protokolů, které by byly schopny zajistit bezpečnou komunikaci. Řešení existují, ale například na jiných síťových vrstvách. Ne vždy jsou však tyto možnosti využity.

Každý návrhář počítačové sítě by měl otázkám bezpečnosti věnovat náležitou pozornost i v případě, kdy nebyl na straně zadavatele projektu požadavek na vysoké zabezpečení.

Také se může zdát, že by mělo být snadné izolovat síť fyzicky tak, že by se k ní neměl nikdo přistup. Takováto vize je ale v mnoha případech zcela nerealizovatelná. A pokud existují organizované skupiny útočníků, vždy najdou prostředky (např. sociální inženýrství), jak se k dané síti dostat.

Průmyslové komunikační systémy jsou v dnešní době naprosto nezbytné. Je velmi frustrující, že někteří výrobci jsou schopni bagatelizovat vážné bezpečnostní slabiny svých systémů. Měli by se poučit a věnovat bezpečnosti svých zařízení více úsilí. V mnoha případech totiž může jít i o lidské životy.

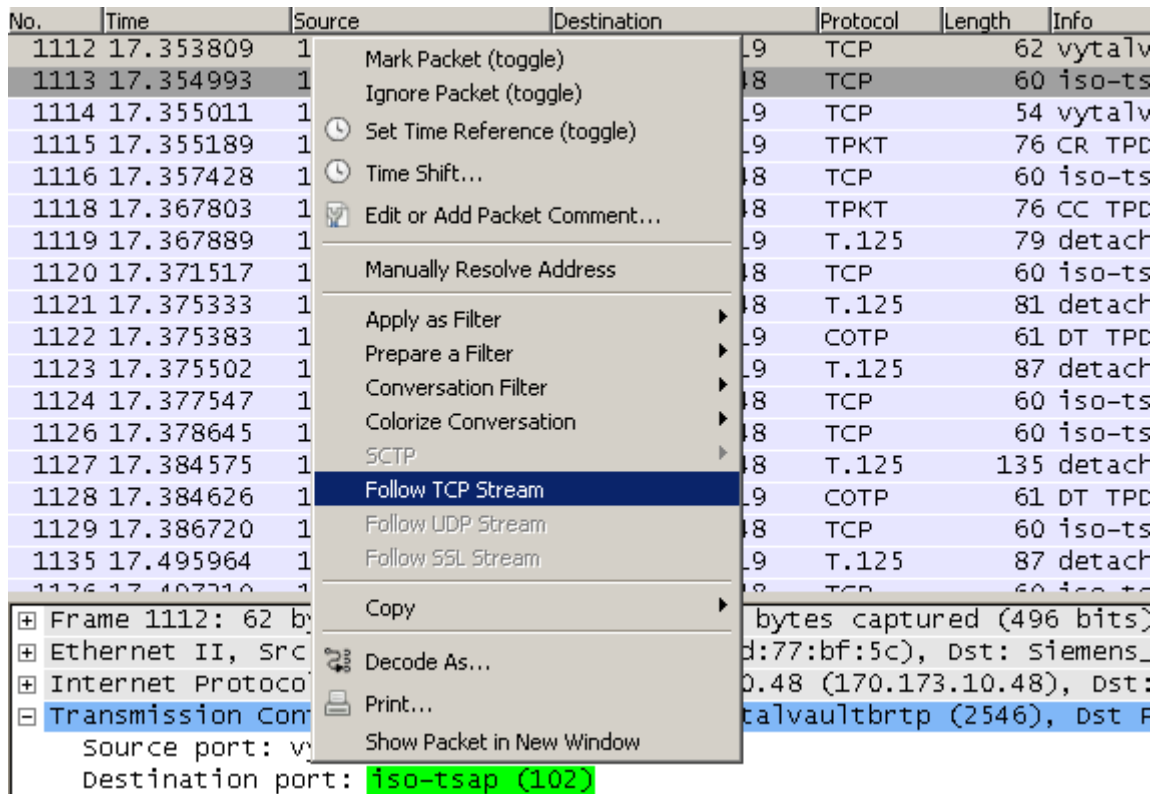
3.3.1 Odposlech sítě

Komunikaci mezi STEP 7 TIA Portal (STEP 7) a PLC zajišťuje TCP protokol ISO-TSAP, který se standardně užívá pro programování všech S7 programovatelných automatů Siemens. Tento protokol používají i jiní výrobci, např. Rockwell (Allen-Bradley), Honeywell, ABB nebo GE (Fanuc).

Základy protokolu TSAP byly ustanoveny na základě dokumentů RFC 793 a RFC 791. Tento protokol umožňuje v čitelné podobě zaznamenávat pakety jdoucí do a z inženýrské pracovní stanice (PC) do řídicí jednotky (PLC), a dělá z PLC řady SIMATIC S7 cíl pro útočníky, kteří mohou snadnou změnou obsahu paketů podvrhnout komunikaci. Je k tomu potřeba pouze vývojový software STEP 7 a software pro odposlech síťové komunikace.

Pro zachycení klientských ISO-TSAP paketů se musí nejdříve zajistit přístup k TCP komunikaci. Na nepřepínané síti se lze připojit ke kterémukoliv zařízení a odposlouchávat veškerý provoz na síti. K tomu je potřeba přepnout síťové zařízení do tzv. promiskuitního

režimu (promiscuous mode). Většina programů pro odchyťávání paketů touto funkcí disponuje. [12, s. 264]



Obr. 6. Wireshark: Záznam síťové komunikace – funkce Follow TCP Stream

Vhodným nástrojem pro odposlech síťového provozu je program Wireshark [13], který disponuje nástroji potřebnými k analýze komunikace po síti PROFINET. Zaměříme se na pakety protokolu ISO-TSAP (Transport Service Access Point), který využívají všechna zařízení společnosti Siemens.

Pro odfiltrování ISO-TSAP komunikace je vhodné využít funkci Follow TCP Stream (viz Obr. 6).

Když se na obsah těchto paketů podíváme, je zřejmé, že jsou informace přenášeny ve formě prostého textu (plain text), což velmi usnadňuje analýzu komunikace. Můžeme zaznamenávat jakoukoliv komunikaci mezi PLC a STEP 7 nebo mezi PLC a vizualizačním prostředím SCADA. Beresford uvádí, že je možné zachycené pakety dokonce kdykoliv replikovat a poslat do PLC vlastní příkazy. [1, s. 7]

Je možné vypnout PLC, deaktivovat ochranu paměti nebo nahrát zcela nové funkční bloky (FC, FB, DB) v projektu PLC [4, s. 56–59]. Útočník také může na PLC umístit „backdoor“ uložením škodlivého kódu na konec SIMATIC projektu.

Jako příklad lze uvést chování červu Stuxnet: Pokud je motor centrifugy nakonfigurován tak, aby se otáčel určitým počtem otáček za minutu, je možné buď změnit tuto hodnotu (a způsobit tak poškození centrifugy) nebo úplně zničit celý výrobní závod tím, že se centrifuga rozkolísá tak, že její obsah způsobí explozi. [14]

Z komunikace ISO-TSAP pomocí prostého textu lze, stejně jako např. u protokolů Telnet nebo HTTP, snadno extrahovat uživatelská jména, hesla, příkazy, navázaná spojení atd. Každá takováto informace může vést ke kompromitování celého systému PLC. Lze snadno provést útok MITM (man-in-the-middle). SIMATIC PLC navíc používá i výše uvedené protokoly a služby. S7-300 disponuje Telnet serverem i webovým serverem. S7-1200 ale už navíc obsahuje SimaticHTTP (proprietární HTTPS webový server).

3.3.2 Replay Attack

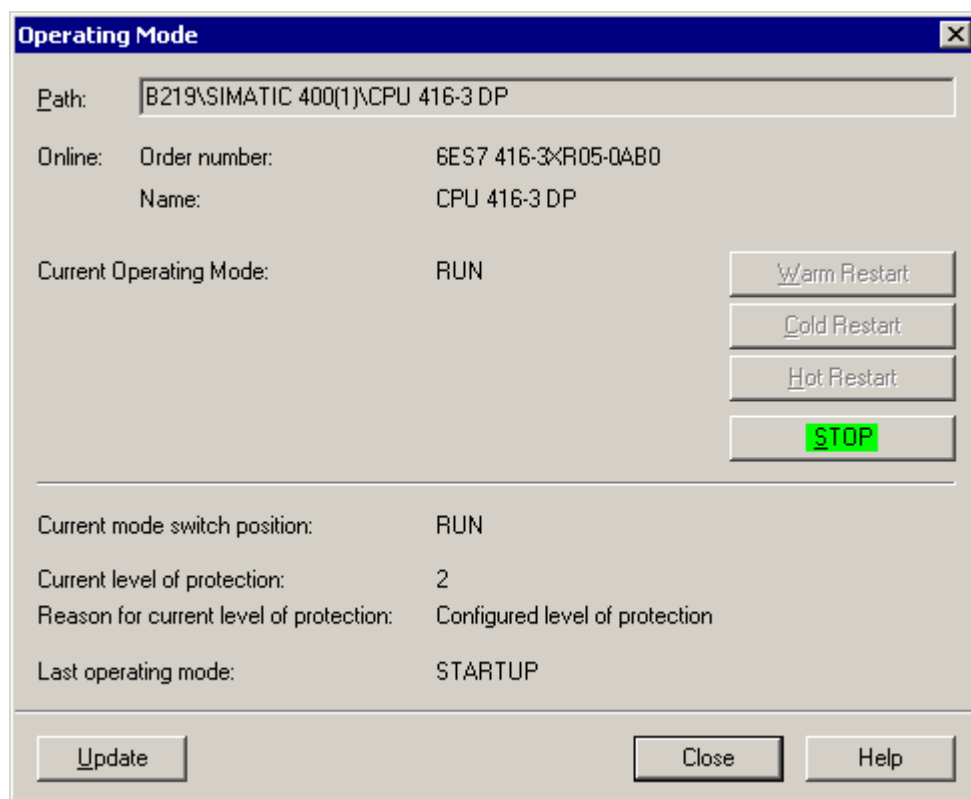
Útok opakováním (tzv. Replay Attack) se od MITM útoku liší. Lze ho použít, když nemaniplujeme se šifrovanými pakety. Jeho obrovskou výhodou je fakt, že PLC ani STEP 7 tento útok neodhalí [1, s. 8]. Jediný rozdíl mezi normálními řídicími a podvrženými pakety je jen jejich zdroj.

Pokud chce jakýkoliv uživatel komunikovat s PLC SIMATIC S7, přístroj může vyžadovat heslo. To znamená, že je PLC chráněn, ale většinou však nejsou. Beresford připomíná, že většina provozovatelů průmyslových sítí věří, že tato zařízení obvykle běží uvnitř hermeticky uzavřené sítě, ve které se neočekává útok proti PLC. Prohlášení zástupců průmyslových odvětví připouští, že tyto útoky nejsou tak časté. I v případě náhlého vypnutí PLC během výroby se technik vždy domnívá, že jde o nějaké mechanické selhání. Externí útok je to poslední, na co by pomyslel. [1, s. 8]

Pokud oprávněný uživatel zašle do PLC ověřovací paket, zařízení provede srovnání hesel nebo hashů, zda se hash z uživatelského paketu shoduje s hashem uloženým v projektovém souboru v paměti PLC.

Je-li podmínka splněna, přístroj změní autorizační bit a umožní čtení, zápis i možnost spouštění v paměti PLC. Co dělat s pakety obsahující hash? Jednoduše je lze replikovat a pak je už možné se autentizovat jako oprávněný uživatel. [1, s. 9]

Dillon Beresford ve svém příspěvku uvádí jeden z postupů zachytávání komunikace. „Nejdříve spusťte Wireshark nebo váš oblíbený zachytávač paketů, pak potřebujete spustit Simatic Manager a připojit se k cílovému PLC pomocí sítě. Dále je nutné zaslat do PLC příkaz CPU STOP a počkat až se provádění příkazu dokončí. Jakmile se vaše PLC zastaví, zastavte záznam paketů a sledujte TCP stream ISO-TSAP komunikace mezi vývojovým softwarem a PLC.“ [1, s. 11]



Obr. 7. SIMATIC Manager STEP7: Příkaz CPU STOP

V TCP streamu je možné pozorovat velké množství užitečných dat. Odezva obsahuje objednávací číslo, model a typ PLC. Pokud extrahujeme klientovu stranu konverzace, můžeme tyto pakety posílat zpět do kteréhokoliv PLC, a získáme tím ze zařízení mnoho hodnotných informací. Pokud útočník vyžaduje dodatečné znalosti o cílovém systému ještě před započítím útoku, může zaznamenat pakety během procesu zálohování a uložit tím obsah paměti PLC. Také je možné připojit škodlivý kód (payload) na konec projektového souboru Step7 pomocí tzv. exploitace. Exploity (exploitační programy) jsou kódy, které jsou schopny narušit část paměti nebo datového bloku. „Finálním cílem těchto technik je převzít kontrolu nad vykováváním toku programu.“ [12, s. 144]

Nyní se zaměříme na trvalé zakázání ochrany. Útočník může zachytit nebo si vytvořit své vlastní ověřené pakety, které pak mohou být posílány zpět do PLC. Vzhledem k tomu, že v Simatic Manageru existuje funkce k odstranění ochrany paměti, je možné tyto pakety zaznamenat, a poslat je zpět do PLC s vlastní autentizací. Útočník tedy může změnit nastavení ochrany paměti, dokonce je možné zamezit oprávněnému technikovi přístup do jeho vlastního zařízení. Beresford uvádí, že když technik otevře projekt ve svém vývojovém softwaru, neuvidí žádnou změnu, neboť ochrana je součástí vývojového softwaru a není na základě změn v PLC v reálném čase aktualizována. [1, s. 16]

3.3.3 Server Session ID

Dalším zajímavým faktem je skutečnost, že serverová autentizace mezi klientem a PLC nikdy nevyprší. To umožňuje útočníkovi zachytit pouze jeden autentizační paket a znovu jej kdykoliv použít, nebo si dokonce vytvořit svůj vlastní. Paket se Server Session ID (identifikátor relace) je umístěn na začátku každého TCP streamu. Jeho formát je například „_706F82AF“ nebo „_546C56B7“.

Je možné vytvářet vlastní relace a kdykoliv je znovu použít na jiné PLC. Řadiče SIMATIC totiž nekontrolují platnost relací, a dokonce jakékoliv dříve vytvořené relace fungují s jinými zařízeními, pakliže se jedná o stejný model PLC. To znamená, že pokud máme k dispozici S7-1200, S7-300 a S7-400, je možné pakety nahrané z těchto přístrojů použít ke komunikaci s jinými řadiči. [1, s. 16]

Produkty S7-300 a S7-400 jsou chápány jako vlajkové lodi společnosti Siemens. Předpokládá se tedy, že sdílejí stejné klíčové vlastnosti, včetně použití ISO-TSAP a stejného jádra komunikace pomocí protokolu PROFINET. I když je PLC chráněn heslem a útočník nemá správný autentizační paket, je stále možné napadnou PLC tím, že ho uvedeme do trvalého chybového stavu, který zapříčiní přechod do stavu STOP. To znamená, že bez ohledu na to, co PLC řídí, připojené zařízení přestane fungovat a důsledky toho mohou být nepředvídatelné, nebezpečné nebo v případě např. elektrárny i život ohrožující. [1, s. 17]

Zasláním speciálních požadavků je možné získat informace z PLC, dokonce i informace, které nejsou určeny pro veřejnost. Můžeme použít stejný replay útok na čtení či zápis i dalších oblastí paměti PLC. To může být například provádění změn konfigurace hardwaru, změna IP adresy, změna času, hesla, odstranění dat, přidání nového kódu, stahování celého projektu atd. [1, s. 19]

4 VIZUALIZAČNÍ SYSTÉMY SCADA

Systémy pro zobrazení technologického procesu se obecně nazývají vizualizace. Mohlo by se zdát, že tyto technologie slouží pouze k rozšířenému „vidění“ pracovníků dispečinků a velínů výrobních závodů. Mnohem širší a výstižnější pojetí slova vizualizace lze nalézt v definici Jaroslava Vlacha:

„Vizualizace, neboli zviditelnění, technologického procesu je vyšší formou jeho řízení, kdy člověk má možnost nejen do řízení děje zasahovat, sledovat jej, příp. reagovat na vzniklé situace, nýbrž průběh děje poznávat z hlediska zákonitostí a vlastností, celý děj popsat, důležité vlastnosti děje archivovat, vytvářet předpisy pro dosažení požadovaného výsledku a postupně tak vytvářet vyšší formu řízení s cílem eliminovat rutinní práce a zvýšit kvalitu práce.“ [15, s. 109]

Vždy je přehlednější vyjádřit informaci v grafické formě nežli v podobě psaného textu nebo těžko čitelného záznamu. V okamžiku, kdy se nějakým prostředkem připojíme k řídicímu systému, můžeme běh tohoto systému sledovat, ale také ovlivňovat. Mezi sledování lze uvést např. různé stavové hodnoty systému, poruchová hlášení, parametry subsystému apod. Smysl má přímo sledovat pouze ty události, které mají zásadní informační hodnotu nebo vyžadují okamžitý zásah člověka (pracovník údržby, ostrahy nebo obsluhy).

Vizualizační systém je soubor prostředků, které jsou nutné pro vizualizaci technologického děje. Dalšími často uváděnými pojmy, které souvisí s vizualizací, jsou HMI (Human-Machine Interface), tedy rozhraní mezi člověkem a strojem, a SCADA (Supervisory Control and Data Acquisition), tedy nadřazené řízení a sběr dat. [15, s. 110]

Vizualizační systém se neobejde bez komunikačního rozhraní, kterými mohou být například RS-485, RS-232C, Profibus DP, Industrial Ethernet nebo Profinet, ale také i GSM, satelitní komunikace, Internet. Vždy je při výběru vhodné zohlednit prostředí, do jakého je systém nasazován.

„Mezi důležité vlastnosti vizualizačního programového vybavení řadíme především:

- *grafické znázornění řízeného technologického děje, příp. s možností animace scény,*
- *popsání řízeného děje (tzv. parametrizace) formou receptur a jejich archivace,*
- *archivace vybraných parametrů řízeného děje,*
- *sledování a archivace zvláštních a chybových stavů (alarmů),*
- *vytváření protokolu o průběhu řízení děje (směnový protokol) a jeho archivace,*

- *sledování vývoje (trendu) vybraných parametrů v čase a jejich archivace,*
- *možnost zpětného vyvolání průběhu děje z archivu a zpracování vybraných parametrů.“ [15, s. 111]*

Na trhu existuje mnoho vizualizačních systémů různých výrobců. Některé jsou díky své příznivé pořizovací ceně vhodné pro menší aplikace, jiné systémy jsou stavěny pro nasazení ve velkých průmyslových provozech, kde počty sledovaných veličin přesahují statisíce a objem zpracovávaných dat přesahuje možnosti běžné pracovní stanice.

4.1 Siemens SIMATIC WinCC

Siemens SIMATIC WinCC je software určený k vizualizaci dat a veličin. Může být spuštěn na jedné stanici nebo jako server pro více klientů. Verze licencí se liší v počtu současně zpracovávaných procesních proměnných (tagů), které se z PLC přenášejí. [6, s. 145]

WinCC se řadí do velké skupiny vizualizačních systémů společnosti Siemens, které pokrývají širokou oblast řešení při různých úrovních obtížnosti nasazení a provozu. Systém WinCC využívá jednotné úložiště správy dat. Od verze WinCC 6.0 se pro ukládání dat používá databázový systém MS SQL Server. WinCC umožňuje kromě sledování a řízení technologie také zpracování velkého množství dat, které lze archivovat nebo předávat dále, například nadřazenému řízení. Data jsou umístěna na pracovní stanici, na kterém je systém nainstalován a spuštěn, ale mohou být také dostupná pomocí komunikačních rozhraní. Dokument WinCC V6 Communication Manual uvádí jako maximální možný počet spojení 60. Novější verze WinCC také umožňují integraci webového rozhraní. Pomocí těchto nástrojů lze využívat spojení přes Internet.

Systém WinCC poskytuje několik druhů konfigurací. Kromě samostatné stanice podporuje konfiguraci server-klient, která umožňuje spojení až 32 klientů. Třetím režimem je tzv. multiklient, který spravuje různé hladiny oprávnění přístupu.

Návrhové prostředí systému WinCC disponuje množstvím vektorových komponent, které lze parametrizovat buď staticky nebo dynamicky pomocí skriptů. Velká variabilita objektů umožňuje vytvářet uživatelsky přívětivá prostředí.

5 PŘEHLED A VOLBA KOMUNIKAČNÍCH BLOKŮ

PLC systémy disponují velkým množstvím komunikačních bloků pro výměnu dat, souborů (FTP), komunikaci po různých sběrnících (Ethernet, Profibus, Profibus FMS, Profinet IO, Profinet CBA). Každý požadavek je specifický a možností návrhu komunikačního rozhraní je vždy více. Proto se vyplatí nejdříve si nastudovat, jaké možnosti a alternativy daný systém nabízí.

5.1 Přehled typů komunikačních funkcí

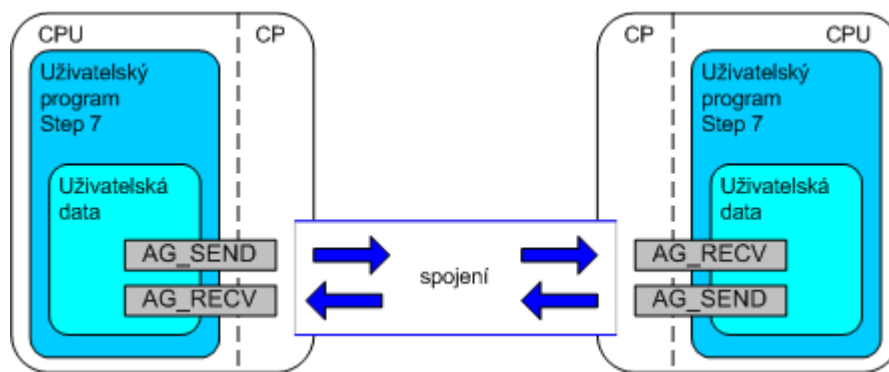
Obousměrnou výměnu dat mezi komunikačními procesory na předem konfigurovaném spojení zajišťují knihovní programové bloky AG_xSEND a AG_xRCV. Jednotlivé verze se liší v dispozici na určitých typech jednotek S7. Například jedinou podporovanou dvojicí funkcí na systému S7-300 je AG_SEND / AG_RECV, která umožňuje zasílání dat o objemu až 8192 bajtů. Komplikací je, že systémy S7-400 sice dvojicí funkcí AG_SEND a AG_RECV podporují, avšak velikost přenášených dat je omezena na 240 bajtů. Pro přenášení dat do velikosti 8192 bajtů u systémů S7-400 poskytuje dvojice funkcí AG_LSEND / AG_LRCV. Základní představu o rozdělení funkcí nabízí tabulka (Tab. 4).

Tab. 4. Přehled standardních funkcí pro přenos dat

| Odesílání | Příjem | S7-300 | S7-400 |
|-----------------|----------------|--------|--------|
| AG_SEND (FC5) | AG_RECV (FC6) | ano | ano |
| AG_LSEND (FC50) | AG_LRCV (FC60) | ne | ano |
| AG_SSEND (FC53) | AG_SRCV (FC63) | ne | ano |

AG_SSEND a AG_SRCV jsou programové bloky optimalizované pro urychlený přenos dat v průmyslových sítích (Profinet). V sítích LAN nemá jejich užití smysl.

U systémů S7-400 nelze použít funkci FC6 pro příjem dat pomocí TCP spojení. K tomu jsou určeny pouze funkce FC60 a FC63.



Obr. 8. Schéma propojení dvou PLC

Jak již bylo uvedeno, při volbě komunikačních bloků je nutné mít na paměti maximální délku přenášených dat, kterou daný typ funkce podporuje. Až do verze 3.0 bloků byla maximální velikost přenesených dat 240 bajtů. Aktuální verze umožňují výměnu až 8192 bajtů dat u jednotek S7-300. U systémů S7-400 je nutné použít funkce AG_LSEND / AG_LRECV. Dřívější verze S7-300 a všechny S7-400 podporují AG_LSEND / AG_LRECV o maximálním objemu dat 8192 bajtů. Pro názornost lze maximální objemy přenesených dat vyčíst z Tab. 5.

Tab. 5. Přehled mezních hodnot objemů dat (AG_xSEND, AF_xRECV)

| FC | ISO transport | ISO-on-TCP | TCP | UDP |
|---|---------------|------------|--------|--------|
| AG_LSEND (S7-400), AG_SEND (S7-300) | 8192 B | 8192 B | 8192 B | 2048 B |
| AG_SEND (S7-400) | 240 B | 240 B | 240 B | 240 B |
| AG_LRECV (S7-400), AG_RECV (S7-300) | 8192 B | 8192 B | 8192 B | 2048 B |
| AG_RECV (S7-400) | 240 B | 240 B | 240 B | 240 B |
| AG_SSEND (S7-400), AG_SRECV (S7-400) | 1452 B | 1452 B | 1452 B | 1452 B |

V okamžiku, kdy je přenos zahájen, není možné měnit parametry spojení volání funkcí AG_xSEND nebo AG_xRECV dokud není indikován konec přenosu jedním z příznaků DONE = 1 nebo ERROR = 1. V opačném případě dojde k chybě přenosu.

5.2 Volba vhodného grafického vyjádření

Grafická podoba vyjádření lépe vystihuje podstatu problému. Programování v programovacím jazyku Step 7 umožňuje grafické ztvárnění přímo při tvorbě, ta to buď v jazyku LAD nebo FBD. Tyto jazyky tak pomáhají k lepšímu porozumění programového kódu. Ne vždy je ale možné zaznamenat sekvenční jev pomocí sledu příkazů tak, aby bylo sdělení srozumitelné.

Sekvenční diagramy UML zachycují chování jednoho případu užití a jednoho scénáře. Mají výhodu v tom, že přehledně popisují zasílání zpráv a jednotlivé objekty jsou jasně vymezené. V neposlední řadě je sekvenční diagram dobře čitelný i pro laika, protože téměř nevyžaduje hlubší studium notace. [16, s. 68]

Sekvenční diagramy mají tu nevýhodu, že u složitějších diagramů není vždy zcela patrná posloupnost zpráv. Při popisu komunikačních funkcí [16, s. 68] ale tato skutečnost nebude na obtíž, protože komunikační bloky budou popisovány samostatně.

Z každého účastníka (objektu) vychází tzv. čára života, která je místy rozšířená. Těmto místům se říká pruh aktivace a symbolizují okamžiky, kdy je objekt aktivní. Aktivace je vždy vázána na některou z metod objektu. Pouze první zpráva nenáleží účastníkovi sekvenčního diagramu a přichází z vnějšku. V případě PLC se jedná o cyklus OB1, který zajišťuje opakované volání a návrat do prováděné struktury.

II. PRAKTICKÁ ČÁST

6 DEFINICE DATOVÝCH STRUKTUR

Řízení dopravníkové techniky vyžaduje vyjádření charakteru jednotlivých prvků dopravníkové techniky pomocí datových struktur. Základem všech informačních systémů je vyjádření informací ve formě dat, které jsou dále organizovány [17, s. 88]. Jak již bylo uvedeno, mezi logické prvky dopravníkové techniky, které jsou v PLC reprezentovány datovou strukturou a vynucují si své stavy sdílet se sousedními částmi technologie, patří zejména semafore, selekční tabulky, průjezdové body a čítače počtu výrobků.

V této kapitole se zaměřím na deklaraci nových datových struktur, které lépe popisují rozsah datových oblastí, které bude nutné mezi jednotlivými PLC sdílet. Je zřejmé, že elementární datové typy není nutné znovu deklarovat a mohou být použity přímo v datovém bloku DB. Jedná se zejména o čítače (velikost zpravidla 1 bajt) či stavy semaforů (1 bit).

Jiné prvky dopravníkové techniky však neposkytují ihned transparentní představu o jejich velikosti. Pokud například chceme vytvořit cyklickou frontu FIFO [18, s. 129] s prvky typu PIN (identifikační označení výrobku), musíme počítat s paměťovým prostorem pro samotné položky a také pro ukazatele na začátek a konec fronty. Odhad velikosti takové struktury již není triviální, zvláště pokud nemáme jasné zadání a představu o budoucí funkci nasazovaného systému.

Zaměřím se především na otázky, zda záleží na charakteru reprezentace dat, co ovlivňuje jejich velikost, a zda je možné bez znalosti zadání znát významnost přenášených dat.

6.1 Popis dopravníkové techniky

Dopravníková technika je soubor strojů a zařízení sloužících k manipulaci, přemísťování, ložení, skladování a usměrňování materiálu (výrobků) a skládá se z dopravníků a podpůrné technologie. Dopravníky jsou různého typu, např. válečkové tratě (dráhy), pásové dopravníky, zdviže, výtahy, závěsné dopravníky, korečkové dopravníky, dopravní skluzy apod. Pro manipulaci s materiálem je vždy určujícím faktorem sledovaný výrobní proces [19, s. 4].

Pro možnost řízení výrobního procesu je však nutné definovat další prvky, které mají buď ryze informativní charakter nebo určují chování pohybu výrobku po dopravníku. Tyto prvky jsou reprezentovány určitou datovou strukturou, která je v době návrhu informačního

systemu neznámá. Pro přehlednost uvádím seznam vybraných prvků dopravníkové techniky a odhad velikosti datové struktury, která daný prvek popisuje pro potřeby řízení (Tab. 6).

U většiny položek je velikost jejich datové reprezentace zřejmá či snadno určitelná. Větší množství podobných prvků nijak výrazně nezvyšuje paměťové nároky. Například 100 semaforů obsadí pouze necelých 13 bajtů, obsazenost v oblasti s 200 dopravníkovými stoly lze vyjádřit pomocí proměnné o velikosti 1 bajt.

Tab. 6. Přehled některých prvků dopravníkové techniky

| Název | Velikost | Popis datové reprezentace |
|---|----------------|---|
| Dopravníkový stůl | 1 bit | Obsazenost dopravníku. |
| Počet výrobků v oblasti dopravníkové techniky | 1 bajt | Lze rozdělit na několik úseků po jednom bajtu. |
| Průjezdni bod | 12 bajtů | Identifikace výrobku pomocí čárového kódu nebo pomocí RFID. |
| Fronta FIFO průjezdního bodu | <i>neznámá</i> | Neznáme velikost zásobníku. |
| Výrobek na dopravníku | 6 bajtů | Informace o typu a barvě výrobku. |
| Obraz zásobníku | <i>neznámá</i> | Záznam jednotlivých pozic pro potřeby funkce volby linií. |
| Položka funkce volby linie | 8 bajtů | Informace o typu, barvě a cíli. |
| Funkce volby linie | <i>neznámá</i> | Určení směru pohybu výrobků na základě jejich typu. |

Problém nastane například u dopravníkového stolu, kde každý průjezd je evidován pomocí 12bajtové struktury PIN. Často ale potřebujeme, ať už z důvodu možnosti krátkodobého výpadku nebo jen pro možnost zpětné analýzy, vytvořit frontu těchto průjezdů. Každá položka navíc způsobí nárůst datové struktury fronty o dalších 12 bajtů. Podobné je to také u obrazu zásobníku, kde ke každému dopravníkovému spolu potřebujeme datovou strukturu VYROBEK o velikosti 6 bajtů. Nejnáročnější datovou strukturou jsou volby linií, jejich paměťovou náročnost lze vyjádřit pomocí následujícího vzorce:

$$\text{obsazenaPamet} = |\text{VYROBEK}| \cdot \text{pocetLinii} \cdot \text{pocetVolebLinii}. \quad (1)$$

Pokud by tedy byl některý zásobník tvořen 10 liniemi o 10 volbách vjezdu příslušného typu reprezentovaném datovým typem VYROBEK, datová struktura by zásobníku by v uživatelské masti zabírala celých 600 bajtů.

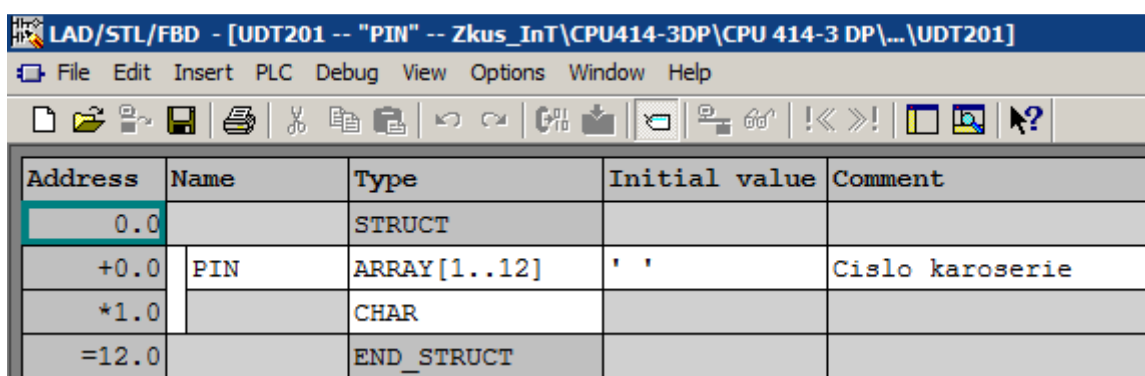
6.2 Tvorba uživatelských datových typů (UDT)

Uživatelské datové typy (UDT) jsou speciální datové struktury pro použití v kterékoliv části programu. Může se jednat o elementární datové typy nebo o složitější datové struktury. Programátor má možnost si takovéto datové typy předem jednou deklarovat, a poté již používat v kterémkoliv typu programového bloku projektu Step7. Hodí se zejména tam, kde je potřeba definovat určitou datovou strukturu jednou a již se k návrhu nevracet. Uživatelské datové typy se nenahrávají do PLC.

UDT fungují jako šablona pro vytváření proměnných. (V jazyku C k podobným účelům slouží klíčová slova typedef struct.) Také je možné vytvářet pole datových bloků s opakující se strukturou.

Uživatelské datové typy se vytvářejí pomocí nástroje SIMATIC Manager. V menu zvolíme volbu Insert – S7 Block – 5 Data Type. Zobrazí se LAD/STL/FBD Editor v deklaračním módu, ve kterém je předpřipravena tabulka pro deklaraci nových datových typů. Datová struktura je ohraničena identifikátory STRUCT na začátku deklarace a END_STRUCT na posledním řádku; tato dvě pole nelze upravovat.

Do jednotlivých řádků lze vkládat jakékoliv již deklarované datové typy. Datová struktura se může skládat z elementárních datových typů, komplexních datových typů a již existujících uživatelských datových struktur.



| Address | Name | Type | Initial value | Comment |
|---------|------|--------------|---------------|-----------------|
| 0.0 | | STRUCT | | |
| +0.0 | PIN | ARRAY[1..12] | ' ' | Cislo karoserie |
| *1.0 | | CHAR | | |
| =12.0 | | END_STRUCT | | |

Obr. 9. LAD/STL/FBD Editor: Definice UDT pro PIN

Pro jednotlivé prvky dopravníkové techniky byly vytvořeny příslušné uživatelské datové typy: Pro uchování informace o průjezdu výrobku evidenčním bodem je nutné znát identifikační číslo výrobku v podobě PIN, který má velikost 12 bajtů. Deklarace této struktury je uvedena na obrázku (Obr. 9). Adresa 0.0 uvádí ukazatel na počátek datové struktury, inkrement +0.0 určuje offset adresy v rámci datové struktury, multiplikátor *1.0 informuje o velikosti každého prvku pole (zde je 12 položek typu CHAR, tedy o velikosti 1 byte). Náväšší =12.0 udává ukazatel za konec datové struktury, tj. velikost v bajtech.

Důležitá je také hodnota Initial value, která určuje počáteční hodnotu proměnné (datové struktury) po inicializaci datového bloku (DB).

| Address | Name | Type | Initial value | Comment |
|---------|----------|-------------|---------------|------------------|
| 0.0 | | STRUCT | | |
| +0.0 | VL_CIL | ARRAY[1..2] | '0' | Linie |
| *1.0 | | CHAR | | |
| +2.0 | VL_TYP | ARRAY[1..2] | '0' | Interní kod typu |
| *1.0 | | CHAR | | |
| +4.0 | VL_BARVA | ARRAY[1..4] | '0' | Kod barvy |
| *1.0 | | CHAR | | |
| =8.0 | | END_STRUCT | | |

Obr. 10. LAD/STL/FBD Editor: Definice UDT pro volbu linie

Na obrázku (Obr. 10) je uvedena datová struktura pro definici volby vjezdu výrobku do konkrétní linie dopravníkového zásobníku. Položka VL_CIL uvádí kód linie, VL_TYP interní identifikátor typu výrobku a VL_BARVA obsahuje alfanumerické označení barevného odstínu výrobků.

6.3 Volba jednotné datové struktury

V předchozí kapitole byl popsán způsob definice datových struktur, které lze použít pro popis a řízení materiálového toku. Nyní máme k dispozici nástroj pro určení fyzických i logických prvků dopravníkové techniky. Lze tvrdit, že nezáleží na charakteru popisovaného prvku, všechny jejich vlastnosti lze reprezentovat pomocí proměnných a uživatelských datových struktur.

Existují ale aspekty, které nelze zobecnit, a je nutné je při návrhu vždy sledovat. Těmi jsou zejména tyto problémy:

- Objem (velikost) dat,
- užitná hodnota dat (ne všechny údaje jsou stejně důležité),
- perioda zasílání dat,
- aktuálnost dat,
- způsob reakce na ztrátu či poškození datového spojení.

Tyto faktory budou určující a zároveň limitující pro další sestavování datové části komunikačního rozhraní. Užitná hodnota záleží na zadání a návrhu konkrétní aplikace a nebudu se jí dále zabývat.

Velikost zasílaných dat může být ošetřena pokročilým řízením správy zasílaných dat nebo lze tento problém řešit využitím takových komunikačních bloků, které umožňují zaslání co největšího objemu dat najednou. Tím bude pravděpodobně limitována univerzálnost řešení, protože se ve všechna PLC podporují stejný horní limit velikosti zasílané zprávy.

Periodu zasílání je možné volit v rozmezí délky cyklu PLC až po libovolně dlouhý časový úsek. Je tedy na programátorovi, jakou periodu zvolí. V případě volby krátké periody hrozí, že se zahltí komunikační kanál. Zbytečně dlouhá perioda způsobí neaktuálnost dat. Horní časový limit neaktuálnosti dat je stejně dlouhý jako je délka periody znovuzasílání. V případě ukázkového projektu bude zvolena perioda zasílání 2 sekundy.

Aktuálnost dat lze zjistit například časovým razítkem. Nelze se však spoléhat na správnost časové synchronizace systémů, které ani nemusí mít časovou synchronizaci nastavenou. Jako optimální řešení pro zjištění aktuálnosti dat se zdá být, který se při každém odeslání zprávy inkrementuje svoji hodnotu. Aktuálnost dat lze pak na straně příjemce zjistit jednoduše tak, že budou vždy srovnávány periodické změny čítače s obvyklou délkou periody příjmu dat.

Velikost datového bloku, ve kterém budou uložena data k odeslání musí mít stejnou velikost jako datový blok na straně příjmu. Stejně tak obráceně. V projektu bude definována symetrická komunikace dvou 100bajtových bloků, přičemž vždy první dva bajty budou obsahovat inkrementální čítač pro diagnostiku aktuálnosti dat.

7 INSTALACE A KONFIGURACE PROGRAMOVÉHO VYBAVENÍ

Pro tvorbu a správu programů pro PLC Siemens řady SIMATIC S7-400 je nutné použít proprietární software Siemens SIMATIC STEP 7, který je v posledních letech postupně integrován do nové koncepce integrace inženýrských nástrojů TIA Portal. Siemens SIMATIC STEP 7 je však stále možné instalovat samostatně a je standardně distribuován na DVD nosičích. Jedinými podporovanými operačními systémy jsou operační systémy Microsoft Windows.

Software pro řízení toku výroby, sběr dat a dálkové sledování průmyslových procesů je zpravidla označován jako SCADA (Supervisory Control and Data Acquisition). Slouží také například ke sledování spotřeby elektřiny, vody, sledování dopravních a komunikačních sítí apod. Prostředí TIA nabízí nástroj Siemens SIMATIC WinCC. Přímé datové spoje lze z WinCC vytvářet pouze pokud je nainstalováno rozhraní Siemens SIMATIC SOFTNET-S7.

7.1 Siemens SIMATIC STEP 7 Professional 2010

Přestože je software Siemens SIMATIC STEP 7 komerční, lze si jeho instalaci volně stáhnout z webových stránek společnosti Siemens. Tato instalace obsahuje zkušební licenci, která umožňuje testování softwaru po dobu 14 dnů. Pro komerční využití je nutné koupit softwarovou licenci. Součástí všech produktů řady Siemens SIMATIC je společný správce licencí Automation License Manager. Každá varianta produktu vyžaduje zakoupení samostatné licence v podobě datového souboru EKB.

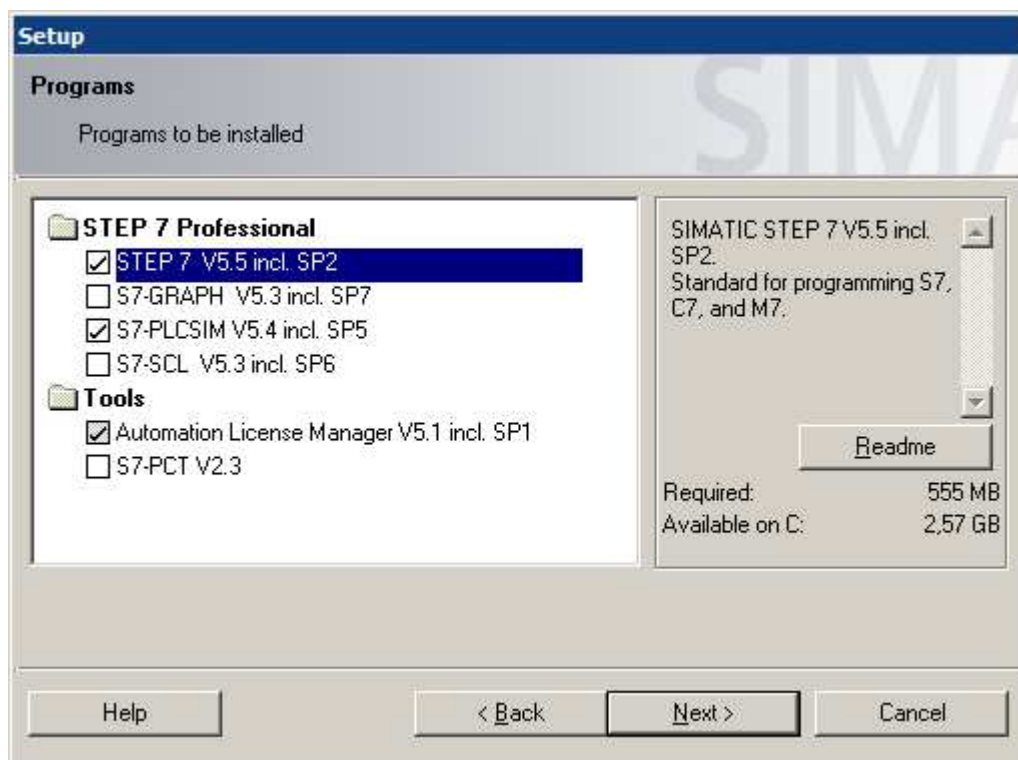
Před koupí licence je nutné zvážit, která verze operačního systému je se kterou distribucí produktu Siemens SIMATIC STEP 7 kompatibilní. Výrobce průběžně aktualizuje informace o doporučených konfiguracích. Pro 64bitový operační systém Microsoft Windows 7 Professional SP1 je ověřená kompatibilita s produkty STEP 7 verze 5.5 SP2 a vyššími. [20]

Před samotnou instalací je nutný restart operačního systému. Po vložení instalačního DVD se spustí instalace. V prvním kroku lze vybrat jazyk uživatelského prostředí; nabízí se němčina, angličtina, francouzština, španělština a italština. Po přečtení poznámek k instalaci (soubor Readme.rtf), licenční smlouvy a jejím potvrzení se zobrazí dialogové okno voleb instalace (Obr. 11).

Program STEP 7 slouží pro samotnou tvorbu programů pro PLC, S7-GRAPH umožňuje programování pomocí grafických programových schémat a speciálních sekvenčních diagramů. S7-PLCSIM je softwarový simulátor PLC. Instalace licenčního nástroje Automation License Manager je, jak již bylo uvedeno, nutná. Po odsouhlasení přehledu provedených změn se spustí instalace všech zvolených programů.

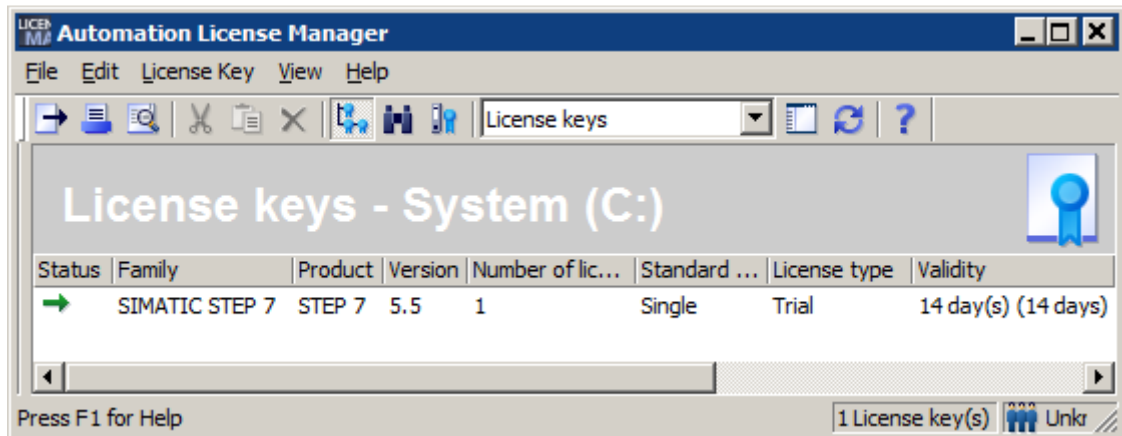
Software STEP 7 nabízí tři druhy instalací: Typickou (Typical), minimální (Minimal) a volitelnou (Custom), kterou lze doporučit. Poté se instalátor uživatele dotáže, jaké jazyky bude používat. Jedná se zejména o uživatelské rozhraní a soubory nápovědy. Je vhodné instalovat alespoň angličtinu a němčinu. Instalace se dokončí tlačítky Next a Install. Na konci instalačního procesu se instalátor dotáže, zda chceme počítač restartovat.

Výrobce doporučuje software pravidelně aktualizovat. Aktualizace jsou dostupné zdarma na webu <https://support.automation.siemens.com> ve formě archivu ZIP nebo lze objednat DVD. Po spuštění aktualizace je nutné zvolit variantu upgrade a instalátor sám detekuje instalovanou verzi. Průběh instalace je obdobný jako u první. V případě instalace licencovaného produktu vyzve instalátor uživatele k importu licenčního souboru.



Obr. 11. STEP 7 Professional: Volba programových komponent

Ke správě klíčů slouží program Automation License Manager. Při prvním spuštění uživatele varuje, že nebyl nalezen žádný platný klíč, pro účely vyzkoušení programu lze potvrdit předvolenou instalaci 14denní licence Trial.



Obr. 12. STEP 7 Professional: Automation License Manager

7.2 Siemens SIMATIC WinCC 6.0

Tato verze vizualizačního systému vyžaduje mít na operátorské stanici operační systém Microsoft Windows XP SP2 a novější. Jsou podporovány i systémy Microsoft Windows Vista a Microsoft Windows 7. Podrobný návod na instalaci je popsán v příložené uživatelské příručce. Je nezbytné dbát jeho pokynů, protože se spolu s WinCC instaluje také databázový server Microsoft SQL Server. V případě existence tohoto databázového na operátorském počítači je nutné dbát zvýšené obezřetnosti při konfiguraci WinCC.

Postup instalace licenčního klíče je obdobný jako u softwaru Siemens SIMATIC STEP 7.

Hlavním programem pro správu vizualizačních projektů je WinCCExplorer. V daný okamžik je možné mít otevřený pouze jeden projekt. Každý projekt se skládá z adresářového stromu, přičemž v hlavní složce projektu je vždy umístěný pivot s názvem shodným s názvem projektu a příponou mcp.

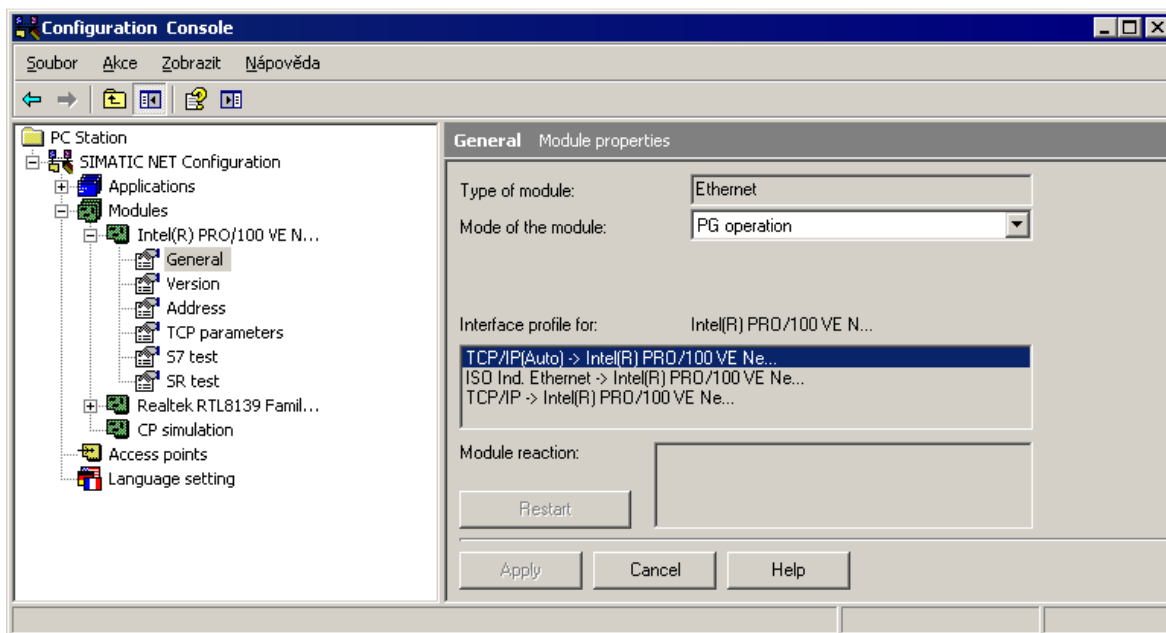
WinCCExplorer je možné používat jako spouštěč run-time režimu vizualizačního projektu, ale spuštění projektu se dá také nastavit ve vlastnostech spuštění. V případě potřeby otevření jiného projektu je nutné nejprve aktuální projekt zavřít. Při uzavírání programu WinCCExplorer je uživatel dotázán, zda chce pouze uzavřít vývojové prostředí a chce

ponechat vizualizační projekt v režimu run-time, nebo také nabízí ukončení a uzavření práce s projektem.

7.3 Siemens SIMATIC Softnet-S7

Aby bylo možné vytvářet přímé datové spoje, je nutné mít nainstalován také ovladač Siemens SIMATIC SOFTNET-S7 BASIC ze softwarového balíku SIMATIC NET.

Dle konfigurace operátorské stanice je po instalaci nutné vytvořit tzv. Access Point (přístupový bod). Po spuštění nástroje SIMATIC NET (Obr. 13) se zobrazí hierarchie konfiguračního stromu PC Station. Přístupový bod se volí v záložce SIMATIC NET Configuration – Modules – síťový adaptér (zde „Intel(R) 82567LM-3 Gigabit Network Connection“) – General. V seznamu „Interface profile for:“ je nutné zvolit síťový profil TCP/IP, tedy „TCP/IP -> Intel(R) 82567LM-3 Gigabit Network Connection“.



Obr. 13. SIMATIC NET Configuration Console

8 KONFIGURACE HARDWARE

Volba hardwaru je zásadní pro kvalitu vytvořeného spojení. Bylo experimentálně ověřeno, že rychlost datové komunikace mezi několika PLC závisí především na použitém hardwaru (typ CPU) a typu zvolené průmyslové sítě. [21]

Pro testování rozhraní pro výměnu dat mezi dvěma systémy Siemens SIMATIC S7-400 jsem měl k dispozici osazené racky se procesory CPU 414-3 DP a CPU 416F-2, oba s komunikačním procesorem CP 443-1 (Obr. 14).

| Slot | Module | Order number | Firmware | MPI address | I address |
|------|---------------------|----------------------------|-------------|-------------|-----------|
| 1 | PS 407 10A | 6ES7 407-0KA00-0AA0 | | | |
| 3 | CPU 414-3 DP | 6ES7 414-3XJ00-0AB0 | V3.1 | 3 | |
| X2 | DP | | | | 8191* |
| X1 | MPI/DP | | | 3 | 8190* |
| IF1 | IF 964-DP | 6ES7 964-2AA01-0AB0 | | | 8181* |
| 5 | CP 443-1 | 6GK7 443-1EX11-0XE0 | V1.1 | | 8189* |

| Slot | Module | Order number | Firmware | MPI address | I address |
|------|-------------------|----------------------------|-------------|-------------|-----------|
| 1 | PS 405 10A | 6ES7 405-0KA01-0AA0 | | | |
| 3 | CPU 416F-2 | 6ES7 416-2FN05-0AB0 | V5.1 | | |
| X2 | DP | | | | 16383* |
| X1 | MPI/DP | | | | 16382* |
| 4 | CP 443-1 | 6GK7 443-1EX11-0XE0 | V1.1 | | 16378* |

Obr. 14. Hardwarová konfigurace zkušebních CPU

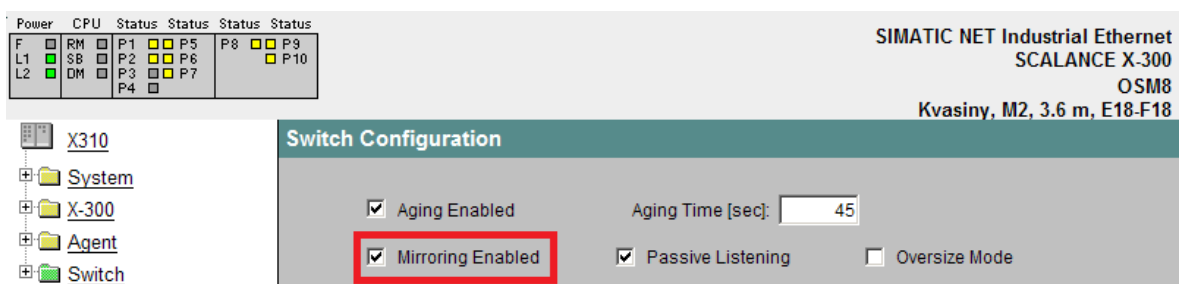
Z obrázku lze vyčíst, že racky jsou napájeny zdroji, které zaujímají dvě pozice. CPU 414-3 DP obsazuje také dvě pozice, ale CPU 416F-2 jednu, stejně tak oba komunikační procesory CP 443-1. Sloupec Order number uvádí jedinečné objednávací číslo produktu. Za povšimnutí také stojí vstupní adresa komunikačního protokolu, která je zde uvedena v desítkové soustavě.

8.1 Síťové propojení

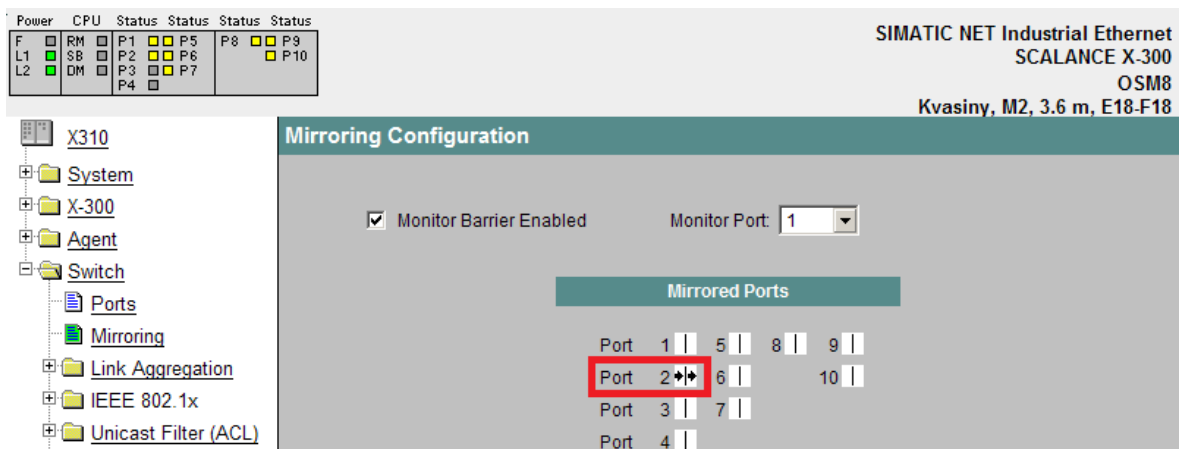
Obě CPU jsou propojena patch kabely přes průmyslový přepínač SCALANCE X-308-2 (Obr. 17). Ten lze konfigurovat, a pro potřebu diagnostiky a odchyťování datových paketů bylo také nutné nastavit zrcadlení portů.

Nejprve je nutné nastavit IP adresu přepínače. K tomu slouží nástroj Primary Setup Tool (PST), který vyhledá všechna průmyslová zařízení v síti a nabídne uživateli základní konfiguraci včetně IP adresy. Od okamžiku nastavení je možné přepínač spravovat pomocí webového prohlížeče. Do adresního řádku prohlížeče stačí zadat IP adresu přepínače a stisknout Enter. Zobrazí se výzva k zadání uživatelského hesla, které bylo nastaveno pomocí PST.

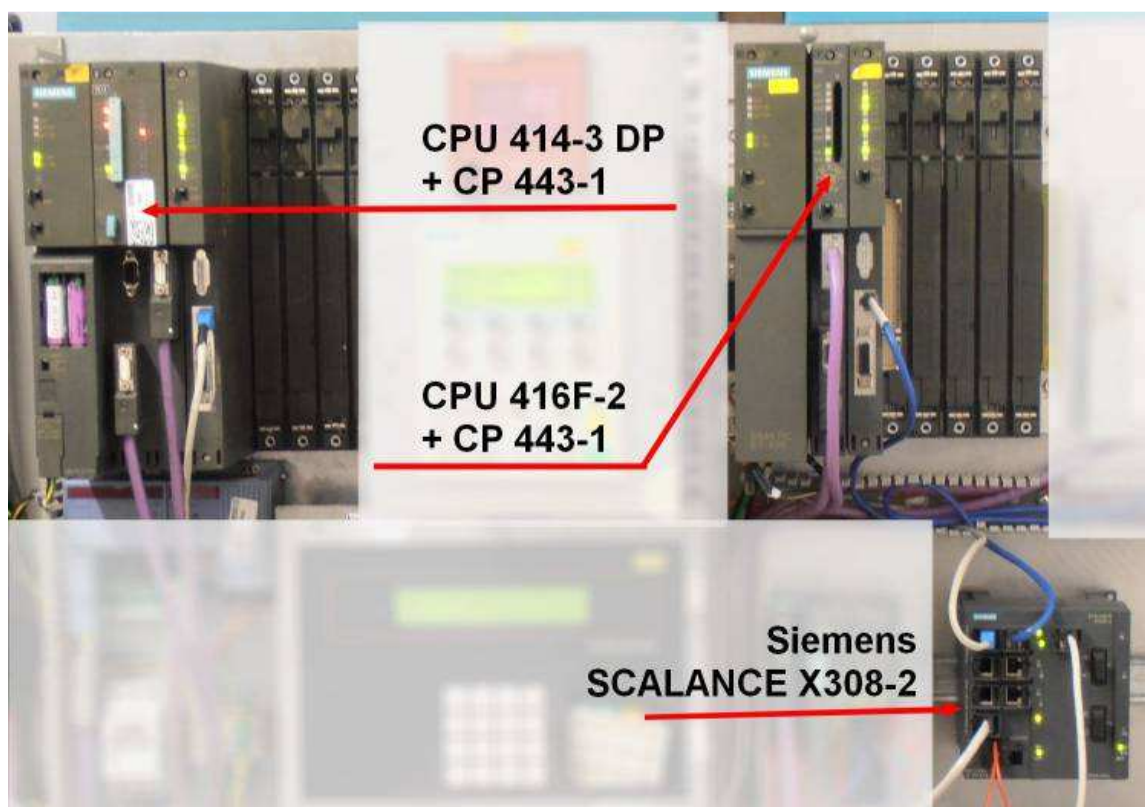
Kromě běžného nastavení služeb a VLAN je nutné nastavit zrcadlení portu. Nejdříve je třeba aktivovat volbu „Mirroring Enabled“ (Obr. 15). Po potvrzení je potom nutné zvolit port, který je v záměru sledovat (Mirrored Port) a který port bude sledující (Monitor Port). V menu Mirroring lze nastavit výše popsané volby. Např. na obrázku (Obr. 16) je nastaven jako monitorující port č. 1; z portu č. 2 bude zaznamenávána příchozí i odchozí komunikace a bude posléze kopírována do portu č. 1



Obr. 15. SCALANCE: Aktivace funkce zrcadlení portu



Obr. 16. SCALANCE: Aktivace zrcadlení portu na zvolený port



Obr. 17. Pohled na instalaci zkušebních CPU a průmyslového switche

9 PROGRAM V JAZYKU STEP7

Výměnu dat mezi zařízeními lze realizovat několika způsoby. Pro ilustraci tvorby spojení jsem zvolil velmi často používaný protokol TCP. Komunikační procesory jsou však schopny navázat spojení pomocí mnoha různých protokolů. Ke každému protokolu existuje doporučená komunikační systémová funkce [22].

Pro realizaci spojení pro oboustrannou výměnu dat jsem zvolil komunikační bloky FC50 (AG_SEND) a FC60 (AG_RECV), které PLC S7-400 podporuje. Tyto bloky jsou určeny pro komunikaci zejména protokolů TCP, ISO-on-TCP (RFC 1006), ISO transport, UDP a FDL.

Mezi hlavní charakteristiky funkcí (komunikačních bloků) FC50 (AG_LSEND) a FC60 (AG_LRCV) jsou:

- FC50 a FC60 jsou asynchronní komunikační funkce,
- běh je rozprostřen do několika cyklů procesoru,
- FC50 je aktivován vstupním parametrem ACT,
- konec úlohy je indikován příznaky DONE nebo ERROR,
- AG_LSEND a AG_LRCV mohou komunikovat souběžně pomocí jediného spojení,
- nejnovější verze komunikačních bloků FC50 (AG_LSEND) a FC60 (AG_LRCV) jsou k dispozici v knihovně SIMATIC_NET_CP v menu CP 400 / Blocks.

9.1 Popis programu

Program vytvořený v jazyku S7 volá komunikační bloky FC50 (AG_LSEND) a FC60 (AG_LRCV). Tyto bloky jsou k dispozici v knihovně funkcí SIMATIC_NET_CP. Protože mají funkce standardní popisy parametrů, používám i stejnou symboliku. České názvy a význam jednotlivých vstupů a výstupů jsou uvedeny v komentářích projektu Step7.

FC50 (AG_LSEND) je určen pro odesílání dat na vzdálenou stanici. Ta může být součástí systému S7 nebo S5 nebo dokonce se může jednat o jiné komunikační zařízení, které podporuje protokol IEEE 802.3 Ethernet a vyšší komunikační vrstvy. FC60 (AG_RECV) data přijímá a stejně jako AG_LSEND akceptuje různé komunikační partnery.

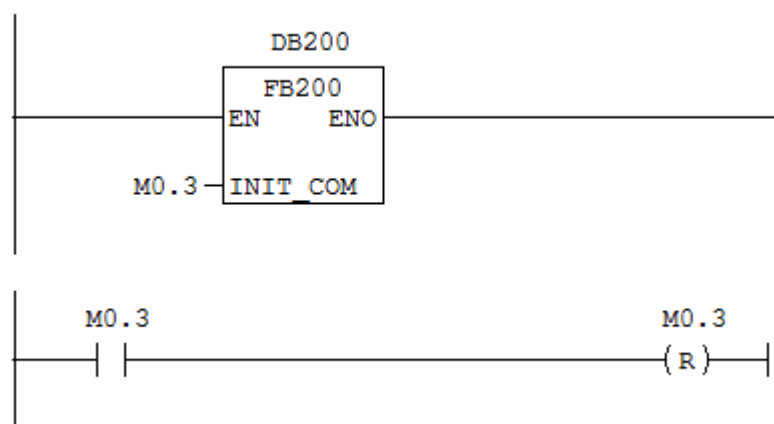
Nejnovější verzi těchto bloků lze zkopírovat z knihovny SIMATIC_NET_CP nebo ze standardní knihovny vývojového prostředí Simatic Manager.

Podrobnému nastavení síťového rozhraní a komunikace se věnuje v kapitole 9.2.2.

Kromě výše uvedených bloků se program skládá z bloků FB200, DB200 a DB201. Součástí programu jsou také rutiny volané v organizačních blocích OB1 a OB100.

Blok OB100 blok je spuštěn právě jednou a to při kompletním restartu PLC (tzv. warm start). V programu se předpokládá využití uživatelských „konstant“ v podobě M0.1 (vždy true), M0.2 (vždy false) a M0.3, který je aktivní pouze v nultém cyklu PLC při restartu systému. Tyto konstanty jsou blíže popsány v kapitole 9.2.1.

Do OB1, který obvykle nazývá jako cyklický, je nutné vložit následující kód, který volá funkční blok FB200 (Obr. 18). Ten využívá pro uložení statických hodnot instanční datový blok DB200. Parametrem volání je příznak inicializace PLC (M0.3), který je po úspěšném průběhu funkce navždy resetován.



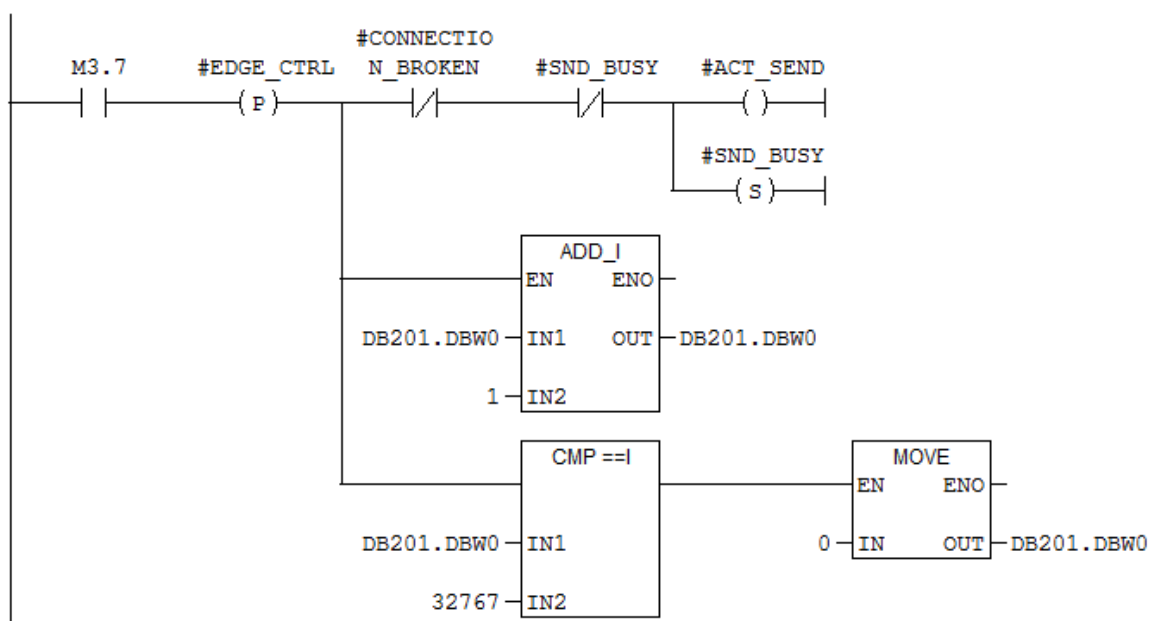
Obr. 18. Volání komunikačního funkčního bloku z OB1

Hlavní částí programu je funkční blok FB200, který je volán z OB1. Má na starosti následující tři funkce: Zajištění odesílání dat a zpracování stavů komunikace, zajištění příjmu dat a zpracování stavů komunikace a nakonec zpracování statistik spojení.

Nejdříve jsou definovány parametry spojení. Ty lze vyčíst z nástroje NetPro (Obr. 29). Jedná se o identifikátor komunikačního procesoru (ID) a jeho počáteční adresu (LADDR).

Hodnota požadavku odeslání se stanoví vzestupnou hranou časového memory bitu (Clock Memory) s periodou cyklu 2 sekundy. K aktivaci požadavku může dojít pouze pokud není přerušena komunikace a neprobíhá vysílání dat.

Dále je prováděna inkrementace stavového čítače DB201.DBW0, který v případě navýšení o jednotku za 2 sekundy signalizuje příjemci bezchybný řádný chod zasílání dat. V případě, že tato hodnota ustrne na určité hodnotě, příjemce může snadno vyhodnotit, k jakému problému došlo. Implementace diagnostiky nebyla realizována.

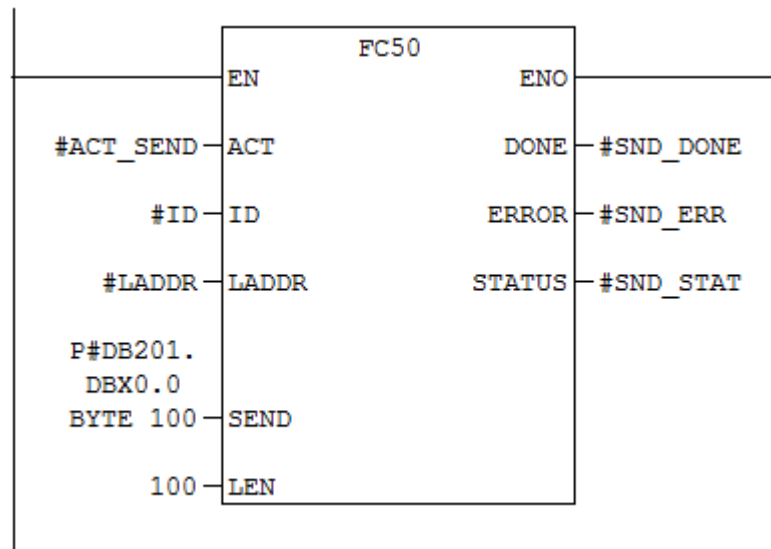


Obr. 19. Podmínky inicializace požadavku odeslání dat a life signál

Požadavek k obdržení dat je řízen proměnnou RCV_DISABLE. Hodnota této proměnné je vždy false, takže funkce FC60 (AG_LRCV) je vždy připravena k příjmu a data mohou být kdykoliv přijímány. Tato možnost blokace je obzvlášť důležitá, protože komunikace je definována jako asynchronní a přenos dat může trvat několik cyklů. Neustálé zasílání dat bez zřetele na dokončení předchozího přenosu způsobí zahlcení komunikace a komunikační bloky zahlásí chybu z přetížení.

Parametr SEND funkce FC50 je typu ukazatel a uvádí počátek přenášených dat. Může se jednat o vyrovnávací paměť, u které můžeme uvést i velikost v bytech. Formát ukazatele v jazyku Step7 je P#DB???.DBX??.? BYTE ???. kde místo otazníků jsou číselné identifikátory. Parametr LEN uvádí délku přenášených dat v bytech.

Výstupní parametry DONE, ERROR a STATUS jsou nutné pro správné vyhodnocení prováděné úlohy a mají platnost pouze jeden cyklus. V případě potřeby je nutné tyto hodnoty uchovat ve statických proměnných.



Obr. 20. Volání funkce AG_LSEND (FC50)

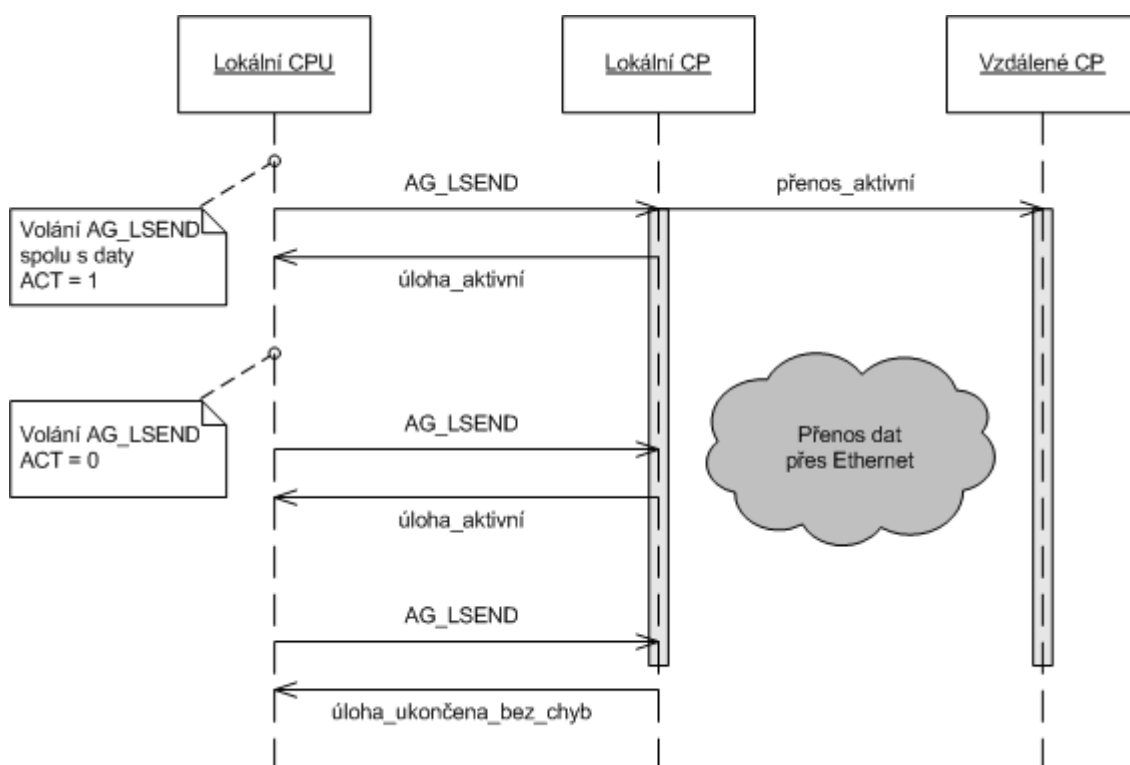
Volání funkce FC50 (AG_LSEND) je znázorněno na obrázku (Obr. 20). Je-li žádost o zaslání dat úspěšně dokončena, příznak SND_BUSY se vynuluje a blok je v dalším cyklu PLC připravený znovu vysílat data. V případě chyby se tento příznak rovněž vynuluje, ale dál je také zpracován chybový příznak z výstupního parametru STATUS. Pokud je hodnota parametru výstupu rovna 0x7000, pak je funkce AG_LSEND volána znovu.

Tab. 7. Přehled základních stavů funkce AG_LSEND

| Stav | Význam |
|-------|---|
| 0000H | Úloha byl zpracována bez chyb |
| 0000H | Žádná úloha nebyl spuštěna |
| 8181H | Úloha je aktivní |
| 7000H | Tento kód je možný pouze u procesorů S7-400. Funkční blok byl deaktivován hodnotou ACT = 0, avšak úloha ještě nebyla zpracována |

Pokud je stavový parametr roven hodnotám 0x8183 nebo 0x8304, nelze navázat spojení. V tomto případě je dojde k deaktivaci funkce AG_LSEND na 10 sekund (Obr. 22). Přehled základních chybových stavů FC50 je uveden v tabulce (Tab. 7).

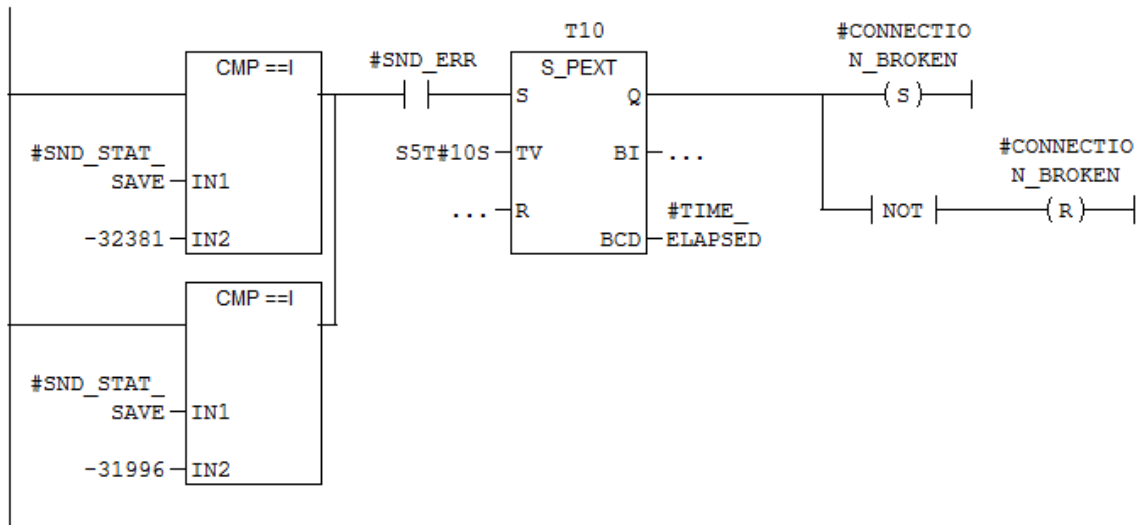
Sekvenční diagram (Obr. 21) znázorňuje vazby funkcí AG_LSEND na události spojené s odesláním dat. [22]



Obr. 21. Sekvenční diagram funkce AG_LSEND (FC50)

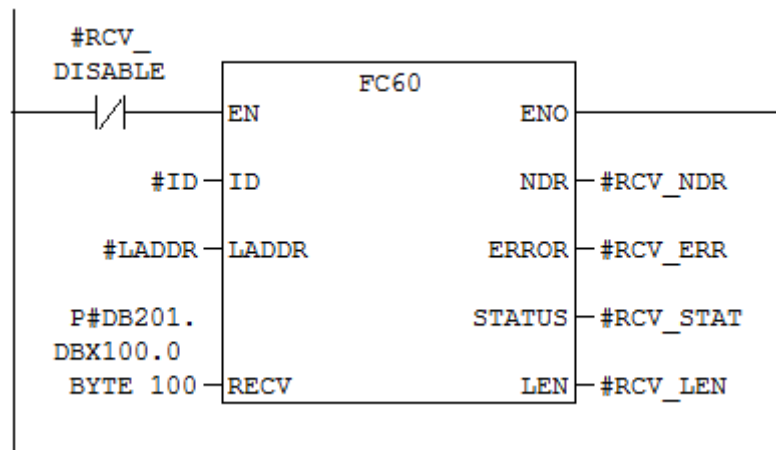
Volání funkce FC60 má podobné parametry jako FC50. Jak již bylo uvedeno, je nutné zavést možnost deaktivovat volání této funkce z důvodu zpracovávání požadavku, výskytu chyby nebo i z jiných důvodů definovaných programátorem.

Výstupní parametr NDR (New Data Received) poskytuje informaci o nově doručených datech. Vždy je vhodné vyhodnocovat tento příznak spolu s parametry STATUS i ERROR, protože jejich hodnoty mohou mít společné souvislosti.



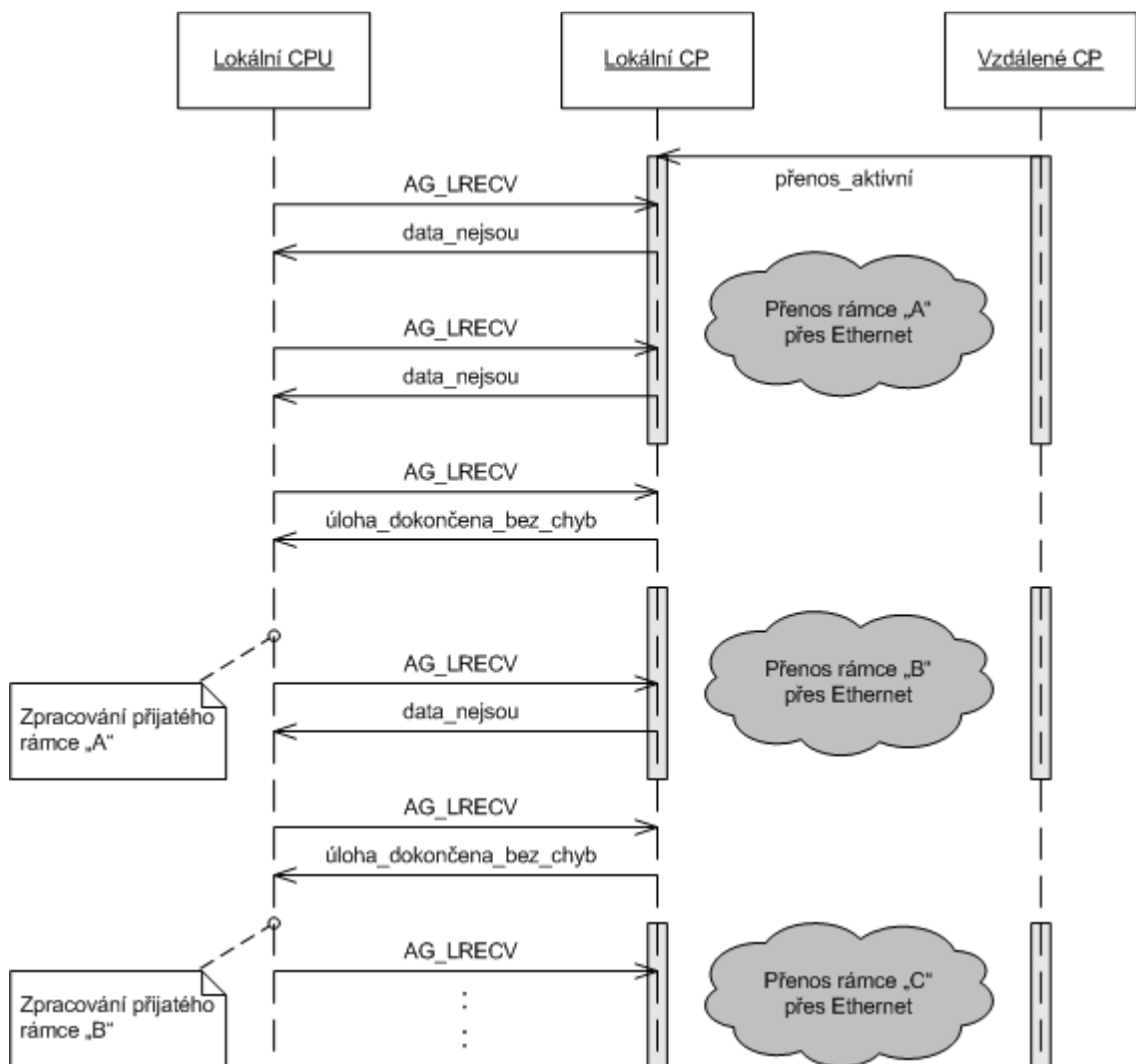
Obr. 22. Deaktivace volání funkce AG_LSEND v případě poruchy

Obdobně jako u funkce FC50 je při výskytu stavu 0x8183 nebo 0x8304 vyvolána deaktivace příjmu na 10 sekund. Během této doby není možné žádná data přijímat.



Obr. 23. Volání funkce AG_LRCV (FC60)

Sekvenční diagram (Obr. 24) znázorňuje vazby funkcí AG_LSEND na události spojené s příjmem dat. [22]



Obr. 24. Sekvenční diagram funkce AG_LRECV (FC60)

Pro analýzu správné funkce komunikace obsahuje FB200 také statistický modul, který zaznamenává četnost chybových hlášení z parametrů STATUS. Pro tyto účely byla vytvořena statická datová struktura, která výsledky vyhodnocení uchovává v datovém bloku DB200. Statistický modul je možné kdykoliv zapnout či vypnout bitem STATISTIC ON/OFF. Přehled základních chybových stavů FC60 je uveden v tabulce (Tab. 8).

V případě, že výměna dat probíhá pomocí TCP spojení, pak je do výstupního parametru NDR uložen příznak o přijetí pouze v případě, když je vyrovnávací paměť na straně příjmu zcela zaplněn. Hodnota výstupního parametru LEN tedy vždy označuje celkovou délku vyrovnávací paměti na straně příjemce.

Tab. 8. Přehled základních stavů funkce AG_LRECV

| Stav | Význam |
|-------|--|
| 0000H | Nová data byla přijata |
| 8180H | Doposud nejsou k dispozici žádná nová data |
| 8181H | Úloha je aktivní |

9.2 Nasazení programu

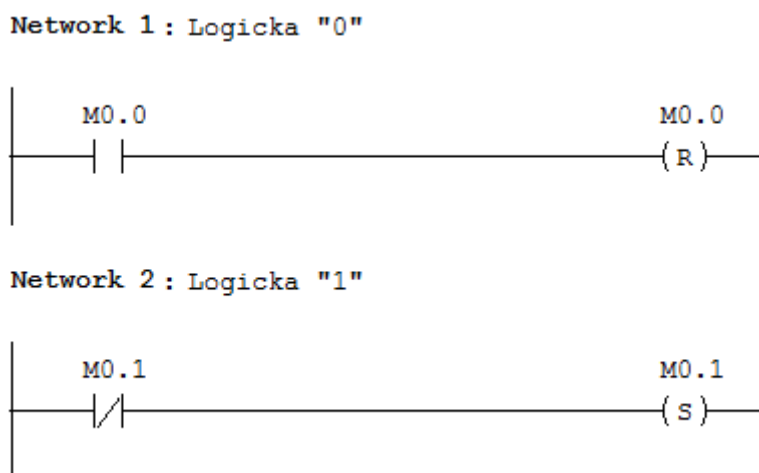
Každá instalace má svá specifika, obzvláště když je potřeba nasadit zdrojový kód do již funkčního systému. Je vždy nutné se přizpůsobit místnímu nastavení systému a dané konfiguraci. U systémů Siemens SIMATIC S7 je vždy nutné brát na zřetel zejména tyto aspekty:

- adresy trvalé nuly a jedničky, příznak náběhu systému,
- adresa časového memory bitu,
- velikost volné uživatelské paměti,
- obsazenost symbolických názvů programových bloků.

9.2.1 Konstanty, paměť a symbolické názvy

PLC SIMATIC nedisponuje trvalou konstantou logické jedničky a nuly. Tyto konstanty je vždy nutné vytvořit. Programátor, který nový PLC systém nasazuje, obvykle tyto bitové „konstanty“ definuje jako první (Obr. 25).

Další často definovanou konstantou je příznak náběhu systému. Tato hodnota je často využívána v prvním cyklu běhu programu pro inicializace a náběhy různých podsystémů a podprogramů. Má tedy podobné využití jako organizační blok OB100, avšak OB100 podprogramy volá, příznak náběhu systému je používán jako parametr volání cyklicky zpracovávaných bloků.



Obr. 25. Inicializace trvalé jedničky a trvalé nuly

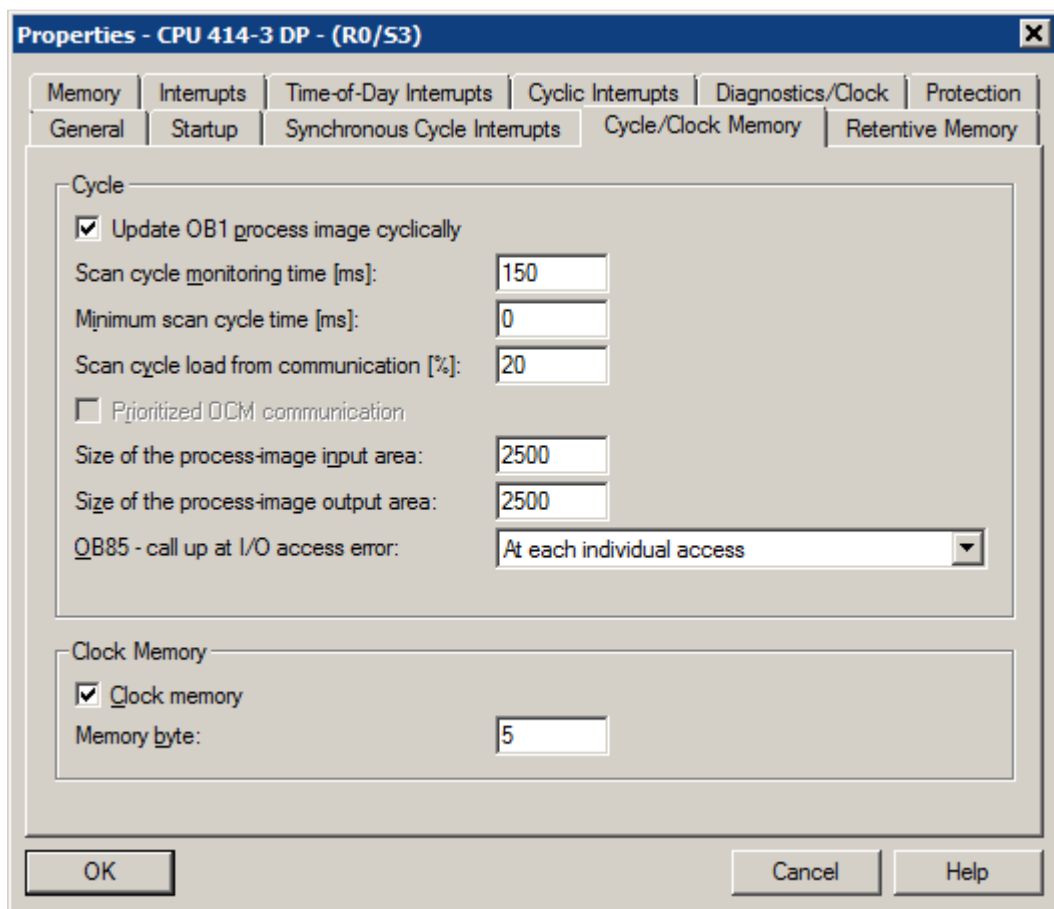
Clock Memory je speciální byte v uživatelské oblasti dat, který se periodicky mění v závislosti na času. Každému bitu je přiřazena perioda změn. Často se využívá pro blikání signálních světel, cyklickému spouštění různých podprogramů apod. Adresa tohoto bytu se nastavuje v nástroji Hardware Configuration.

U CPU zvolíme Object Properties a zobrazí se dialogové okno (Obr. 26). Clock Memory se nastavuje v kartě Cycle/Clock Memory.

Tento byte se již v existujícím projektu pravděpodobně využívá, proto tato volba souží pro zaznamenání adresy časového memory bitu (součást uživatelské paměti). Pro úplnost uvádím, že Clock Memory není synchronní s cykly CPU, takže u dlouhých cyklů může dojít ke změně stavu některých bitů i několikrát za jeden cyklus.

Tab. 9. Přiřazení časových period jednotlivým bitům Clock Memory

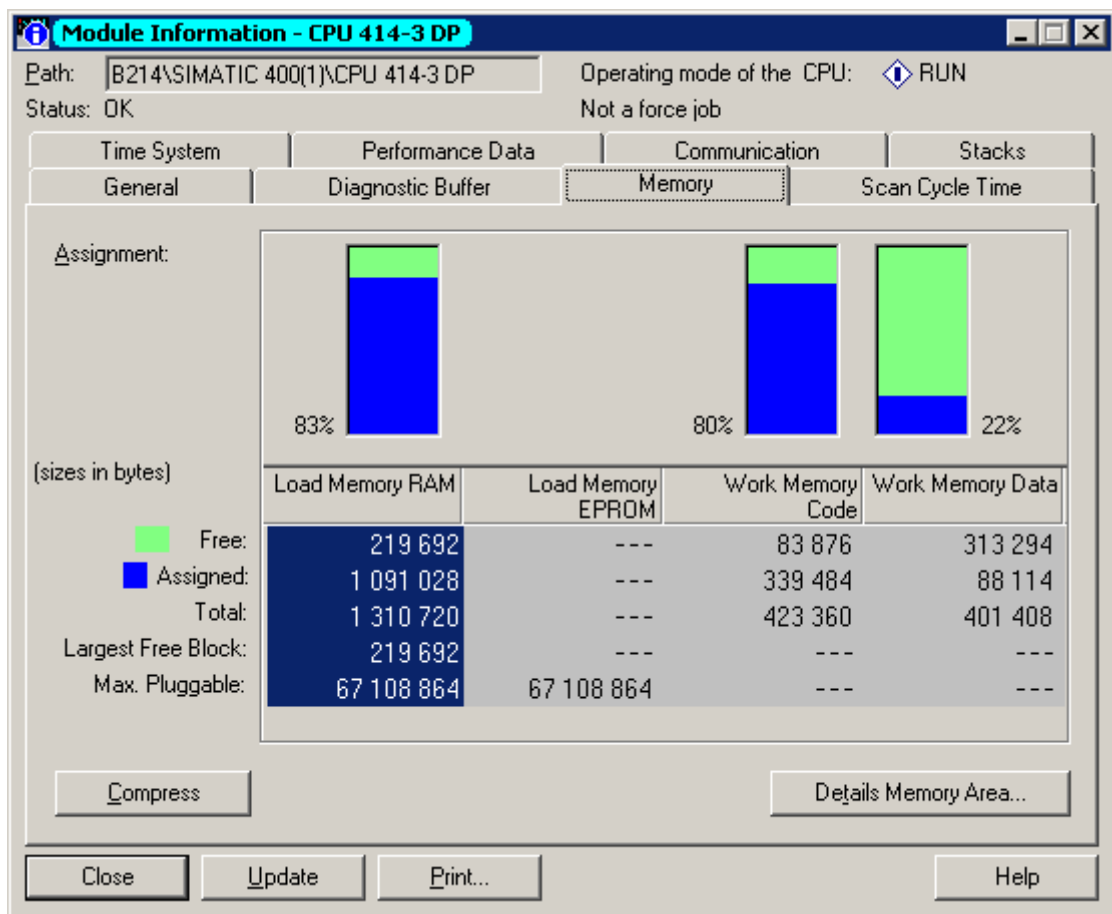
| Bit | 7 | 6 | 5 | 4 | 3 | 2 | 1 | 0 |
|----------------|-----|-------|-----|------|-----|-----|-----|-----|
| Perioda [s] | 2,0 | 1,6 | 1,0 | 0,8 | 0,5 | 0,4 | 0,2 | 0,1 |
| Frakvence [Hz] | 0,5 | 0,625 | 1,0 | 1,25 | 2 | 2,5 | 5,0 | 10 |



Obr. 26. Nastavení Clock Memory

Před jakoukoliv úpravou projektu je dobré vždy zkontrolovat obsazení uživatelské paměti, zda nedochází k velké fragmentaci dat, a zda máme dostatečný prostor pro vložení nových dat. Potřebné informace lze zjistit v dialogovém okně Module Information (Obr. 27), které zobrazíme v programu Simatic Manager pomocí stisku klávesové kombinace Ctrl+D. Pro tuto operaci musíme být s PLC spojeni. V případě velkého zaplnění lze stisknout tlačítko Compress a provede se zhuštění (defragmentace) datových boků v uživatelské paměti. Tuto operaci lze provést i za běhu (režim RUN-P).

Posledním uváděným problémem při nasazování částí nového programu je kolize symbolických názvů jednotlivých bloků. Organizační bloky přejmenovat nelze, u nich musí dojít k implementaci kódu do již existujícího bloku. Ostatní funkce, datové a funkční bloky je nutné jednoduše přejmenovat a provést příslušné úpravy v jejich volání.



Obr. 27. Kontrola obsazenosti uživatelské paměti

9.2.2 Nastavení sítě

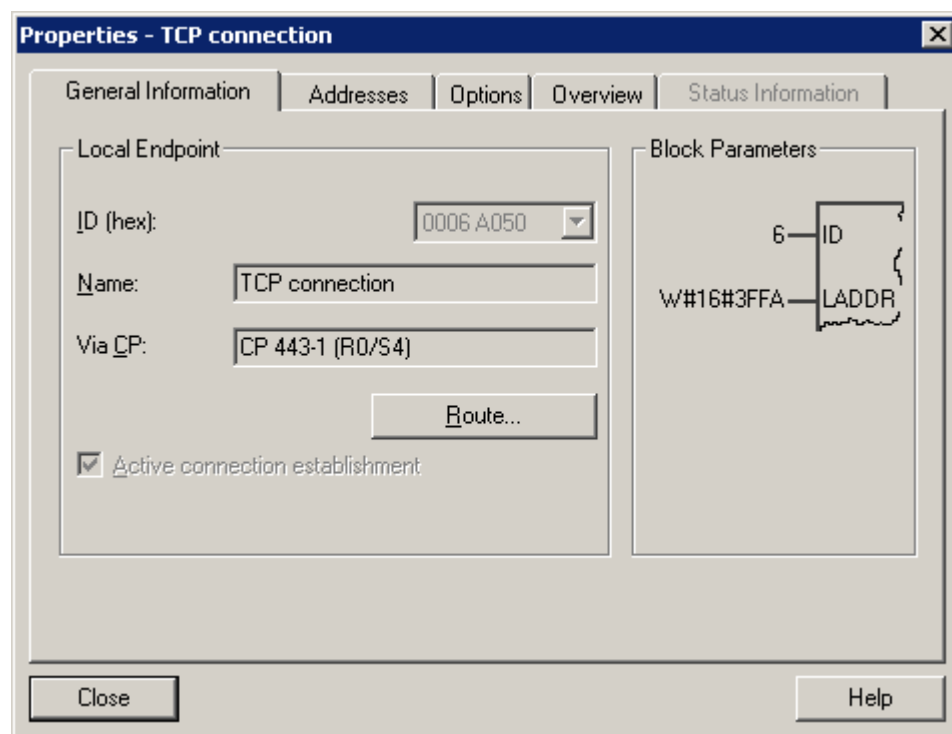
Jak již bylo uvedeno, pro konfiguraci spojení jsem zvolil TCP komunikaci. Tu je nutné definovat v nástroji NetPro, který je součástí balíku vývojových nástrojů STEP 7. Pro konfiguraci spojení pomocí průmyslového Ethernetu zvolíme na obou komunikačních partnerech volbu Insert New Connection a nastavíme dle obrázku (Obr. 28).

| Local ID | Partner ID | Partner | Type | Active | Local inte | Partner int | Local address | Partner address |
|-----------|------------|-------------|----------------|--------|------------|-------------|---------------|-----------------|
| 0006 A050 | 0004 A050 | CPU414-3... | TCP connection | Yes | CP 443-1 | CP 443-1 | 170.173.0.221 | 170.173.0.220 |
| 0004 A050 | 0006 A050 | CPU416F-... | TCP connection | No | CP 443-1 | CP 443-1 | 170.173.0.220 | 170.173.0.221 |

Obr. 28. Nastavení parametrů obou komunikačních partnerů

U každé stanice je pak nutné opsat parametry nutné k nastavení komunikace v programu. Jedná se o identifikátor komunikace ID, který může nabývat hodnot 1 až 64 u PLC systémů S7-400 a hodnot 1 až 16 u systémů S7-300. Parametr LADDR určuje počáteční adresu modulu komunikačního procesoru (Obr. 29). K tomuto dialogovému oknu se lze dostat pomocí stisku pravého tlačítka na řádek parametrů (Obr. 28) a zvolit volbu Properties a záložku General Information.

Nejsou-li komunikační partneři konfigurováni ve stejném projektu STEP 7, vytvoří se nespecifikované spojení. Je nutné správně nastavit IP adresy a masku sítě tak, aby spolu mohly jednotky komunikovat.



Obr. 29. Parametry komunikace

9.3 Sledování a analýza datových paketů

Pro analýzu správnosti komunikace jsou vhodné různé nástroje. Vývojové prostředí Siemens STEP 7 disponuje volbou přepnutí z pasivního náhledu do on-line režimu ve většině svých vývojových modulů (NetPro, LAD/STL/FBD Editor). Sledování jednotlivých stavů proměnných prostředí lze sledovat, a za běhu měnit, pomocí editoru VAT (Varia-

ble table). Základní představu o existenci linkového spojení mezi komunikačními procesory lze získat při pohledu na stavové LED, které jsou umístěny na přední části čele těla modulu. Statistiky o historii úspěšnosti přenosu paketů jsou součástí projektu Step7.

Chceme-li ale analyzovat skutečně přenášená data mezi komunikačními procesory, je nutné výměnu dat zaznamenávat. K tomu slouží zachytávače a analyzátory paketů. Mezi nej-používanější patří pravděpodobně nástroje tcpdump a Wireshark.

Pakety lze zaznamenávat na počítači, na kterém je zachytávač paketů nainstalován. Viditelné jsou standardně zejména tyto pakety:

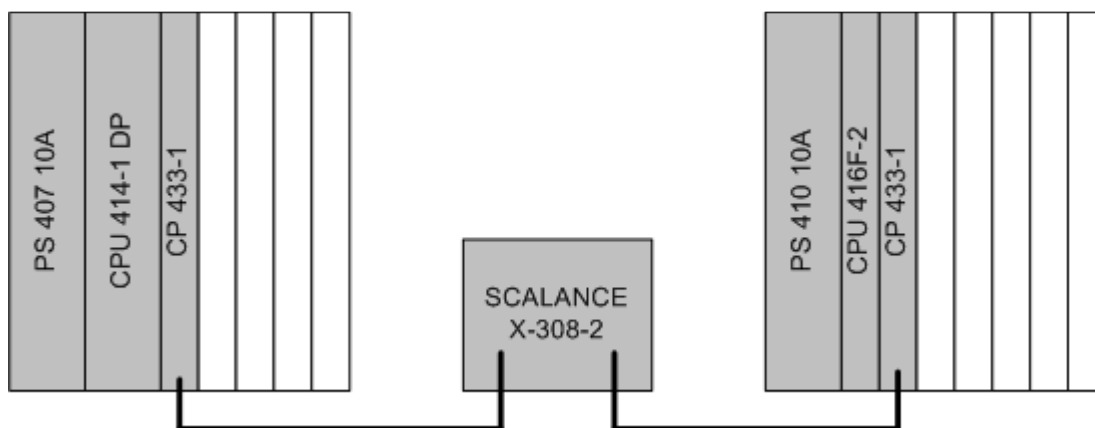
- Odchozí unicasty (jsou adresovány kterémukoliv jinému účastníkovi sítě),
- příchozí unicasty (těm naslouchá síťový adaptér),
- broadcasty (těm naslouchají všechna síťová zařízení v síti).

Pro úspěšný odposlech síťové komunikace je nutné přivést data tekoucí mezi jinými účastníky k síťovému adaptéru analyzujícího počítače. Běžně k takové situaci nedochází, neboť síťové přepínače zasílají unicasty pouze do těch portů, kterými vede cesta k adresátovi. K záznamu datového provozu slouží například nástroj rpcapd.exe, který je součástí programu WinPcap. Pro záznam paketů stačí tento nástroj spustit a později zaznamenaná data analyzovat například v programu Wireshark. [23, s. 169]

Nevýhodou tohoto řešení je aplikovatelnost pouze na počítače s podporovaným operačním systémem. Průmyslové systémy spuštění analyzátoru běžně neumožňují.

Řešením může být použití staršího typu síťového rozbočovače – hubu. Ten síť nepřepíná a vytváří tzv. kolizní doménu, ve které všichni účastníci vysílají do celé sítě. V případě kolize dojde k její detekci a zpráva se zašle znovu.

Nejoptimálnější řešení v průmyslovém prostředí je využití funkce zrcadlení, kterou je možné zapnout na průmyslovém přepínači Siemens SCALANCE X_308-2 (Obr. 30). Výhodou tohoto řešení je možnost vrátit systém zase do původního stavu bez nutnosti přepojování kabelů. Více o konfiguraci funkce zrcadlení je uvedeno v teoretické části práce.



Obr. 30. Propojení dvou PLC pomocí průmyslového přepínače SCALANCE

10 VIZUALIZACE DATOVÉHO SPOJENÍ VE WINCC

Existenci datového spojení lze zjistit buď přímým sledováním běhu programu v PLC nebo je možné tyto stavy vizualizovat pomocí některého dostupného nástroje. Vzhledem k přímé návaznosti funkcí vizualizačního systému Siemens SIMATIC WinCC na PLC systémy Siemens SIMATIC S7 a dispozici vývojové licence jsem zvolil WinCC verze 6.0, který je instalovaný na PC s operačním systémem Microsoft Windows XP SP3.

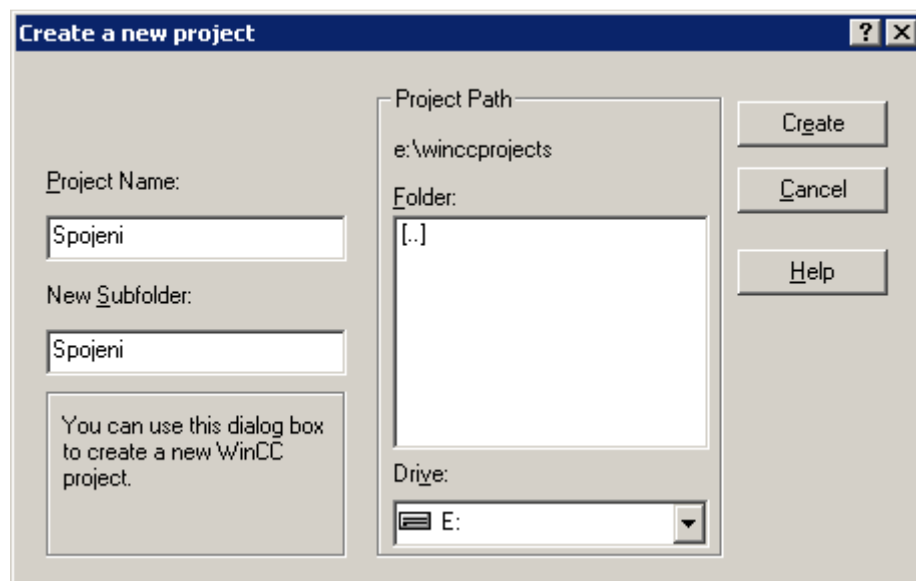
Vizualizační projekt vyžaduje spuštění na pracovní stanici (PC nebo IPC), na které je instalován systém WinCC s licencí, která odpovídá počtu použitých tagů. Ke spuštění a běhu vizualizace slouží tzv. run-time licence (RT), které se distribuují dle počtu použitých tagů. Pro návrh a tvorbu vizualizace je nutné použít vývojovou licenci (RC).

Dále musí být splněna podmínka existence datového spojení pomocí některé z podporovaných komunikačních sběrnic. V tomto případě se jedná o komunikační kanál TCP/IP, který využívá síť Ethernet. Další podporované komunikační kanály jsou např. Profibus, MPI, Industrial Ethernet aj.

Přímé datové spojení s PLC Siemens SIMATIC S7 lze realizovat pouze v případě, pokud zakoupěna a instalována licence komunikačního prostředí Siemens SIMATIC NET.

10.1 Nový vizualizační projekt

Celý proces návrhu, tvorby a oživení vizualizačního projektu probíhá ve vývojovém prostředí Siemens SIMATIC WinCC – v nástroji WinCC Explorer. Nástroj je k dispozici ihned po instalaci a je přístupný z menu Start – Siemens Automation – SIMATIC – WinCC nebo z plochy pomocí zástupce WinCC v 6.0. Po spuštění se zobrazí prázdná pracovní plocha nástroje. Nový projekt se zakládá spuštěním příkazu „New Project“ (ikona na nástrojové liště nebo menu File). Nyní je nutné zvolit typ projektu. Vizualizační systém bude provozován pouze na jedné pracovní stanici a nebude se jednat o server. Tomuto modelu vyhovuje nejlépe volba „Single-User Project“. Stisk tlačítka „OK“ vyvolá dialogové okno, ve kterém se určí název a umístění projektu na pevném disku pracovní stanice (Obr. 31). Projekt tvoří stromová struktura složek a datových souborů (Obr. 35); ta se vytvoří po stisku tlačítka „Create“.



Obr. 31. WinCC Explorer: Definice nového vizualizačního projektu

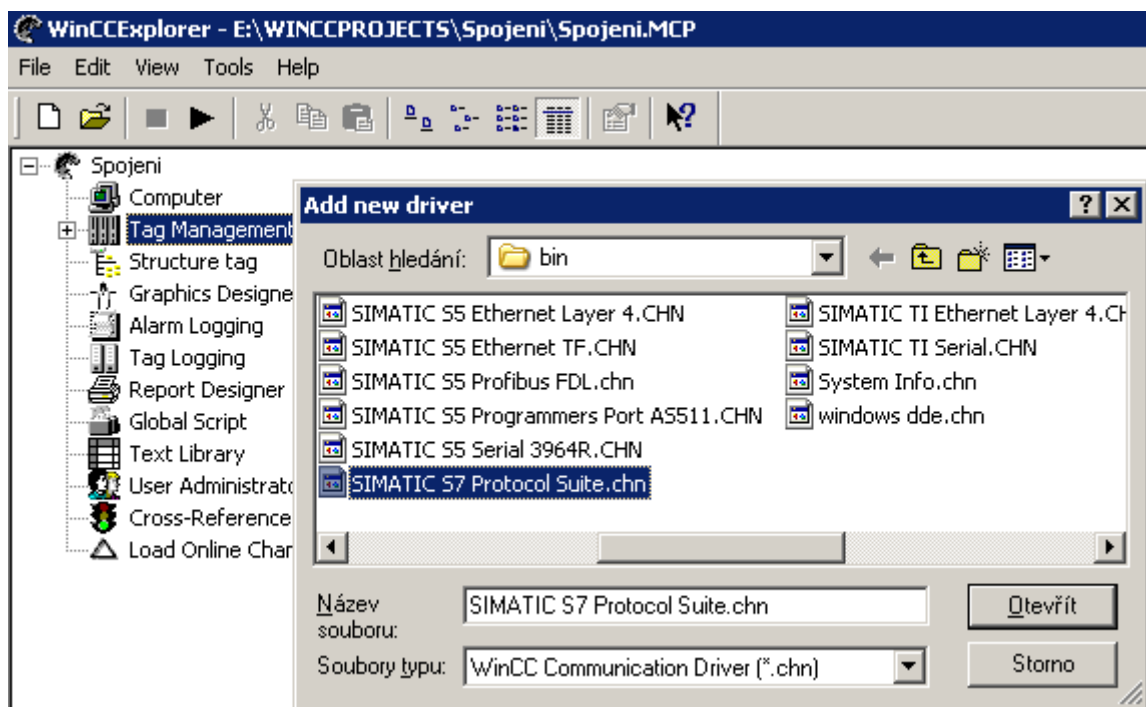
10.2 Definice komunikačního rozhraní a spoje

Komunikace mezi vizualizačním systémem a sledovanými zařízeními je zprostředkován pomocí tzv. komunikačních ovladačů (Communication Drives). Každá instalace WinCC disponuje velkým množstvím rozhraní pro zařízení a sběrníkové systémy různých výrobců.

Každý komunikační ovladač je ve vývojovém prostředí WinCC propojen s nástrojem pro správu tzv. tagů. Tag je speciální datová struktura, která reprezentuje datovou strukturu na straně sledovaného (řízeného systému).

Datové spojení se vytváří pomocí nástroje „Tag Management“ volbou „Add New Driver“. V dialogovém okně se zobrazí ve formě výpisu datových souborů seznam všech dostupných komunikačních ovladačů (Obr. 32). Komunikační ovladače jsou reprezentovány datovými soubory s příponou „chn“ a jsou ve výchozí konfiguraci instalovány do složky „bin“ systému WinCC (umístění této složky se může lišit).

V každém vizualizačním projektu může být zvoleno více komunikačních ovladačů, ale vícenásobný import stejného ovladače do jednoho projektu pro různá spojení stejného typu nejsou třeba.



Obr. 32. WinCC Explorer: Volba komunikačního ovladače

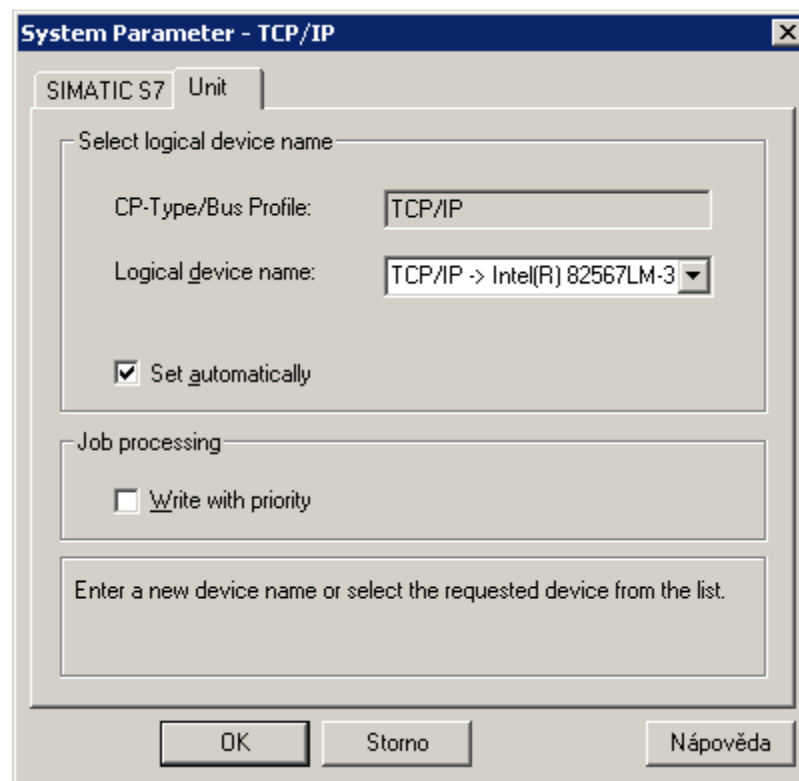
Zvolením některého komunikačního ovladače (zde „SIMATIC S7 Protocol Suite.chn“) dojde k aktualizaci stromové struktury projektu a v položce Tag Management (vždy umístěna pod položkou Internal Tags) se zobrazí nové rozhraní s možností připojení zařízení daného typu.

Každý komunikační ovladač může zprostředkovávat spojení s jedním či více datovými spoji. V projektu WinCC je tento prostředník reprezentovaný kanálem (Channel Unit), zde „TCP/IP“. Každý kanál je podřízený zvolenému komunikačnímu ovladači. Každému kanálu se během konfigurace vnitřně přiřazuje jednoznačná adresa.

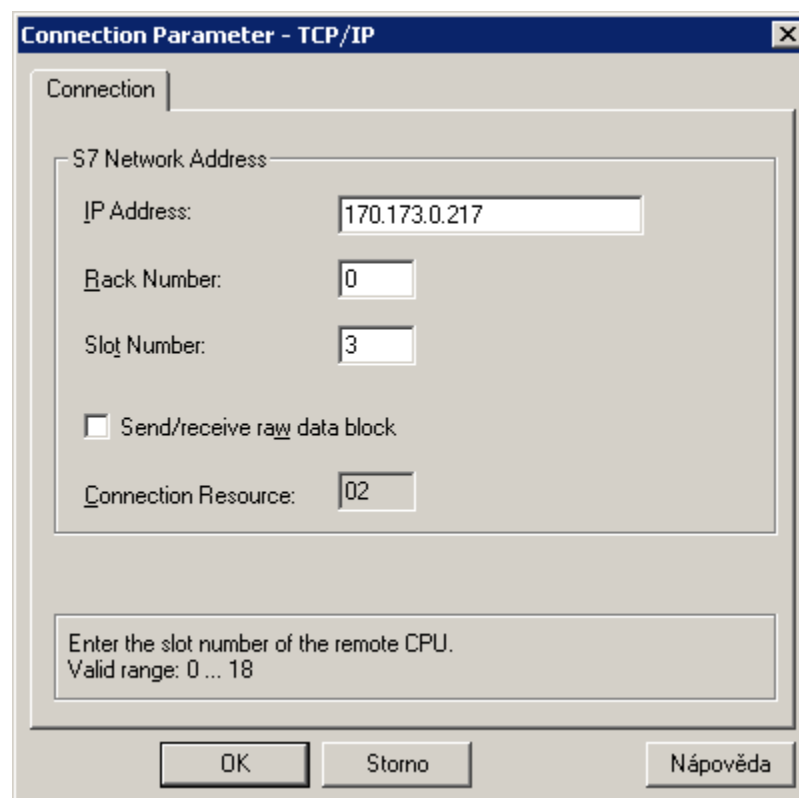
Vlastní přiřazení se nastavuje v okně „System Parameter“, to lze vyvolat pomocí menu zvoleného komunikačního kanálu.

Každý komunikační ovladač má odlišné možnosti nastavení, proto se také liší jeho konfigurační dialogové okno. Vždy jsou zde volby nastavení komunikačního rozhraní, ostatní parametry jsou vždy specifické pro daný typ zařízení.

U komunikace pomocí standardního ethernetového rozhraní stačí zvolit nabízený název komunikačního modulu, zde „TCP/IP -> Intel(R) 82567LM-3 Gigabit Network Connection“ (Obr. 33).



Obr. 33. WinCC Explorer: Nastavení komunikačního rozhraní



Obr. 34. WinCC Explorer: IP adresa a pozice CPU v racku S7

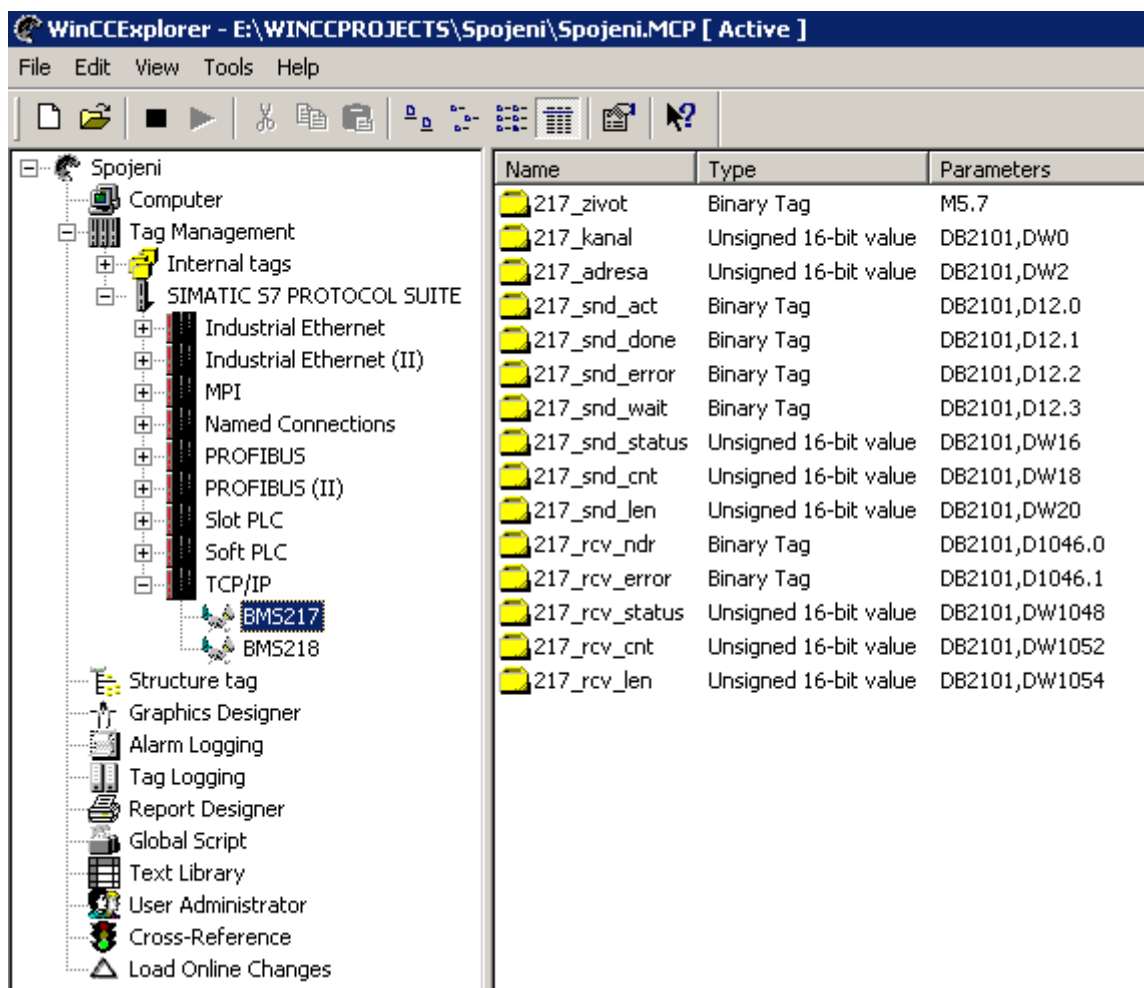
Aby bylo možné komunikovat se vzdáleným zařízením (např. PLC), je nutné vytvořit spojení. Spojení umožňuje oboustrannou výměnu dat. Vytvoří se tak, že v menu položky kanálu se zvolí položka „New Driver Connection“. Každému spojení je nutné přiřadit název a v nastavení „Connection Parameter“ také zvolit IP adresu komunikačního partnera a umístění CPU řídicí jednotky v racku (Obr. 34). Toto nastavení je odlišné pro různá komunikační zařízení.

Každý typ spojení má své speciální nastavení a zjednodušeně lze říci, že specifické parametry vždy určují hardwarovou adresu komunikačního partnera. Každé spojení musí mít v rámci vizualizačního projektu jedinečný název.

10.3 Určení datových bodů

Datové body (tagy) umožňují přístup ke většině oblastí uživatelské paměti PLC. Před vlastním návrhem grafické podoby vizualizace je nutné tyto tagy definovat. Tagy jsou dvojího druhu – tagy vázané na spojení a interní tagy. Tagy vázané na spojení (někdy označované jako externí) se od interních tagů liší tím, že nemají žádnou přímou vazbu na připojené zařízení. Tagy je nutné vytvořit pro každé datové spojení zvlášť. Nový tag se vytváří pomocí volby „New Tag“ na položce zvoleného datového spojení. Každý tag musí mít v rámci celého vizualizačního projektu jedinečný název. Dialogové okno dále nabízí volbu mezi několika datovými typy. Externí tagy mohou mít ve WinCC tyto typy:

- Binární tag,
- 8bitový bezznaménkový typ,
- 8bitový znaménkový typ,
- 16bitový bezznaménkový typ,
- 16bitový znaménkový typ,
- 32bitový bezznaménkový typ,
- 32bitový znaménkový typ,
- číslo s plovoucí desetinnou čárkou dle IEEE 754 (32bitové),
- číslo s plovoucí desetinnou čárkou dle IEEE 754 (64bitové),
- řetězcový (textový) typ 8bitové znakové sady,
- řetězcový (textový) typ 16bitové znakové sady,
- nspecifikovaná data (tzv. „Raw Data“).



Obr. 35. Vizualizace datového spojení: Definice tagů

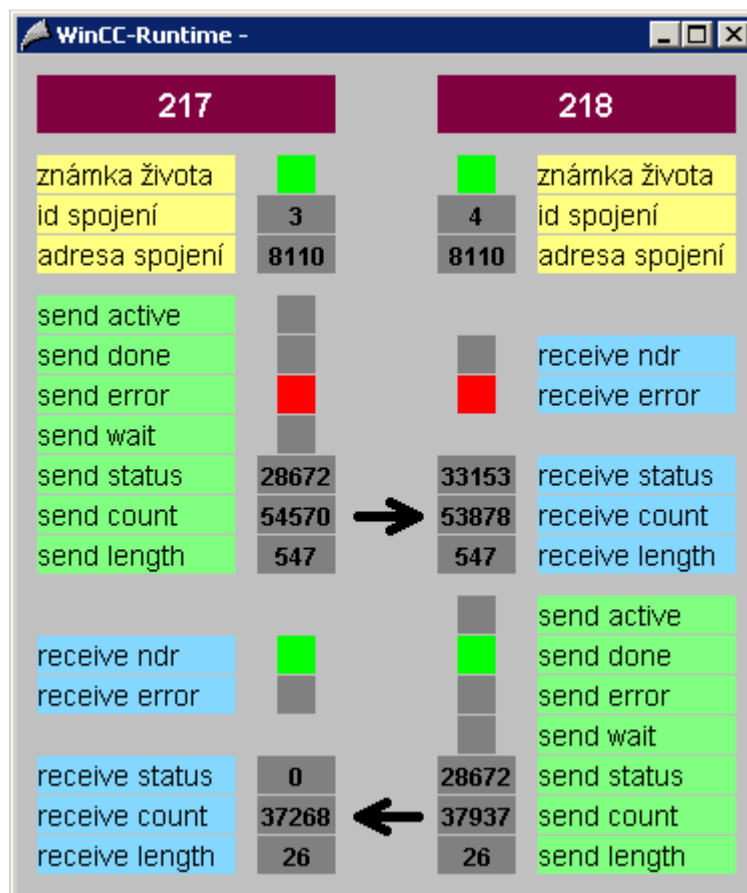
S výjimkou binárních datových typů lze mezi všemi výše uvedenými typy provádět typovou konverzi pomocí vestavěných funkcí. Typová konverze není ve výchozím nastavení volána, WinCC tag je spárován přímo s datovou strukturou PLC dle jejího typu.

Pro potřebu vizualizace dvou datových spojení jsem vytvořil dvě datová spojení pomocí komunikačního ovladače TCP/IP a pro každé s těchto spojení jsem definoval stavové tagy, které slouží k zobrazení aktuálního stavu spojení dvou PLC. Pro binární datové typy je ve výchozím nastavení použit binární tag, pro hodnoty typu Word (PLC) je použit beznámenkový 16bitový tag (Obr. 35).

10.4 Vizualizační schéma

Pro tvorbu vizualizačních schémat slouží nástroj WinCC Graphic Designer. Základním datovým objektem je plátno, na které lze umisťovat různé vektorové grafické objekty. Tyto objekty mají jednak vlastnosti statické (styly, barvy, rozměry), na druhé straně jim lze přiřadit speciální dynamické vlastnosti. Ty jsou zpravidla vázány na tagy. Dynamickou obsluhu objektu lze volat přímým spojením na tagy nebo sestavením programu v jazyku ANSI-C nebo pomocí jazyka VBS.

Pomocí palety objektů jsem vytvořil přehled všech stavových hodnot datového spojení mezi dvěma programovatelnými automaty. Poruchové stavy jsou znázorněny červeně, varovné žlutě a stavové zeleně. Jsou zde také k dispozici čítače počtu zpráv a hodnota délky poslední úspěšně zaslané zprávy. Pro rychlou identifikaci spojení na straně PLC slouží informace o identifikátoru spojení a adresa komunikačního rozhraní (Obr. 36).



Obr. 36. Vizualizace datového spojení v režimu run-time

Vizualizace se spouští pomocí programu WinCC Explorer. V menu File/Open je potřeba nalézt složku s vizualizačním projektem „Spojení“ a najít datový soubor Spojeni.MCP, který slouží k popisu celkého projektového stromu. Stiskem tlačítka Run se provede inicializace všech datových spojení a externích tagů, ihned poté se zobrazí okno samotné vizualizace (Obr. 36).

10.5 Uvedení do provozu

Projekt vizualizačního projektu lze spustit na kterékoliv pracovní stanici PC nebo IPC, na které je instalovaný vizualizační systém Siemens SIMATIC WinCC 6.0 a vyšší a pro možnost přímého datového spojení také Siemens SIMATIC NET. Oba produkty musejí být instalovány s potřebnými licenčními soubory.

V případě nasazení vizualizačního projektu pro sledování stavu komunikace mezi průmyslovými automaty v libovolném prostředí, je nutné nastavit následující parametry:

- Komunikační zařízení v okně System Parameter komunikačního kanálu TCP/IP,
- IP adresa, číslo racku a slotu v dialogovém okně Connection Parameter,
- číslo datového bloku S7 PLC,
- v případě odlišností struktury datového bloku S7 také změnit příslušné adresy a datové typy v rámci tohoto datového bloku.

Vizualizační část projektu si neklade za cíl kompletní správu spojení. Tu lze sledovat i upravovat pomocí nástroje Siemens SIMATIC Step7. Vizualizace v tomto provedení slouží pouze k pasivnímu prohlížení aktuálního stavu komunikace mezi dvěma programovatelnými automaty a umožňuje tak obsluhu diagnostikovat příčinu selhání nebo nefunkčnosti spojení. Pomocí tohoto nástroje lze také sledovat objem přenesených dat v poslední datové zprávě.

ZÁVĚR

V této práci byly popsány technické a bezpečnostní aspekty možnosti nasazení přímého datového spojení pro výměnu dat mezi průmyslovými automaty SIMATIC S7-400 vyvinuté společností Siemens. Důraz byl kladen především na možnosti volby softwarových komunikačních prostředků na straně PLC v závislosti na charakteru přenášených dat.

Určil jsem hlavní slabá místa datových spojení mezi PLC. Zaměřil jsem se také problémy s konfigurací aktivních síťových prvků na jejich spojové vrstvě.

Zhodnotil jsem možnosti použití jednotlivých komunikačních funkcí, kterými disponují průmyslové automaty Siemens SIMATIC S7-300 a S7-400. Zaměřil jsem se na vzájemnou kompatibilitu komunikačních bloků a na možnosti jejich využití.

Pomocí jazyku Step7 jsem realizoval datové spojení mezi dvěma PLC a vytvořil kanál pro obousměrnou výměnu dat pomocí protokolu TCP. Vytvořil jsem vizualizaci tohoto spojení pomocí SCADA systému Siemens SIMATIC WinCC. Vytvořené programové kódy byly úspěšně oživeny a testovány na dvou PLC řady S7-400.

Práce by měla posloužit k rychlejšímu nasazení komunikačních tras se stejnými či podobnými požadavky na objem přenášených dat. Měla by také upozornit na možná bezpečnostní rizika při úpravách stávajících instalací, zejména v souvislosti s potenciálním rizikem napadení často užívaných průmyslových automatizačních systémů.

V místě realizace nebyly bezpečnostní otázky komunikace mezi průmyslovými řídicími systémy doposud zohledňovány. Principů výměny dat je mnoho, v této práci byly popsány technologie, které jsou pro potenciální místa budoucího nasazení charakteristické.

Je pravděpodobné, že v místě instalace dojde k postupnému přechodu řízení toku výroby z centrálního na decentralizované autonomní celky, které budou i nadále řízeny programovatelnými automaty. Postupem času ale dojde ke zvyšování objemu přenášených dat mezi PLC, a zde je nutné si položit otázku, jakou budou mít tato data velikost, charakter a citlivost obsahu na případný odposlech, ztrátu nebo změnu.

Přímé spojení PLC do budoucna umožní rychlejší odezvu řídicího systému na aktuální stavy dopravníkové techniky (zaplnění, prostoje) a možnost téměř okamžité reakce na změny parametrů systému řízení výroby. To si však žádá kvalitní návrh budoucího informačního systému řízení výrobního toku.

SEZNAM POUŽITÉ LITERATURY

- [1] BERESFORD, Dillon. Exploiting Siemens Simatic S7 PLCs. In: *Black Hat USA 2011, Las Vegas* [online]. Las Vegas, 2011 [cit. 2014-08-02]. Dostupné z: http://media.blackhat.com/bh-us-11/Beresford/BH_US11_Beresford_S7_PLCs_WP.pdf
- [2] ZEZULKA, František. *Prostředky průmyslové automatizace*. 1. vyd. Brno: VUTIUM, 2004, 176 s. ISBN 80-214-2610-1.
- [3] MARTINÁSKOVÁ, Marie a Ladislav ŠMEJKAL. *Řízení programovatelnými automaty*. Vyd. 1. Praha: ČVUT, 1998, 160 s. ISBN 80-010-1766-4.
- [4] BERGER, Von Hans. *Automatisieren mit STEP 7 in AWL: speicherprogrammierbare Steuerungen SIMATIC S7-300/400*. 2., wesentlich überarb. und erw. Aufl. Erlangen: Publicis-MCD-Verl, 1998. ISBN 38-957-8089-8.
- [5] ČSN EN 61131-3 ed. 2. *Programovatelné řídicí jednotky - Část 3: Programovací jazyky*. Praha: Český normalizační institut, 2013.
- [6] MARTINÁSKOVÁ, Marie a Ladislav ŠMEJKAL. *Řízení programovatelnými automaty III: softwarové vybavení*. Vyd. 1. Praha: Vydavatelství ČVUT, 2003, 161 s. ISBN 80-010-2804-6.
- [7] KABELOVÁ, Alena a Libor DOSTÁLEK. *Velký průvodce protokoly TCP/IP a systémem DNS*. 5., aktualiz. vyd. Brno: Computer Press, 2008, 488 s. ISBN 978-80-251-2236-5.
- [8] ŠMRHA, Pavel. *Internetworking pomocí TCP/IP*. 1. vyd. České Budějovice: KOPP, 1994, 134 s. ISBN 80-858-2809-X.
- [9] PROFINET: the leading Industrial Ethernet Standard. *PROFIBUS and PROFINET International* [online]. 2014 [cit. 2014-08-06]. Dostupné z: <http://www.profibus.com/technology/profinet/overview/>
- [10] PUŽMANOVÁ, Rita. *TCP/IP v kostce*. 1. vyd. České Budějovice: Kopp, 2004, 607 s. ISBN 80-723-2236-2.
- [11] What should you pay attention to with the autonegotiation function for negotiating the LAN mode in Industrial Ethernet CPs? *Siemens Industry Online Support* [online]. 2014 [cit. 2014-08-02]. Dostupné

- z: <https://support.automation.siemens.com/WW/llisapi.dll?func=cslib.csinfo&objId=28710262>
- [12] ERICKSON, Jon. *Hacking: umění exploitace*. 2., upr. a dopl. vyd. Překlad Jan Pokorný. Brno: Zoner Press, 2009, 544 s. ISBN 978-80-7413-022-9.
- [13] WIRESHARK FOUNDATION. *Wireshark* [software]. Dostupné z: <http://www.wireshark.org>.
- [14] FALLIERE, Nicolas, Liam O'MURCHU a Eric CHIEN. W32.Stuxnet Dossier. SYMANTEC CORPORATION. *Symantec* [online]. Cupertino, 2011 [cit. 2014-07-30]. Dostupné z: http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf
- [15] VLACH, Jaroslav. *Řízení a vizualizace technologických procesů*. 1. vyd. Praha: BEN - technická literatura, 1999, 159 s. ISBN 80-860-5666-X.
- [16] FOWLER, Martin. *Destilované UML*. 1. vyd. Praha: Grada, 2009, 173 s. *Knihovna programátora (Grada)*. ISBN 978-80-247-2062-3.
- [17] VLASÁK, Rudolf. *Základy projektování informačních systémů*. 1. vyd. Praha: Karolinum, 2003, 144 s. ISBN 80-246-0727-1.
- [18] WRÓBLEWSKI, Piotr. *Algoritmy: datové struktury a programovací techniky*. Vyd. 1. Překlad Marek Michalek, Bogdan Kiszka. Brno: Computer Press, 2004, 351 s. ISBN 80-251-0343-9.
- [19] GAJDŮŠEK, Jaroslav a Miroslav ŠKOPÁN. *Teorie dopravních a manipulačních zařízení*. Brno: Rektorát VUT v Brně, 1988. ISBN 55-517-88.
- [20] Compatibility list of STEP 7 (TIA Portal) and MS Windows. SIEMENS AG. *Siemens Industry Online Support* [online]. 2014 [cit. 2014-08-02]. Dostupné z: https://support.automation.siemens.com/WW/llisapi.dll/csfetch/8250891/8250891_Kompat_STEP7_Win_e.pdf?func=cslib.csFetch&nodeid=58364079
- [21] BYSTRICĀNOVÁ, Anna a Daniel RYBOVIČ. Data communication between programmable logic controllers in the industrial distribution applications. *Advances in electrical and electronic engineering*. 2011, roč. 9, č. 2, 96–102.
- [22] Program blocks for SIMATIC NET S7 CPs: Programming Manual. SIEMENS AG. *Siemens AG* [online]. 2012 [cit. 2014-07-16]. Dostupné z: <http://support.automation.siemens.com/WW/view/en/30564821>

- [23] LOCKHART, Andrew. *Bezpečnost sítí na maximum*. Vyd. 1. Překlad Jiří Veselský. Brno: CP Books, 2005, 276 s. ISBN 80-251-0805-8.

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

| | |
|----------|--|
| FBD | Functional Block Diagram; schéma funkcí; něm. der Funktionsplan (FUP). |
| ICS | Industrial Control System; průmyslový řídicí systém. |
| IEC | International Electrotechnical Commission; organizace zabývající se standardizací elektronických a souvisejících technologických norem. |
| IEEE | Institute of Electrical and Electronics Engineers; mezinárodní nezisková profesní organizace, která se zabývá elektrotechnikou. |
| IPC | Industrial PC, průmyslové PC. |
| ISO | International Organization for Standardization; Mezinárodní organizace pro normalizaci. |
| LAD | Ladder Diagram; kontaktní schéma; něm. der Kontaktplan (KOP). |
| MPI | Multipoint Interface. Základní komunikační rozhraní využívané systémy Siemens SIMATIC S7. |
| PG | Programmierungsgerät. PC nebo notebook sloužící k programování PLC. |
| PLC | Programable Logic Controller; programovatelný logický automat; něm. die Speicherprogrammierbare Steuerung (SPS). |
| PROFIBUS | Process Field Bus; průmyslová sběrnice určená pro automatizaci a řízení výrobních technologií. |
| PROFINET | průmyslová komunikační sběrnice, nástupce Industrial Ethernet. |
| SCADA | Supervisory Control And Data Acquisition. Systém pro řízení toku výroby, sběru dat a dálkovému sledování průmyslových procesů. |
| STEP 7 | vývojové prostředí a jazyk pro PLC řady SIMATIC S7. |
| STL | Statement List; seznam instrukcí; něm. die Anweisungsliste (AWL). |
| TIA | Totally Integrated Automation. Strategie vyvinutá v roce 1996 společností Siemens; definuje vztahy mezi komponentami, nástroji a službami. |
| TSAP | Transport Service Access Point, nebo též ISO-TSAP; komunikační protokol využívající port TCP 102, který se používá pro přenos dat v oblasti průmyslové automatizace. |

SEZNAM OBRÁZKŮ

| | |
|--|----|
| Obr. 1. Blokové schéma modulárního PLC | 13 |
| Obr. 2. Programová smyčka PLC | 16 |
| Obr. 3. Časový diagram základní funkce PLC | 16 |
| Obr. 4. SIMATIC Manager STEP 7 | 17 |
| Obr. 5. STEP 7: LAD/STL/FBD editor | 18 |
| Obr. 6. Wireshark: Záznam síťové komunikace – funkce Follow TCP Stream | 28 |
| Obr. 7. SIMATIC Manager STEP7: Příkaz CPU STOP | 30 |
| Obr. 8. Schéma propojení dvou PLC | 35 |
| Obr. 9. LAD/STL/FBD Editor: Definice UDT pro PIN | 40 |
| Obr. 10. LAD/STL/FBD Editor: Definice UDT pro volbu linie | 41 |
| Obr. 11. STEP 7 Professional: Volba programových komponent | 44 |
| Obr. 12. STEP 7 Professional: Automation License Manager | 45 |
| Obr. 13. SIMATIC NET Configuration Console | 46 |
| Obr. 14. Hardwarová konfigurace zkušebních CPU | 47 |
| Obr. 15. SCALANCE: Aktivace funkce zrcadlení portu | 48 |
| Obr. 16. SCALANCE: Aktivace zrcadlení portu na zvolený port | 48 |
| Obr. 17. Pohled na instalaci zkušebních CPU a průmyslového switchu | 49 |
| Obr. 18. Volání komunikačního funkčního bloku z OB1 | 51 |
| Obr. 19. Podmínky inicializace požadavku odesílání dat a life signál | 52 |
| Obr. 20. Volání funkce AG_LSEND (FC50) | 53 |
| Obr. 21. Sekvenční diagram funkce AG_LSEND (FC50) | 54 |
| Obr. 22. Deaktivace volání funkce AG_LSEND v případě poruchy | 55 |
| Obr. 23. Volání funkce AG_LRECV (FC60) | 55 |
| Obr. 24. Sekvenční diagram funkce AG_LRECV (FC60) | 56 |
| Obr. 25. Inicializace trvalé jedničky a trvalé nuly | 58 |
| Obr. 26. Nastavení Clock Memory | 59 |
| Obr. 27. Kontrola obsazenosti uživatelské paměti | 60 |
| Obr. 28. Nastavení parametrů obou komunikačních partnerů | 60 |
| Obr. 29. Parametry komunikace | 61 |
| Obr. 30. Propojení dvou PLC pomocí průmyslového přepínače SCALANCE | 63 |
| Obr. 31. WinCC Explorer: Definice nového vizualizačního projektu | 65 |
| Obr. 32. WinCC Explorer: Volba komunikačního ovladače | 66 |

| | |
|---|----|
| Obr. 33. WinCC Explorer: Nastavení komunikačního rozhraní..... | 67 |
| Obr. 34. WinCC Explorer: IP adresa a pozice CPU v racku S7..... | 67 |
| Obr. 35. Vizualizace datového spojení: Definice tagů | 69 |
| Obr. 36. Vizualizace datového spojení v režimu run-time | 70 |

SEZNAM TABULEK

| | |
|---|----|
| Tab. 1. Struktura rámce protokolu IEEE 802.3-2012 | 19 |
| Tab. 2. CP-x43-1: Přehled dostupných komunikačních režimů | 24 |
| Tab. 3. ISO-TSAP: Struktura hlavičky paketu | 26 |
| Tab. 4. Přehled standardních funkcí pro přenos dat | 34 |
| Tab. 5. Přehled mezních hodnot objemů dat (AG_xSEND, AF_xRECV)..... | 35 |
| Tab. 6. Přehled některých prvků dopravníkové techniky | 39 |
| Tab. 7. Přehled základních stavů funkce AG_LSEND..... | 53 |
| Tab. 8. Přehled základních stavů funkce AG_LRECV | 57 |
| Tab. 9. Přiřazení časových period jednotlivým bitům Clock Memory..... | 58 |